ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗ ΧΡΗΣΤΩΝ ΣΕ ΔΙΚΤΥΑΚΕΣ ΠΥΛΕΣ ΚΑΙ ΥΠΗΡΕΣΙΕΣ

«ΕΦΑΡΜΟΓΕΣ ΣΕ ΔΙΚΤΥΑΚΕΣ ΥΠΗΡΕΣΙΕΣ ΔΗΜΟΣΙΩΝ ΟΡΓΑΝΙΣΜΩΝ»

Δημήτριος Καλλέας
Μεταπτυχιακός Φοιτητής, ΑΜ: ΜΑΙ 04/05

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Επιβλέπων: Ιωάννης Μαυρίδης, Επίκουρος Καθηγητής

Εξετεστής: Μανιτσάρης Αθανάσιος, Καθηγητής

Τμήμα Εφαρμοσμένης Πληροφορικής
Πρόγραμμα Μεταπτυχιακών Σπουδών Ειδίκευσης

Πανεπιστήμιο Μακεδονίας
Θεσσαλονίκη

Φεβρουάριος, 2007

ΠΕΡΙΛΗΨΗ

Τα τελευταία χρόνια οι ηλεκτρονικές υπηρεσίες μέσω του World Wide Web έχουν εξελιχθεί από την αρχική απλή εμφάνιση πληροφοριών σε πολύπλοκες εφαρμογές λογισμικού (*Web Applications*) οι οποίες προσπελαύνονται είτε μέσω μεμονωμένων δικτυακών τόπων (*Sites*) είτε μέσω εκτεταμένων Sites όπου προσφέρεται ένα ευρύ σύνολο συγκεντρωμένων δικτυακών πόρων και υπηρεσιών (*Portals*). Η παρούσα εργασία εξετάζει τις υπάρχουσες τεχνολογίες και πρωτόκολλα «αυθεντικοποίησης» ("*authentication*") χρηστών ηλεκτρονικών υπηρεσιών, του ελέγχου δηλαδή της αυθεντικότητας των ηλεκτρονικών στοιχείων που αντιστοιχούν στην ταυτότητα αυτών των χρηστών, ώστε να εγκριθεί η πρόσβασή τους. Επιπροσθέτως, επεξηγείται η φιλοσοφία τους και αντιδιαστέλλονται τα χαρακτηριστικά και οι αποδόσεις τους, ώστε να προκύψουν συγκριτικά αποτελέσματα αξιολόγησής τους. Η παρούσα εργασία επεκτείνεται και στην κάλυψη των απαιτήσεων διευκόλυνσης των χρηστών στα πλαίσια των πολλαπλών ηλεκτρονικών υπηρεσιών ενός οργανισμού (*Single Sign – On*) και στη διεύρυνση αυτών των λύσεων και της διαχείρισης των ταυτοτήτων χρηστών εκτός των ορίων ενός μόνο οργανισμού, μέσα στα πλαίσια συνεργασιών πολλών οργανισμών (*Federated Identity Management*). Με την εξέταση των συγκεκριμένων χαρακτηριστικών της αυθεντικοποίησης καταδεικνύεται ο σύνθετος χαρακτήρας της, αλλά και οι σοβαρές δυνατότητες που δημιουργεί προς την κατεύθυνση της αξιοποίησης του Internet, ειδικότερα από e-Commerce και e-Government εφαρμογές, καθώς καθίσταται δυνατή η εγκαθίδρυση συνεργασιών μεταξύ διαφορετικών οργανισμών στο επίπεδο της διαχείρισης ταυτοτήτων και είναι εφικτή η ύπαρξη ενιαίας αυθεντικοποίησης των χρηστών σε αυτές τις συνεργασίες (*Federations*). Η μελέτη εφαρμογών των συγκεκριμένων λύσεων εστιάζεται στην παρούσα εργασία στα έργα ανάπτυξης συστημάτων αυθεντικοποίησης σε ηλεκτρονικές υπηρεσίες Δημοσίων Οργανισμών, καθώς η έννοια της ταυτότητας και η επιβεβαίωσή της είναι πρωταρχικής σημασίας στις συναλλαγές πολιτών – κράτους και τα συγκεκριμένα συστήματα αποτελούν απαραίτητο τμήμα κάθε έργου e-Government που αποσκοπεί στη βελτίωση της παραγωγικότητας του Κράτους και του επιπέδου εξυπηρέτησης των πολιτών.

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΙΝΑΚΑΣ ΕΙΚΟΝΩΝ

ΠΙΝΑΚΑΣ ΠΙΝΑΚΩΝ

1. ΕΙΣΑΓΩΓΗ

1.1 Αντικείμενο της Εργασίας

Τα τελευταία χρόνια οι ηλεκτρονικές υπηρεσίες μέσω του World Wide Web έχουν εξελιχθεί από την αρχική απλή εμφάνιση πληροφοριών σε πολύπλοκες εφαρμογές λογισμικού οι οποίες έχουν αποκτήσει ρόλο εργαλείου παραγωγικότητας για τις ιδιωτικές επιχειρήσεις και το Δημόσιο Τομέα (*Web Applications*). Οι συγκεκριμένες υπηρεσίες προσφέρονται είτε μέσω μεμονωμένων δικτυακών τόπων (*Sites*) είτε μέσω εκτεταμένων Sites όπου προσφέρεται ένα ευρύ σύνολο συγκεντρωμένων δικτυακών πόρων και υπηρεσιών (*Portal*). Ειδικότερα τα Portals γίνονται ολοένα και πιο πολύπλοκα και η επιτυχία τους στηρίζεται στην εκμετάλλευση πολλών πηγών δεδομένων, οι οποίες συνήθως βρίσκονται σε διαφορετικούς εξυπηρετητές (*Web Servers*). Το γεγονός αυτό δημιουργεί ένα μεγάλο αριθμό θεμάτων προς επίλυση για τους σχεδιαστές – κατασκευαστές των Portals σχετικά με τη διαχείριση των χρηστών που χρησιμοποιούν τις ηλεκτρονικές υπηρεσίες. Ένα από αυτά τα ζητήματα είναι η πιστοποίηση της ταυτότητας των χρηστών των ηλεκτρονικών υπηρεσιών. Η συγκεκριμένη διαδικασία περιλαμβάνει τον έλεγχο της αυθεντικότητας των ηλεκτρονικών στοιχείων που αντιστοιχούν στην ταυτότητα των χρηστών, ώστε να εγκριθεί η πρόσβασή τους και καλείται «*αυθεντικοποίηση*» ("*authentication*").

Το πρόβλημα της αυθεντικοποίησης φαίνεται αρχικά εύκολο να μηχανοποιηθεί ή συστηματοποιηθεί μέσω ενός πρωτοκόλλου ή μίας τυποποιημένης διαδικασίας. Κατά την εφαρμογή, όμως, όλων αυτών σε ένα δικτυακό περιβάλλον Internet ή Intranet υπεισέρχονται επιπρόσθετοι παράμετροι πολυπλοκότητας. Το πρώτο, αυτονόητο πρόβλημα που έχουν να αντιμετωπίσουν οι εφαρμογές που διατίθενται μέσω του Internet είναι η προσβασιμότητά τους από ένα αναρίθμητο σύνολο χρηστών, από τους οποίους μόνο ορισμένοι είναι οι επιθυμητοί. Επιπροσθέτως, η πλειοψηφία των «απειλών» επέμβασης σε δικτυακές μεταδόσεις μέσω του Internet αποσκοπεί στην παραποίηση της διαδικασίας αυθεντικοποίησης, καθώς αυτή ρυθμίζει την είσοδο ενός χρήστη σε μία δικτυακή εφαρμογή ή όχι. Σε τεχνολογικό επίπεδο, ένα πρώτο ζήτημα είναι η διαλειτουργικότητα μεταξύ των διαφορετικών τεχνολογιών με τις οποίες αναπτύσσονται οι ηλεκτρονικές υπηρεσίες στα πλαίσια της λειτουργίας τους μέσω του Internet. Ταυτόχρονα, η ανάπτυξη μεγάλου αριθμού εφαρμογών καθιστά αναγκαία τη διευκόλυνση του χρήστη κατά τη διαδικασία της αυθεντικοποίησης, έτσι ώστε να μην διατηρεί πολλαπλά αντίγραφα της ταυτότητάς του σε πολλά διαφορετικά συστήματα και να μην υποχρεούται να υποβάλλει επανειλημμένα τα «πιστοποιητικά» της ταυτότητάς του καθώς προσπελαύνει διαφορετικές υπηρεσίες στα πλαίσια ενός Portal ή συνεργαζόμενων Sites. Από την πλευρά των οργανισμών που κατασκευάζουν αυτές τις υπηρεσίες υπάρχει η απαίτηση της μείωσης του κόστους διαχείρισης των στοιχείων των χρηστών άρα και της εγκατάστασης των μηχανισμών αυθεντικοποίησης. Παράλληλα, είναι απαραίτητο οι εφαρμοζόμενοι μηχανισμοί να μην καθιστούν το Internet εχθρικό προς τους χρήστες, αλλά αντίθετα να συνεισφέρουν στην εξάπλωση της χρήσης των υπηρεσιών του με τη φιλικότητα και την ασφάλεια που πρέπει να παρέχουν. Επιπροσθέτως, πρέπει να υποστηρίζουν τεχνολογικά κάθε προσπάθεια αξιοποίησης του Internet από οργανισμούς του Ιδιωτικού και Δημόσιου Τομέα με την εγκαθίδρυση συνεργασιών μεταξύ τους, την ανάπτυξη νέων επιχειρηματικών ή διοικητικών μοντέλων και τη διεξαγωγή πολλών διαδικασιών τους με ηλεκτρονικές μεθόδους.

Η πρώτιστη μέριμνα μίας λύσης αυθεντικοποίησης είναι η ασφάλεια και η μυστικότητα της συνολικής διαδικασίας. Η επιλογή των μηχανισμών που εξασφαλίζουν αξιόπιστη επιβεβαίω-

ση της πραγματικής ταυτότητας του χρήστη και η προστασία των στοιχείων ταυτότητας κατά τη διάρκεια υποβολής και ελέγχου τους είναι οι σημαντικότερες αρχές που διέπουν τις προτεινόμενες λύσεις αυθεντικοποίησης. Συνεπώς, πέρα από τη διατύπωση συγκεκριμένων σταδίων ενός πρωτοκόλλου αυθεντικοποίησης, μία ικανοποιητική λύση πρέπει να συνδυάζει και τεχνολογίες ή συσκευές προστασίας των δεδομένων ταυτοτήτων και εξασφάλισης της μοναδικότητας των στοιχείων διαφορετικών χρηστών, ώστε να είναι δυνατή η διάκρισή τους. Μέρος του εξεταζόμενου προβλήματος, επομένως, είναι και η κατάλληλη χρήση ή η αναζήτηση νέων τεχνολογιών, τεχνικών ή μηχανισμών κρυπτογράφησης και προστασίας των δεδομένων των χρηστών, ώστε να εμπλουτίζονται οι διαδικασίες της αυθεντικοποίησης, κάνοντας πιο περίπλοκη και ασύμφορη κάθε απόπειρα παραβίασης ή παραπλάνησης της διαδικασίας.

Από τα ανωτέρω βασικά προβλήματα που καλούνται να αντιμετωπίσουν οι τρέχοντες μηχανισμοί και λύσεις αυθεντικοποίησης παρουσιάζουν μεγαλύτερο ενδιαφέρον και αμεσότητα επίλυσης δύο συγκεκριμένα:

- Η διευκόλυνση των χρηστών κατά τη διαδοχική πρόσβασή τους σε πολλαπλές ηλεκτρονικές υπηρεσίες.

- Η τεχνολογική ενίσχυση των συνεργασιών και ανταλλαγών σε επίπεδο πληροφοριών ταυτοτήτων χρηστών μεταξύ διαφορετικών επιχειρηματικών ή κρατικών οργανισμών.

Στην πρώτη περίπτωση η αυθεντικοποίηση πρέπει να περιλαμβάνει μηχανισμούς με τους οποίους η επικύρωση των στοιχείων ταυτότητας ενός χρήστη κατά την είσοδό του σε ένα Portal να μπορεί να διατηρήσει την ισχύ της κατά την περαιτέρω επίσκεψη του χρήστη στις υπηρεσίες του Portal χωρίς την επανάληψη της διαδικασίας αυθεντικοποίησης. Η συγκεκριμένη υπηρεσία ονομάζεται *Single Sign – On* (*SSO*) και αποτελεί βασική απαίτηση προς τις λύσεις αυθεντικοποίησης χρηστών για την πρόσβασή τους σε πολλαπλές ηλεκτρονικές υπηρεσίες. Αυτή η απαίτηση βασίζεται στο γεγονός ότι με το SSO εξασφαλίζεται ομοιόμορφη προσέγγιση στη φάση της αυθεντικοποίησης η οποία απομονώνεται από την κύρια εφαρμογή και αποτελεί ένα αυτόνομο υποσύστημα. Οι χρήστες δεν είναι υποχρεωμένοι να διατηρούν πολλαπλά «πιστοποιητικά» για καθεμιά ηλεκτρονική υπηρεσία και περιορίζεται η επαναλαμβανόμενη μετάδοσή τους στο δίκτυο η οποία καθιστά αυτά τα στοιχεία ευάλωτα για υποκλοπή.

Η δεύτερη σημαντική απαίτηση για τις σύγχρονες διαδικασίες αυθεντικοποίησης σε υπηρεσίες του Internet περιλαμβάνει την επέκταση της ανωτέρω υπηρεσίας SSO εκτός των ορίων του Portal ενός οργανισμού και την παροχή της σε δικτυακές εφαρμογές διαφορετικών οργανισμών. Είναι, δηλαδή, έντονη η ανάγκη τόσο των επιχειρήσεων όσο και των δικτυακών χρηστών τους να μπορούν με ομοιόμορφο τρόπο να μεταβαίνουν από τη μία υπηρεσία ενός οργανισμού σε μία άλλη ενός άλλου, συνεργαζόμενου οργανισμού με μοναδικό, ασφαλή και αξιόπιστο τρόπο επιβεβαίωσης της ταυτότητάς τους. Με αυτό τον τρόπο δημιουργούνται συνεργασίες ή «ομοσπονδίες» ("*Federations*") οργανισμών στο επίπεδο των στοιχείων ταυτότητας των εξωτερικών χρηστών τους, ώστε να επεκτείνουν την επιχειρηματική τους δράση μέσω του Internet, να μειώσουν το κόστος διατήρησης και διαχείρισης ενός απροσδιόριστου αριθμού χρηστών και να προστατέψουν τα δεδομένα ταυτοτήτων των χρηστών τους. Η αυθεντικοποίηση, επομένως, πρέπει να καλύπτει και τις περιπτώσεις όπου ο έλεγχος της ταυτότητας ενός χρήστη δεν υλοποιείται στο σύστημα το οποίο επιχειρεί αυτός να προσπελάσει, αλλά σε ένα άλλο σύστημα το οποίο περιέχει τα γνήσια στοιχεία της ταυτότητάς του και πιθανώς να βρίσκεται σε έναν εντελώς διαφορετικό οργανισμό. Υπάρχουν επίσης και οι περιπτώσεις όπου ένας χρήστης διατηρεί πολλές εγγραφές της ταυτότητάς του σε διαφορετικούς οργανι-

σμούς και πρέπει να μεταβαίνει από τις υπηρεσίες του ενός οργανισμού σε αυτές ενός άλλου με τη σύνδεση των διαφορετικών ταυτοτήτων του, ώστε να του δίνεται η εντύπωση μίας ενιαίας ταυτότητας πρόσβασης σε ηλεκτρονικές υπηρεσίες (*Federated Identity*). Η συγκεκριμένη δυνατότητα, εφόσον μπορέσει να εξασφαλίσει αξιόπιστη και ασφαλή αυθεντικοποίηση, αποτελεί το έναυσμα για τη γρήγορη ανάπτυξη περισσότερων ηλεκτρονικών υπηρεσιών που θα είναι απαλλαγμένες από την αντιμετώπιση των προβλημάτων του ελέγχου των χρηστών, αλλά θα επικεντρώνονται στην εξυπηρέτηση του χρήστη και την διεύρυνση των επιχειρηματικών ή διοικητικών μοντέλων μέσα στο Internet.

Από τα παραπάνω γίνεται σαφές ότι η αυθεντικοποίηση, ειδικά σε ένα περιβάλλον υπηρεσιών μέσω Internet, είναι ένα σύνθετο πρόβλημα, πρωτίστως γιατί δεν είναι ελεγχόμενος ο αριθμός των χρηστών αυτών των υπηρεσιών. Γι αυτό το λόγο τα σύγχρονα συστήματα αναπτύσσουν ή ενσωματώνουν αυτόνομα συστήματα Διαχείρισης Χρηστών και Ταυτοτήτων τους (*Identity Management Systems*). Η αυθεντικοποίηση αποτελεί μέρος τέτοιων συστημάτων και ένα πρόσθετο πρόβλημα που προκύπτει είναι οι τρόποι συνεργασίας της με τα υπόλοιπα υποσυστήματά τους. Τα πιο σημαντικά υπο-συστήματα της Διαχείρισης Ταυτοτήτων είναι συνήθως:

- Η πρώτη εγγραφή των χρηστών στο σύστημα, όπου αποδεικνύεται η ταυτότητά τους και τους αποδίδονται τα ηλεκτρονικά «πιστοποιητικά» με τα οποία θα τους αναγνωρίζει και διακρίνει το σύστημα (*Registration*).

- Η δομή καταλόγου διατήρησης και αποθήκευσης των δεδομένων ταυτοτήτων και όλων των επιπρόσθετων ιδιοτήτων που χαρακτηρίζουν ένα χρήστη (*Directory*).

- Ο έλεγχος πρόσβασης των χρηστών και των εξουσιοδοτήσεων που έχει για την εκτέλεση ή απαγόρευση πρόσβασης σε συγκεκριμένες επιλογές της δικτυακής υπηρεσίας, εφόσον οι χρήστες περάσουν επιτυχώς τη φάση της αυθεντικοποίησης (*Authorization*).

Η αυθεντικοποίηση, συνεπώς, δεν μπορεί να αντιμετωπιστεί ως μία μεμονωμένη και αυτόνομη διαδικασία, καθώς οι μηχανισμοί που την υλοποιούν πρέπει να συνεργάζονται και με τις ανωτέρω διαδικασίες. Οι προτεινόμενες λύσεις αυθεντικοποίησης πρέπει να λειτουργούν βάσει διαδεδομένων προτύπων, για να εξασφαλίζεται έτσι η συνεργασία με τα συγκεκριμένα υπο-συστήματα. Το καθένα υπο-σύστημα ακολουθεί τη δικιά του πορεία τεχνολογικής εξέλιξης και δεν είναι άρρηκτα συνδεδεμένο με συγκεκριμένη υλοποίηση των υπολοίπων υποσυστημάτων, αλλά η διαλειτουργικότητά τους εξασφαλίζεται με διεπαφές που βασίζονται σε κοινά πρότυπα.

Η παρούσα εργασία εξετάζει τις υπάρχουσες τεχνολογίες και πρωτόκολλα αυθεντικοποίησης χρηστών ηλεκτρονικών υπηρεσιών. Πέρα από την παρουσίαση του τρόπου εφαρμογής των προτεινόμενων λύσεων αναλύεται η φιλοσοφία τους και γίνεται αντιδιαστολή των χαρακτηριστικών και αποδόσεών τους, ώστε να προκύψουν συγκριτικά αποτελέσματα αξιολόγησής τους. Η εξέταση των λύσεων επεκτείνεται και στην κάλυψη των προβλημάτων διευκόλυνσης των χρηστών στα πλαίσια των πολλαπλών υπηρεσιών ενός οργανισμού (*Single Sign – On*) και στη διεύρυνση αυτών των λύσεων και της διαχείρισης των ταυτοτήτων χρηστών εκτός των ορίων ενός μόνο οργανισμού, μέσα στα πλαίσια συνεργασιών πολλών οργανισμών (*Federated Identity Management*). Συμπληρωματικά όλων αυτών, παρουσιάζονται τα βασικά χαρακτηριστικά των συστημάτων Διαχείρισης Ταυτοτήτων και σημαντικών πρωτοκόλλων και

διαδικασιών των υπολοίπων υπο-συστημάτων τέτοιων συστημάτων, ώστε να καταδειχθούν οι τρόποι διεπαφής τους με τη φάση της αυθεντικοποίησης.

Όλα τα θέματα που αποτελούν το αντικείμενο της παρούσας εργασίας είναι άμεσα εφαρμόσιμα και συχνά οι εξελίξεις οδηγούνται από το χώρο των επιχειρήσεων ή των οργανισμών που τα απαιτούν για την αποδοτικότερη λειτουργία τους. Από όλο το φάσμα των εφαρμογών, στην παρούσα εργασία επιλέγεται η εξέταση και ανάλυση έργων ανάπτυξης συστημάτων αυθεντικοποίησης σε ηλεκτρονικές υπηρεσίες Δημοσίων Οργανισμών. Η συγκεκριμένη επιλογή έγινε με βάσει τις παραμέτρους:

- Η έννοια της ταυτότητας είναι πρωταρχικής σημασίας στις συναλλαγές πολιτών – κράτους και έχει υπόσταση που καθορίζεται από εκτεταμένο νομικό και θεσμικό πλαίσιο, ενώ η επιβεβαίωσή της με ηλεκτρονικές – δικτυακές διαδικασίες προσθέτει επιπλέον προβλήματα σε ένα σύστημα αυθεντικοποίησης.

- Η διαχείριση ταυτοτήτων των πολιτών – χρηστών διέπεται από κανόνες και επιλογές που δεν είναι αποκλειστικά τεχνολογικής προέλευσης, αλλά και νομικής ή ακόμα και Συνταγματικής.

- Σε καθαρά τεχνολογικό επίπεδο, οι διάφοροι Δημόσιοι οργανισμοί χρησιμοποιούν διαφορετικές ιδιότητες των πολιτών για τη μοναδική αναγνώρισή τους (πχ Α.Φ.Μ., Αρ. Μητρώου Ι.Κ.Α., Αριθ. Αστυνομικής Ταυτότητας κλπ) με αποτέλεσμα να υφίσταται πολύπλοκη ανομοιογένεια στις μεθόδους αυθεντικοποίησης που χρήζει αντιμετώπισης από μοντέρνες και αποδοτικές λύσεις ομογενοποίησής τους.

- Η ανάπτυξη ασφαλών και αποδοτικών ηλεκτρονικών υπηρεσιών στο Δημόσιο Τομέα (*e-Government*) συνεισφέρει στην παραγωγικότητα του Κράτους, στην καλύτερη εξυπηρέτηση των πολιτών άρα και στη βελτίωση της καθημερινότητάς τους.

Πριν την έναρξη εξέτασης των θεμάτων της παρούσας εργασίας στις επόμενες παραγράφους, είναι απαραίτητη η διευκρίνιση μερικών εννοιών και όρων. Οι ηλεκτρονικές υπηρεσίες που αναφέρονται στην παρούσα εργασία είναι οι εφαρμογές λογισμικού που διατίθενται μέσω του Internet ή ενός Intranet και υλοποιούνται βάσει των τεχνολογιών και των προτύπων του World Wide Web (*Web Applications*). Το ίδιο περιεχόμενο έχουν στο υπόλοιπο της εργασίας και οι αναφορές «δικτυακές ή διαδικτυακές εφαρμογές» ή «Internet υπηρεσίες» ή «Web εφαρμογές» ή «δικτυακές υπηρεσίες». Η συγκεκριμένη αποσαφήνιση αποσκοπεί στην απαλοιφή της σύγχυσης με την έννοια των αυτόνομων τμημάτων λογισμικού τα οποία εκτελούν ένα συγκεκριμένο έργο και επιστρέφουν μέσω ενός δικτύου συγκεκριμένα αποτελέσματα στη διεργασία που τα καλεί (*Web Services*). Σε οποιοδήποτε σημείο της εργασίας υπάρχει η ανάγκη αναφοράς στα συγκεκριμένα τμήματα λογισμικού θα χρησιμοποιείται διευκρινιστικά και ο όρος "*Web Service*". Επίσης, κατά τη μελέτη εφαρμογής των παρουσιαζόμενων θεωρητικών μοντέλων παρατίθενται παραδείγματα από το χώρο των εμπορικών επιχειρήσεων που διαθέτουν στο Internet υπηρεσίες Ηλεκτρονικού Εμπορίου (*e-Commerce*) και οργανισμών του Δημοσίου Τομέα που διαθέτουν στο Internet υπηρεσίες και διαδικασίες εξυπηρέτησης και ενημέρωσης των πολιτών (*e-Government*). Οι δύο συγκεκριμένοι χώροι μελετών περιπτώσεων αναφέρονται εν συντομία στην παρούσα εργασία ως «*εμπορική/επιχειρηματική*» και «*διοικητική*» εφαρμογή των θεωριών αυθεντικοποίησης, αντίστοιχα.

1.2 Σκοπός και Στόχοι της Εργασίας

Από την ανωτέρω παρουσίαση του βασικού περιβάλλοντος μέσα στο οποίο ανήκουν τα εξεταζόμενα στην παρούσα εργασία θέματα προκύπτει ότι ο κύριος σκοπός της εργασίας είναι η ανάδειξη του σύνθετου χαρακτήρα και της μεγάλης σημασίας που κατέχει η αυθεντικοποίηση χρηστών κατά την πρόσβασή τους σε δικτυακές υπηρεσίες που βασίζονται στις τεχνολογίες του Internet. Ο δευτερεύον σκοπός της εργασίας είναι η αξιολόγηση των υφιστάμενων εφαρμογών συστημάτων αυθεντικοποίησης σε Δημόσιους Οργανισμούς και η διατύπωση γενικής πρότασης περαιτέρω αξιοποίησής τους ειδικότερα στον Ελληνικό Δημόσιο Τομέα. Αναλυτικότερα, με την παρούσα εργασία επιδιώκεται:

- Να αναλυθεί η σημασία και η ανάγκη ασφαλούς αυθεντικοποίησης μέσω της εξέτασης των συστηματοποιημένων «απειλών» που έχουν καταγραφεί για την παραποίηση ή παραπλάνηση των διαδικασιών της.

- Να καταγραφεί η κατάσταση των τρεχουσών εξελίξεων στους μηχανισμούς αυθεντικοποίησης σε σχέση με την ενίσχυση της ασφάλειας και της αποτελεσματικότητάς τους μέσω της συγκεντρωτικής παρουσίασης πρωτοκόλλων και τεχνολογιών.

- Να υπογραμμιστούν τα σημεία όπου εντοπίζεται η πολυπλοκότητα των λύσεων αυθεντικοποίησης μέσω της συγκριτικής παρουσίασης των τρεχόντων τεχνολογικών λύσεων και τάσεων.

- Να καταδειχθεί η πρωτεύουσα θέση της αυθεντικοποίησης ανάμεσα στα υπόλοιπα υποσυστήματα διαχείρισης χρηστών μέσω της παρουσίασης των γενικών χαρακτηριστικών των συστημάτων Διαχείρισης Ταυτοτήτων στις ηλεκτρονικές υπηρεσίες.

- Να αναδειχθούν οι ιδιαιτερότητες των υπηρεσιών που διατίθενται στο Internet μέσω της παρουσίασης των απαιτήσεων που οδήγησαν στην ανάπτυξη συγκεκριμένων λύσεων και μηχανισμών αυθεντικοποίησης στο Internet, αλλά και των οφελών που προκύπτουν από την εφαρμογή τους.

- Να συγκεντρωθούν οι ιδιαίτερες απαιτήσεις των μηχανισμών αυθεντικοποίησης όταν εφαρμόζονται σε ηλεκτρονικές υπηρεσίες Δημοσίων Οργανισμών μέσω της συγκριτικής μελέτης τεχνολογικών χαρακτηριστικών και αποτελεσμάτων επιτυχημένων έργων διεθνών Κρατικών Φορέων.

- Να προταθούν τρόποι αξιοποίησης των συγκεκριμένων λύσεων και για τους Ελληνικούς Δημόσιους Φορείς μέσω της παρουσίασης της υπάρχουσας κατάστασης και της εκτίμησης εφαρμογής των επιτυχημένων παραδειγμάτων του εξωτερικού.

1.3 Δομή της Εργασίας

Η δομή της παρούσας εργασίας, προκειμένου να επιτευχθούν οι ανωτέρω στόχοι, διαμορφώνεται ως εξής:

- Η Ενότητα 2 περιλαμβάνει το κύριο τμήμα του θεωρητικού υπόβαθρου της εργασίας:
  - Στην υπο-ενότητα 2.1 παρουσιάζονται όλοι οι ορισμοί των κεντρικών εννοιών της εργασίας. Οι ορισμοί συνοδεύονται από αναλυτική καταγραφή των «απειλών» εναντίον της αυθεντικοποίησης και στη συνέχεια απαριθμούνται οι μηχανισμοί αντιμετώπισής τους. Στην παράγραφο 2.1.3 όπου αναλύονται οι τρόποι «προστασίας» της αυθεντικοποίησης γίνεται μία περαιτέρω ανάλυση των παραμέτρων της, των συσκευών που μπορούν να τη συνοδεύουν και των μεθόδων κρυπτογράφησης που χρησιμοποιούνται για την υψηλού βαθμού εξασφάλιση της εγκυρότητας της διαδικασίας.
  - Στην υπο-ενότητα 2.2 παρουσιάζονται τα γενικά χαρακτηριστικά των συστημάτων Διαχείρισης Ταυτοτήτων σε ένα σύστημα υπηρεσιών που διατίθενται στο Internet. Περιγράφονται τα γενικά υπο-συστήματά τους και οι μεταξύ τους συσχετίσεις. Επίσης, αναλύονται οι καινούριες έννοιες που υπεισέρχονται τα τελευταία χρόνια σε αυτά τα συστήματα: η έννοια της «*Έμπιστης Σχέσης*» ("*Trust*") και της δημιουργίας «*Ομοσπονδιών*» ("*Federations*") μεταξύ διαφορετικών οργανισμών στο επίπεδο των δεδομένων ταυτοτήτων των χρηστών τους.
  - Στην υπο-ενότητα 2.3 αναλύονται επιμέρους πρωτόκολλα που υλοποιούν ή σχετίζονται με την αυθεντικοποίηση. Συγκεκριμένα, στα πρωτόκολλα της διαδικασίας αυθεντικοποίησης παρουσιάζονται τα χαρακτηριστικά των: "*Kerberos*" (παρ. 2.3.1.1), "*Integrated Windows Authentication – IWA*" (παρ. 2.3.1.2), "*Security Assertion Markup Language – SAML*" (παρ. 2.3.1.3), "*Simple Authentication and Security Layer – SASL*" (παρ. 2.3.1.4). Στην κατηγορία των Ηλεκτρονικών Καταλόγων εξετάζονται δύο αντιπροσωπευτικές τεχνολογίες: το πρωτόκολλο "*Lightweight Directory Access Protocol – LDAP*" (παρ. 2.3.2.1) και το "*Active Directory*" του Microsoft Windows Server (παρ. 2.3.2.2).
  - Στην υπο-ενότητα 2.4 περιγράφονται οι λύσεις που υλοποιούν αυθεντικοποίηση με Single Sign – On και *Federated Identity Management*. Συγκεκριμένα, οι λύσεις SSO που αναλύονται είναι οι:"*CoSign - Open Source Web SSO*" (παρ. 2.4.1),"*CAS – Central Authentication Service*" (παρ. 2.4.2), "*WebAuth*" (παρ. 2.4.3) και "*Pubcookie*" (παρ. 2.4.4). Στη συνέχεια αναλύονται οι παράμετροι της προδιαγραφής *Identity Federation* "*WS-Federation*" μαζί με ένα προϊόν που την ενσωματώνει, τα "*Active Directory Federation Services – ADFS*" του Microsoft Windows Server 2003 (παρ. 2.4.5). Η παρουσίαση λύσεων ολοκληρώνεται με την εξέταση δύο δημοφιλών λύσεων *Identity Federation* που βασίζονται στη γλώσσα *SAML*, την προδιαγραφή "*Liberty Alliance - Identity Federation Framework*" (παρ. 2.4.6.1) και τη λύση "*Shibboleth*" (παρ. 2.4.6.2)
- Στην Ενότητα 3 διεξάγεται σύγκριση και αξιολόγηση των πρωτοκόλλων και λύσεων που παρουσιάστηκαν στην Ενότητα 2: των πρωτοκόλλων αυθεντικοποίησης (παρ. 3.1), των λύσεων SSO (παρ. 3.2.1) και των λύσεων *Federated Identity Management* (παρ. 3.2.2). Επιπροσθέτως, παρουσιάζονται τα γενικά χαρακτηριστικά των έργων αυθεντικοποίησης χρηστών σε Δημόσιους Οργανισμούς (παρ. 3.3.1) μαζί με τρεις αντιπροσωπευτικές περι-

πτώσεις σχετικών έργων: το "*E-Authentication*" των Η.Π.Α. (παρ. 3.3.2.1), το "*Government Gateway*" του Ηνωμένου Βασιλείου (παρ. 3.3.2.2) και το ερευνητικό έργο "*GUIDE*" που απευθύνεται στο χώρο της Ευρωπαϊκής Ένωσης (παρ. 3.3.2.3). Η Ενότητα ολοκληρώνεται με την παρουσίαση της υφιστάμενης κατάστασης στον Ελληνικό Δημόσιο Τομέα σχετικά με τα έργα e-Government γενικά και σχετικά με τις υποδομές εφαρμογής ενιαίας αυθεντικοποίησης σε ηλεκτρονικές υπηρεσίες των εθνικών Δημοσίων Οργανισμών (παρ. 3.3.3).

- Στις Ενότητες 4 και 5 παρουσιάζονται οι Προτάσεις και τα Συμπεράσματα που προκύπτουν από τις παρουσιάσεις και αναλύσεις των προηγούμενων Ενοτήτων με έμφαση στο πως θα μπορούσαν οι εθνικοί Δημόσιοι Οργανισμοί να αξιοποιήσουν τις παρουσιαζόμενες λύσεις και τη διεθνή εμπειρία.

- Στην Ενότητα 6 παρουσιάζονται οι αναφορές στις οποίες βασίζεται η παρούσα εργασία, ενώ στο Παράρτημα Α περιγράφονται συγκεκριμένες, διαδεδομένες έννοιες του λειτουργικού συστήματος Windows της Microsoft, ώστε να αποσαφηνιστούν τμήματα της περιγραφής του *Active Directory* των Windows.

2. ΘΕΩΡΗΤΙΚΟ ΥΠΟΒΑΘΡΟ

2.1 Αυθεντικοποίηση (*Authentication*) & Εξουσιοδότηση (*Authorization*) Χρηστών

2.1.1 Βασικοί Ορισμοί

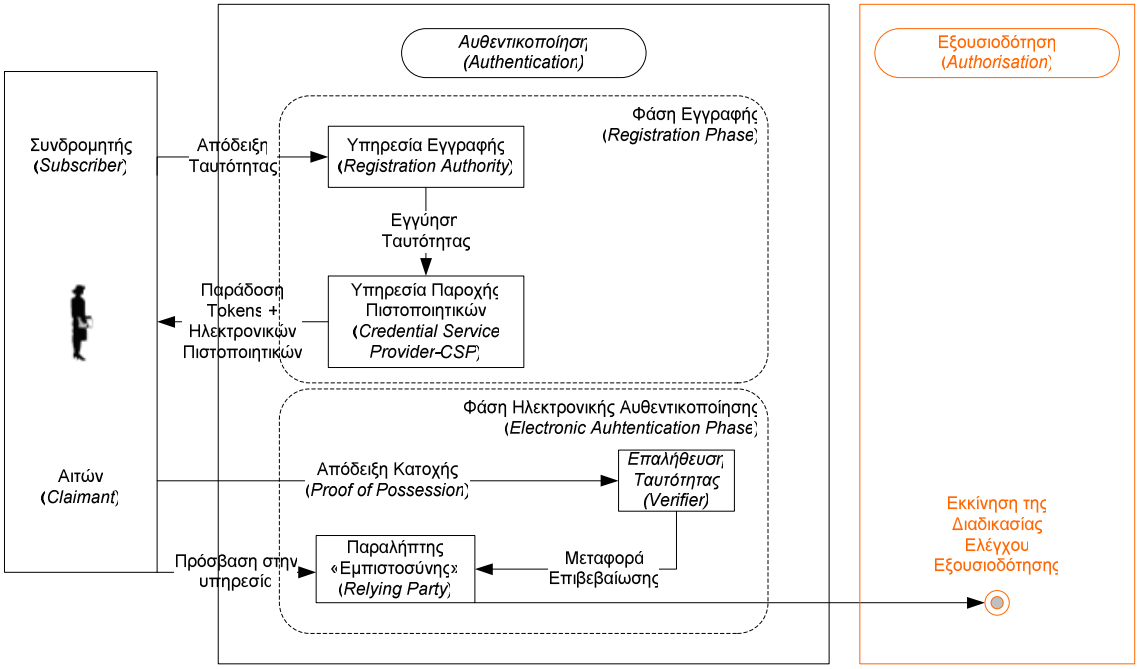
Η αυθεντικοποίηση (*Authentication*) είναι γενικά η διαδικασία απόδειξης της ταυτότητας μίας οντότητας (πρόσωπο – αντικείμενο) σε κάποιο άλλο. Η αυθεντικοποίηση συχνά συγχέεται με την ταυτοποίηση (*Identification*) η οποία συνίσταται στην επίδειξη «πιστοποιητικών» με τα οποία μπορεί να γίνει αναγνώριση ή εξακρίβωση της ταυτότητας κάποιου προσώπου – αντικειμένου. Η αυθεντικοποίηση περιλαμβάνει το στάδιο της ταυτοποίησης και ένα επιπλέον στάδιο, καθώς απαιτεί και την επιβεβαίωσης της αυθεντικότητας – εγκυρότητας των συγκεκριμένων «πιστοποιητικών», ώστε να εξασφαλιστεί ότι αυτός που τα επιδεικνύει είναι και ο πραγματικός («νόμιμος») κάτοχός τους [126]. Στην πραγματική ζωή οι δύο όροι «ταυτοποίηση» και «αυθεντικοποίηση» όντως επικαλύπτονται καθώς οι άνθρωποι «αυθεντικοποιούν» ο ένας τον άλλο με διάφορους τρόπους: με την αναγνώριση της φωνής ή του προσώπου και με πιο τυπικές μεθόδους όπως η επίδειξη ταυτότητας ή διαβατηρίου, στηριζόμενοι στην προσωπική τους εμπειρία και στην εγκυρότητα των Κρατικών Αρχών που εκδίδουν τα συγκεκριμένα «πιστοποιητικά» και έχουν αυτές προηγουμένως «αυθεντικοποιήσει» τον κάτοχό τους. Στην περίπτωση, όμως, της επικοινωνίας μέσω ενός δικτύου δεδομένων υπάρχει η απαίτηση για την επιβεβαίωση και όχι την απλή επίδειξη της «ταυτότητας» του ενός μέρους της επικοινωνίας από το δεύτερο συμμετέχοντα στο άλλο «άκρο» της επικοινωνίας. Η διαδικασία αυτή πρέπει να γίνει τη στιγμή που ξεκινάει η επικοινωνία μεταξύ των δύο μερών, οπότε και αναφερόμαστε σε αυθεντικοποίηση «ζωντανής επικοινωνίας», η οποία είναι διαφορετική από τη διαδικασία αυθεντικοποίησης ενός ηλεκτρονικού εγγράφου ή ενός ηλεκτρονικού μηνύματος η οποία δεν περιλαμβάνεται στο πεδίο μελέτης της παρούσας εργασίας και συνίσταται στην επιβεβαίωση της ταυτότητας του ισχυριζόμενου αποστολέα [64].
Κατά την εκτέλεση της αυθεντικοποίησης σε ένα δίκτυο δεδομένων τα συμμετέχοντα μέρη δεν μπορούν να στηριχθούν σε «βιομετρικές» πληροφορίες όπως η οπτική επαφή ή ο ήχος της φωνής. Στην πραγματικότητα, τα μέρη τα οποία πρέπει να αυθεντικοποιηθούν συχνά δεν είναι χρήστες, αλλά δικτυακές συσκευές (πχ routers) ή προγράμματα (πχ Web Services). Συνεπώς, η αναγνώριση της ταυτότητας πρέπει να στηριχθεί σε μηνύματα και δεδομένα τα οποία ανταλλάσσονται στα πλαίσια ενός *πρωτοκόλλου αυθεντικοποίησης*. Ως πρωτόκολλο αυθεντικοποίησης ορίζεται μία σαφώς καθορισμένη αλληλουχία μηνυμάτων μεταξύ ενός «αιτούντα» και ενός «ελεγκτή» με την οποία ο «ελεγκτής» μπορεί να επιβεβαιώσει ότι ο «αιτών» έχει στην κατοχή του ένα έγκυρο «πιστοποιητικό», για να προσδιορίσει την ταυτότητά του. Η ανταλλαγή των απαραίτητων μηνυμάτων μεταξύ του «αιτούντα» και του «ελεγκτή» η οποία καταλήγει στην αυθεντικοποίηση του χρήστη θεωρείται η εκτέλεση του πρωτοκόλλου [93]. Συνήθως, ένα πρωτόκολλο αυθεντικοποίησης εκτελείται πριν την εκτέλεση οποιουδήποτε άλλου πρωτοκόλλου ανταλλαγής πραγματικών δεδομένων (πχ ένα πρωτόκολλο αξιόπιστης μετάδοσης δεδομένων, ένα πρωτόκολλο ανταλλαγής πληροφοριών δρομολόγησης κλπ) [64].

Η Εξουσιοδότηση (*Authorization*) των χρηστών ενός πληροφοριακού συστήματος αφορά στη διαδικασία προσδιορισμού των δικαιωμάτων και προνομίων που διαθέτει ο καθένας χρήστης πάνω στους πόρους και υπηρεσίες του συστήματος, με βάση συγκεκριμένες χαρακτηριστικές ιδιότητες των χρηστών. Λαμβάνει χώρα εφόσον έχει επιτύχει η φάση της αυθεντικοποίησης

[86]. Συνήθως επιτυγχάνεται με τον καθορισμό ενός μικρού αριθμού «ρόλων» μέσα στο σύστημα, καθένας από τους οποίους έχει περιορισμένα και σαφή δικαιώματα πρόσβασης, και την απόδοση σε καθένα χρήστη του συστήματος του ρόλου που θα διαμορφώνει τα όρια της συμπεριφοράς του μέσα στο σύστημα [36]. Τα υπο-συστήματα που ελέγχουν και επιβεβαιώνουν την εξουσιοδότηση ενός χρήση για την εκτέλεση μίας λειτουργίας σε ένα Portal του Internet ή σε μία εφαρμογή Βάσεων Δεδομένων μπορεί να είναι αρκετά αναλυτικά ώστε να επιτρέπεται από συγκεκριμένους ρόλους χρηστών να έχουν πρόσβαση στην εκτέλεση μίας ενέργειας, χωρίς όμως αυτοί να έχουν πρόσβαση σε μεμονωμένες πληροφορίες που χαρακτηρίζονται ως «εμπιστευτικές». Μέσα από αυτά τα συστήματα εφαρμόζονται οι Πολιτικές Εξουσιοδότησης (*Authorization Policies*) των οργανισμών για το σύνολο των δεδομένων και υπηρεσιών τους [65].

Μία σχηματική αναπαράσταση της σχέσης των δύο λειτουργιών φαίνεται στην παρακάτω Εικόνα:

Πηγή: [128]



Εικόνα 1: Αυθεντικοποίηση και Εξουσιοδότηση

Ο χρήστης οφείλει να γίνει Συνδρομητής (*Subscriber*) στο σύστημα, οπότε αρχικά υποβάλει τα απαραίτητα αποδεικτικά της ταυτότητάς του (*Identity Proofing*) στο αρμόδιο υπο-σύστημα το οποίο, αφού τα ελέγξει, τον εγγράφει στην Υπηρεσία Καταλόγου του συστήματος (*Registration Authority*). Στη συνέχεια δίνεται το έναυσμα στο υπο-σύστημα *Credentials Service Provider – CSP* να δημιουργήσει τον απαραίτητο μηχανισμό – μέσο (*Token*) αυθεντικοποίησης για το νέο χρήστη και ενδεχομένως να το συνδέσει με κάποιο «Πιστοποιητικό» της εγκυρότητάς του, ανάλογα με τη μέθοδο και το επίπεδο αυθεντικοποίησης που εφαρμόζεται. Το *Token* μαζί με τα πιθανά «Πιστοποιητικά» παραδίδονται στο χρήστη. Η συγκεκριμένη φάση ονομάζεται *Registration Phase*. Ο χρήστης, έχοντας στην κατοχή του το *Token* της ταυτότητάς του, μπορεί να ζητήσει πρόσβαση (*Claimant*) σε ανάλογες Δικτυακές Εφαρμογές (*SA*) του συστήματος μέσω του υπο-συστήματος της Αυθεντικοποίησης. Αρχικά, πρέπει να απο-

δείξει την κατοχή του σωστού *Token* (*Proof of Possession*) στο αντίστοιχο τμήμα επιβεβαίωσης της ταυτότητας χρήστη (*Verifier*) το οποίο στη συνέχεια βεβαιώνει (*Assertion*) την ταυτότητα του χρήστη στο τμήμα που ελέγχει την πρόσβαση στη Δικτυακή Εφαρμογή. Από αυτό το σημείο και μετά ο χρήστης θεωρείται έγκυρος και αναλαμβάνει τον έλεγχό του το υποσύστημα της Εξουσιοδότησης, όπου εξετάζεται ποιες ενέργειες επιτρέπεται να υλοποιήσει ο συγκεκριμένος χρήστης.

2.1.2 «Απειλές» κατά της Αυθεντικοποίησης

Με βάση τον παραπάνω ορισμό η αυθεντικοποίηση θα μπορούσε να αντιμετωπιστεί ως μία απλή διαδικασία αποστολής και ελέγχου συγκεκριμένων κωδικών από το ένα μέρος μία δικτυακής επικοινωνίας, ώστε το άλλο μέρος να εξακριβώσει την ταυτότητα του «συνομιλητή» του. Το απλούστερο, επομένως, πρωτόκολλο αυθεντικοποίησης και ταυτόχρονα το πιο διαδεδομένο είναι η αποστολή ενός ονόματος χρήστη (κοινώς γνωστό ως "*username*") και ενός μυστικού κωδικού ("*password*") τα οποία παραλαμβάνει ο «ελεγκτής» και τα αναζητά σε κάποια δομή με στοιχεία χρηστών που αυτός διατηρεί, ώστε να εξακριβωθεί αν ο αποστολέας είναι ένας εγκεκριμένος - καταχωρημένος χρήστης. Το επόμενο βήμα από αυτή την εξακρίβωση είναι είτε η ανταλλαγή πιθανώς σημαντικών δεδομένων είτε η δυνατότητα πρόσβασης σε σημαντικές δικτυακές υπηρεσίες. Το γεγονός αυτό αποτελεί πρόκληση για την ανάπτυξη πολλών «απειλών» και παραπλανητικών μεθόδων με τις οποίες κάποιο «τρίτο μέρος» μπορεί να «εισβάλει» στην «απλή» διαδικασία της αυθεντικοποίησης και να αποκτήσει τα παραπάνω δικαιώματα προσποιούμενο το «νόμιμο» κάτοχό τους [64]:

- ***IP Address Spoofing:*** ένας συνήθης τρόπος αυθεντικοποίησης είναι ο έλεγχος από την πλευρά του «ελεγκτή» της δικτυακής διεύθυνσης (IP Address) του χρήστη. Στην περίπτωση που αυτή η διεύθυνση ανήκει σε μία λίστα «αποδεκτών» διευθύνσεων, αρχίζει η επικοινωνία των δύο μερών. Υπάρχει, όμως, μεγάλη πιθανότητα οι «αποδεκτές» διευθύνσεις να γίνουν γνωστές σε κάποιο «τρίτο μέρος» το οποίο έχει πρόσβαση στη συγκεκριμένη επικοινωνία και με τη δημιουργία κλήσεων οι οποίες να περιέχουν ως διεύθυνση αποστολέα κάποια «αποδεκτή» διεύθυνση (*IP Address Spoofing*) το «τρίτο μέρος» να γίνει αποδεκτός χρήστης από τη συγκεκριμένη, απλή διαδικασία αυθεντικοποίησης.

- ***Sniffing / Eavesdropping***: κατά την αποστολή από ένα χρήστη ενός username και password, ο παραλήπτης των κωδικών ελέγχει την ύπαρξή τους σε λίστες «αποδεκτών» κωδικών και σε περίπτωση επιτυχίας ο αρχικός αποστολέας θεωρείται «αυθεντικοποιημένος». Μέσα, όμως, σε ένα περιβάλλον τοπικού δικτύου (LAN) είναι εύκολο για έναν «τρίτο χρήστη» να «κρυφακούσει ηλεκτρονικά» (*Eavesdropping*) τους ηλεκτρονικούς κωδικούς του αρχικού χρήστη, ειδικά όταν αυτές οι πληροφορίες δεν μεταδίδονται με βάση κάποια κωδικοποίηση (πχ όπως στο διαδεδομένο πρωτόκολλο Telnet). Αυτό μπορεί εύκολα να συμβεί και με τη βοήθεια συγκεκριμένου λογισμικού το οποίο «ανιχνεύει» (*Sniff*) το δίκτυο και επομένως καταγράφει όλα τα πακέτα δεδομένων που κυκλοφορούν σε ένα τοπικό δίκτυο. Μετά από αυτό το βήμα είναι εύκολο για τον «τρίτο χρήστη» να χρησιμοποιήσει τους κωδικούς του «νόμιμου» χρήστη και να ξεπεράσει τη διαδικασία αυθεντικοποίησης.

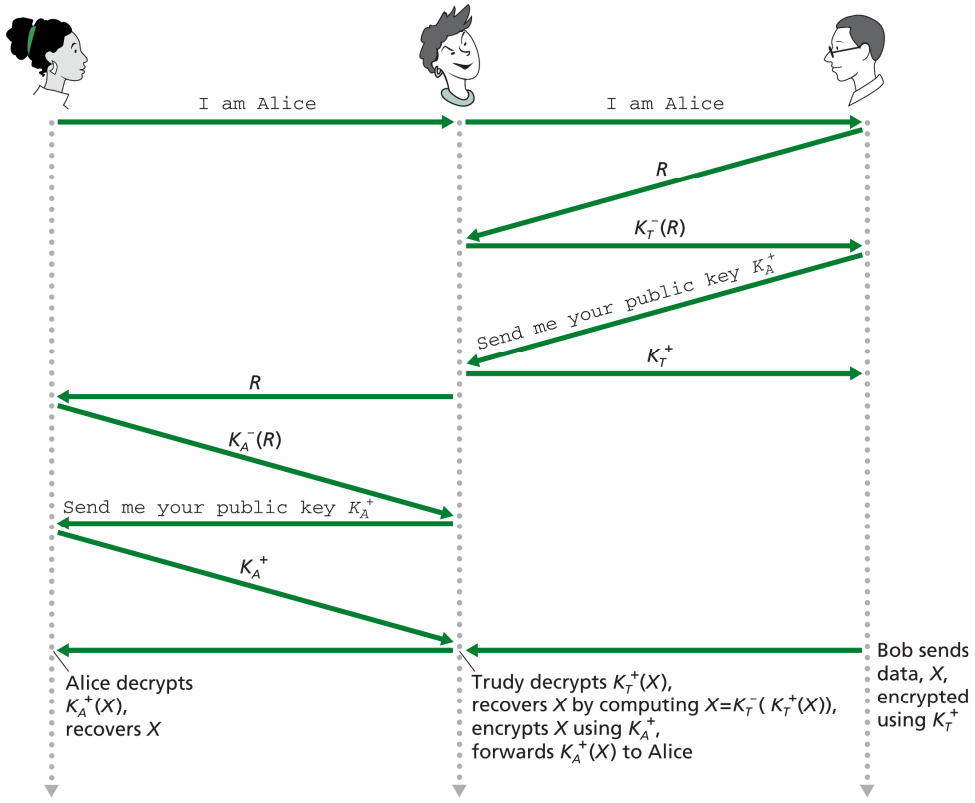
- ***Playback Attack***: η προηγούμενη «απειλή» *Sniffing / Eavesdropping* θα μπορούσε να αποφευχθεί με την αποστολή κωδικοποιημένων προσωπικών πληροφοριών κατά τη διαδι-

κασία της αυθεντικοποίησης. Τα δύο «νόμιμα» μέρη μίας επικοινωνίας, δηλαδή, θα μπορούσαν να συμφωνήσουν σε μία κοινή κωδικοποίηση των προσωπικών πληροφοριών αυθεντικοποίησης με βάση την οποία θα μεταδίδονται οι συγκεκριμένες πληροφορίες στο δίκτυο, ώστε ακόμα και αν «υποκλαπούν» από κάποιον «τρίτο χρήστη» να μην είναι σε «αναγνωρίσιμη» μορφή. Είναι δυνατό όμως ο συγκεκριμένος «τρίτος χρήστης» να «καταγράψει» τις κρυπτογραφημένες πληροφορίες και να τις προωθήσει αναπαράγοντάς τες κρυπτογραφημένες όπως κατεγράφησαν (*Playback Attack*). Ο παραλήπτης της κλήσης επικοινωνίας λαμβάνει τις αναπαραγόμενες, κρυπτογραφημένες πληροφορίες, τις αποκωδικοποιεί με την κοινώς συμφωνημένη διαδικασία και αυθεντικοποιεί εσφαλμένα και τον «τρίτο χρήστη» – «εισβολέα».

- ***Man – in – the – Middle Attack***: μία πιθανή επέκταση του παραπάνω «σεναρίου» μπορεί να έχει περισσότερο καταστροφικές συνέπειες. Στην περίπτωση του *Playback Attack* τα δύο «νόμιμα» μέρη της συνδιάλεξης θα έχουν την εντύπωση ότι επικοινώνησαν, ενώ στην πραγματικότητα ήταν ο «τρίτος χρήστης» που υποδύθηκε το ένα μέρος αναπαράγοντας τους προσωπικούς του κωδικούς. Στην περίπτωση αυτή μπορούν να συνειδητοποιήσουν ότι συνέβη κάποια δολιοφθορά και να ενισχύσουν την ασφάλεια της επικοινωνίας τους. Υπάρχει όμως η χειρότερη πιθανότητα όπου ο «τρίτος χρήστης» έχει τη δυνατότητα εμβόλιμης παρουσίας στη συνδιάλεξη των δύο «νόμιμων» χρηστών και αναπαραγωγής δεδομένων αυθεντικοποίησης προς αυτούς, γι αυτό και ονομάζεται *Man – in – the – Middle Attack*. Η συγκεκριμένη «απειλή» μπορεί να εμφανιστεί σε περιπτώσεις όπου εφαρμόζεται η κρυπτογράφηση Δημοσίου Κλειδιού[i] και η αυθεντικοποίηση επιτυγχάνεται με τη δοκιμαστική κρυπτογράφηση και αποκρυπτογράφηση μίας τυχαίας τιμής (*nonce*). Για παράδειγμα (βλ. παρακάτω Εικόνα) η διαδικασία αυθεντικοποίησης είναι η εξής: η Alice ζητάει επικοινωνία από τον Bob, αυτός της επιστρέφει ένα *nonce* (R) και αυτή το κρυπτογραφεί με το ιδιωτικό της κλειδί K_A^-: [K_A^-(R)]. Ο Bob στη συνέχεια της ζητάει και το δημόσιο κλειδί της K_A^+ (ή το βρίσκει από το Internet) και εφαρμόζοντάς το στην προηγούμενη κρυπτογραφημένη ποσότητα έχει ως αποτέλεσμα το αρχικό *nonce* [ισχύει R = K_A^+(K_A^-(R))]. Η «απειλή» προκύπτει αν στην προηγούμενη συνδιάλεξη μεσολαβήσει η Trudy και είναι ικανή να επικοινωνεί με την Alice «υποδυόμενη» τον Bob, αλλά και με τον Bob «υποδυόμενη» την Alice.

[i] Κρυπτογράφηση Δημοσίου Κλειδιού (*Public Key Cryptography*): διαδικασία κρυπτογραφημένης επικοινωνίας δύο μερών με τη χρήση δύο κλειδιών κρυπτογράφησης, ενός δημοσίου K^+ το οποίο είναι γνωστό και ενός ιδιωτικού K^- το οποίο είναι αυστηρά προσωπικό στο καθένα μέρος. Τα κλειδιά και οι αλγόριθμοι κρυπτογράφησης επιλέγονται έτσι ώστε να έχουν την ιδιότητα:
$K^-(K^+(m)) = m = K^+(K^-(m))$ όπου m = το αρχικό μήνυμα χωρίς κρυπτογράφηση.
Η άλλη μορφή κρυπτογράφησης είναι αυτή του Συμμετρικού Κλειδιού (*Symmetric Key Cryptography*) όπου και τα δύο μέρη της επικοινωνίας χρησιμοποιούν ένα μοναδικό, αμοιβαία γνωστό κλειδί για την κρυπτογράφηση – αποκρυπτογράφηση του αρχικού μηνύματος [64].

Πηγή: [64]



Εικόνα 2: Σχηματική Αναπαράσταση του *Man – in – the – Middle Attack*

- ***Password Cracking***: η συγκεκριμένη απειλή αφορά ένα σύνολο «επιθέσεων» στη διαδικασία αυθεντικοποίησης οι οποίες αποσκοπούν στην ανεύρεση του (των) password(s) των χρηστών. Προϋπόθεση αποτελεί η γνώση των usernames και η δυνατότητα εισχώρησης του «εισβολέα» στο δίκτυο όπου αποστέλλονται οι συγκεκριμένοι κωδικοί. Ένα πρώτο είδος επίθεσης είναι το "***Password Guessing***" όπου με αυτοματοποιημένες μεθόδους γίνονται όσες προσπάθειες είναι δυνατές από το χρόνο και την υπολογιστική ικανότητα του «εισβολέα» να αποστείλει εναλλακτικούς συνδυασμούς passwords. Στην αρχή δοκιμάζεται ένα σύνολο από προφανή ή συνηθισμένα passwords και η συνέχεια ποικίλει ανάλογα με τις δυνατότητες του «εισβολέα» μέχρι την απόπειρα εισαγωγής όλων των πιθανών συνδυασμών χαρακτήρων. Η συγκεκριμένη ύστατη λύση ονομάζεται "***Brute Force Attack***". Μία πιο «εκλεπτυσμένη» παραλλαγή της παραπάνω «απειλής» αποτελεί η "***Dictionary Attack***" κατά την οποία ο «εισβολέας» δοκιμάζει πολλούς συνδυασμούς πιθανών passwords οι οποίοι βασίζονται σε παρατηρημένες τεχνικές και συνήθειες των χρηστών κατά την επιλογή των passwords τους. Συνηθίζεται, δηλαδή, πολλοί χρήστες να αντικαθιστούν συγκεκριμένα γράμματα με αριθμούς ή σύμβολα (πχ το "Ε" με το "3", το "α" με το "@" κοκ) ή να προσθέτουν αριθμούς στο τέλος ονομάτων κλπ. Η «απειλή» επομένως περιλαμβάνει την δοκιμή βασικών λέξεων οι οποίες αναπροσαρμόζονται με βάση τις παραπάνω μεθόδους και ξαναδοκιμάζονται, ώστε το σύνολο όλων των σχηματιζόμενων λέξεων να συμπληρώνει ένα ολόκληρο «λεξικό» (*Dictionary*) [87].

Η επιτυχία των παραπάνω «απειλών» εξαρτάται από τη λεγόμενη «Εντροπία» των επιλεγμένων passwords. Οι λέξεις - κωδικοί, δηλαδή, θα πρέπει να είναι κατάλληλα επιλεγμένες ώστε να είναι όσο το δυνατό μοναδικές και δύσκολες στην αναπαραγωγή. Ένα μέτρο της δυσκολίας που μπορεί να συναντήσει ένας «εισβολέας» για να «μαντέψει» ένα password είναι η «Εντροπία» του, η οποία μετριέται σε bits. Ο όρος «Εντροπία» εισήχθη στην επιστήμη των πληροφοριών από τον Claude Shannon [125] και χρησιμοποιήθηκε από την επιστήμη της κρυπτογραφίας ως ένα μέτρο της δυσκολίας εικασίας ή προσδιορισμού ενός password [93]. Μία ακόμα «απειλή» κατά των passwords αποτελεί και η «επίθεση» κατά της δομής ή Βάσης Δεδομένων στην οποία διατηρούνται μέσα σε ένα πληροφοριακό σύστημα, η οποία όμως συνιστά ευρύτερο πρόβλημα ασφάλειας συστημάτων και όχι μεμονωμένος κίνδυνος της αυθεντικοποίησης [87].

- Υπάρχουν πολλές άλλες γενικές «απειλές» των δικτυακών επικοινωνιών, αλλά αυτή που μπορεί να συσχετιστεί έμμεσα με τη διαδικασία αυθεντικοποίησης είναι το ***Phishing***. Η υλοποίηση γίνεται με πολλούς τρόπους παραπλάνησης των λιγότερο έμπειρων χρηστών του Internet, κυρίως με τη μαζική αποστολή e-mail μηνυμάτων στα οποία ο χρήστης καλείται να ακολουθήσει μία δικτυακή διεύθυνση ώστε να καταχωρήσει τα προσωπικά του στοιχεία, για να αυθεντικοποιηθεί σε μία υποτιθέμενη υπηρεσία (πχ Τράπεζες, e-Shop υπηρεσίες κλπ). Η συγκεκριμένη διεύθυνση, όμως, δεν αντιστοιχεί στην πραγματική φόρμα αυθεντικοποίησης αλλά σε μία ελεγχόμενη φόρμα, όπου τα στοιχεία που καταχωρεί ο χρήστης χρησιμοποιούνται για δολιοφθορές. Το ίδιο μπορεί να συμβεί με τη χρησιμοποίηση παραπλήσιων διευθύνσεων με αυτές δημοφιλών Web Sites, άρα λόγω κάποιας πιθανώς λανθασμένης πληκτρολόγησης της επιθυμητής διεύθυνσης ο χρήστης βρίσκεται στην ελεγχόμενη φόρμα και απρόσεχτα καταχωρεί τα στοιχεία του [151]. Από την πλευρά της διαδικασίας αυθεντικοποίησης, η συγκεκριμένη «απειλή» χαρακτηρίζεται ως «*πλαστοπροσωπία του ελεγκτή*» ("*Verifier Impersonation*") και περιλαμβάνει γενικώς τις τεχνικές όπου ο χρήστης θεωρεί ότι ο «συνομιλητής» του είναι ο σωστός και εισάγει τους κωδικούς του προς επιβεβαίωση, οι οποίοι φυσικά και υποκλέπτονται.

Τα πρωτόκολλα αυθεντικοποίησης επιδιώκουν την επίτευξη της ορθής επιβεβαίωσης της ταυτότητας των χρηστών ξεπερνώντας τις πιθανές «απειλές». Πέρα από τις μεθόδους που εισάγει κάθε πρωτόκολλο υπάρχουν κάποιες γενικές αρχές – συστάσεις αντιμετώπισης των «απειλών» της αυθεντικοποίησης [93]:

- Για την αντιμετώπιση του "*Eavesdropping*" ένα πρωτόκολλο αυθεντικοποίησης πρέπει να καθιστά «μη – πρακτική» την αξιοποίηση όσων πληροφοριών μπορεί να υποκλέψει ένας πιθανός, «παθητικός εισβολέας» κατά την ανταλλαγή κωδικών αυθεντικοποίησης. «Μη – πρακτική» αξιοποίηση σημαίνει ότι ο «εισβολέας» έχει πάντα μη μηδενικές πιθανότητες επιτυχίας, αλλά η περαιτέρω επεξεργασία των πληροφοριών που υπεκλάπησαν απαιτεί πολύ μεγάλη προσπάθεια (τάξης μεγέθους τουλάχιστον 2^{80} κρυπτογραφικές πράξεις) ώστε να προκύψουν οι πραγματικοί κωδικοί.

- Στην περίπτωση του "*Man – in – the – Middle Attack*", το πρωτόκολλο αυθεντικοποίησης μπορεί να απαιτήσει την αμοιβαία αυθεντικοποίηση των δύο μερών της συνομιλίας με τρόπο τέτοιο ώστε να εμποδίζεται η μη ανιχνεύσιμη, εμβόλιμη συμμετοχή ενός «εισβολέα» στη συνομιλία.

- Στην περίπτωση του "*Password Guessing*", ένας εύκολος τρόπος αντιμετώπισης είναι ο περιορισμός του πλήθους διαδοχικών προσπαθειών εισαγωγής των passwords σε ένα πο-

λύ μικρό αριθμό σε σχέση με όλους τους δυνατούς συνδυασμούς των passwords με περαιτέρω «κλείδωμα» του λογαριασμού στην περίπτωση όπου συμβούν τόσες αποτυχημένες απόπειρες σύνδεσης όσες και το ανώτερο επιτρεπτό όριο. Επίσης, είναι δυνατή η επιβολή χρήσης μόνο passwords με μεγάλη «Εντροπία» από τη μεριά του συστήματος διαχείρισης των χρηστών (συγκεκριμένο μεγάλο μήκος, υποχρεωτική χρήση συνδυασμού γραμμάτων, αριθμών και συμβόλων κ.α.). Επιπροσθέτως, μία ακόμα επιλογή ασφαλείας είναι η επιβολή της αλλαγής των passwords σε τακτά χρονικά διαστήματα, έτσι ώστε ακόμα και αν έχουν υποκλαπεί τα παλαιότερα να μην μπορούν να χρησιμοποιηθούν [87].

2.1.3 Αντιμετώπιση «Απειλών» - Τεχνολογίες Αυθεντικοποίησης

Όλες οι παραπάνω «απειλές» αποτελούν ευρύτερες κατηγοριοποιήσεις πιθανών επιθέσεων στην απλή διαδικασία αυθεντικοποίησης με την εισαγωγή username και password. Είναι, επομένως, προφανές ότι η διαδικασία της αυθεντικοποίησης πρέπει να είναι πιο πολύπλοκη, περιλαμβάνοντας περισσότερους από έναν παράγοντες (factors) επιβεβαίωσης της ταυτότητας ενός χρήστη. Οι θεμελιώδεις παράγοντες που μπορούν να ενσωματωθούν σε ένα σύστημα αυθεντικοποίησης είναι [93]:

1. Κάτι που ο χρήστης ***γνωρίζει*** (πχ ένα password)

2. Κάτι που ο χρήστης ***κατέχει*** (πχ ένα σήμα ταυτότητας ή ένα κλειδί κρυπτογράφησης σε μία ηλεκτρονική συσκευή κλπ)

3. Κάτι που ο χρήστης ***είναι*** (πχ ένα δακτυλικό αποτύπωμα, ένα καταγεγραμμένο ηχητικό μήνυμα κλπ)

Η κατηγοριοποίηση των μεθόδων αυθεντικοποίησης γίνεται ανάλογα με το πλήθος των παραγόντων που συνδυάζουν για την επιβεβαίωση της ταυτότητας των χρηστών και ο κανόνας είναι ότι η ταυτόχρονη εφαρμογή πολλών παραγόντων (factors) εξασφαλίζει «ισχυρότερη» αυθεντικοποίηση. Είναι προφανές ότι ένα σύστημα που απαιτεί για την επιβεβαίωση της ταυτότητας ενός χρήστη την επίδειξη τόσο μίας πληροφορίας που αυτός γνωρίζει όσο και του ηλεκτρονικού περιεχομένου που μπορεί να υπάρχει σε μία συγκεκριμένη συσκευή παρέχει μεγαλύτερη ασφάλεια, καθώς η πιθανή υποκλοπή της πληροφορίας του χρήστη δεν είναι ικανή να απειλήσει το σύστημα αν δε συνοδευτεί και από τη φυσική κλοπή της επιπρόσθετης συσκευής. Η συνήθης εφαρμογή «ισχυρών» συστημάτων αυθεντικοποίησης περιλαμβάνει τον έλεγχο δύο παραγόντων («γνωρίζει» & «κατέχει») γι αυτό και ονομάζεται «ισχυρή» (*strong*) ή *two – factor authentication*.

Η περίπτωση της χρήσης ενός απλού κωδικού (πχ password) είναι η πιο διαδεδομένη και απλή, αλλά, πέρα από τις παραπάνω πολλές «απειλές» που μπορεί να δεχθεί χαρακτηρίζεται από επιπρόσθετα μειονεκτήματα [128]:

- Σύμφωνα με την παραπάνω «θεμελιώδη» κατηγοριοποίηση βρίσκονται στο κατώτερο επίπεδο ασφάλειας της διαδικασίας αυθεντικοποίησης (*one – factor authentication*).

- Τα εργαλεία που υλοποιούν τις παραπάνω «απειλές» αυξάνουν σε αριθμό και σε πολυπλοκότητα.

- Η αποδοτικότητα των passwords επαφίεται στην υπευθυνότητα και προσοχή των χρηστών ως προς την επιλογή τους, την ασφαλή τήρηση και προστασία τους.

- Υπάρχουν πολλές εφαρμογές με ενδεχομένως διαφορετικά passwords με αποτέλεσμα τη σύγχυσή τους ή αντίθετα τη χρήση ενός μόνο password για όλες τις χρήσεις με δραματικές επιπτώσεις στην ασφάλεια όλου του συστήματος αυθεντικοποίησης.

Τα συστήματα αυθεντικοποίησης δεν αναφέρονται πια στην απλή έννοια των passwords αλλά στην έννοια των *Tokens*, τα οποία αποτελούν οποιοδήποτε μηχανισμό έχει στη διάθεσή του ένας χρήστης προκειμένου να αποδείξει την ταυτότητά του κατά τη διάρκεια της αυθεντικοποίησης. Τα *Tokens* αφορούν εναλλακτικές χρήσεις ηλεκτρονικής αυθεντικοποίησης, η οποία λαμβάνει χώρα μέσω ενός δικτύου δεδομένων και με την εισαγωγή από την πλευρά του χρήστη κάποιας μορφής ηλεκτρονικής πληροφορίας ταυτότητας. Μία κατηγοριοποίηση των *Tokens* ηλεκτρονικής αυθεντικοποίησης είναι [93, 128]:

1. *Password* ή *PIN Token*: Μία απλή, μοναδική ακολουθία χαρακτήρων την οποία απομνημονεύει και πληκτρολογεί ένας χρήστης, για να επιβεβαιώσει την ταυτότητά του.

2. *One – Time Password* (*OTP*) *Token*: Μία μυστική ακολουθία χαρακτήρων η οποία όμως παράγεται αυτόματα από μία συσκευή και μπορεί να χρησιμοποιηθεί μόνο μία φορά σε διαδικασία αυθεντικοποίησης. Ο μοναδικός μυστικός κωδικός παράγεται με κρυπτογραφικούς αλγορίθμους λαμβάνοντας υπ' όψιν κάποια τυχαία τιμή (πχ την ώρα ή την ημερομηνία), ένα προσωπικό κλειδί που βρίσκεται μέσα σε καθεμιά συσκευή και ενδεχομένως έναν μυστικό αριθμό που γνωρίζει ο χρήστης (PIN) και εισάγει μέσω πλήκτρων της συσκευής. Υπάρχουν περιπτώσεις *Tokens* όπου έχουν κάποια διεπαφή για Ηλ. Υπολογιστή (πχ σε Universal Serial Bus - USB θύρα) και με αυτό τον τρόπο μπορούν να δεχθούν κάποιο κλειδί για τον αλγόριθμο της παραγωγής του μοναδικού password. Η μοναδικότητα του τελικού password ενισχύεται με την προσθήκη στο σχηματιζόμενο αριθμό ενός μοναδικού για καθένα χρήστη κωδικού αριθμού (PIN). Το τελικό password εμφανίζεται σε ειδική οθόνη της συσκευής και το πληκτρολογεί ο χρήστης ή μπορεί να εισαχθεί αυτόματα από τη συσκευή αν αυτή διαθέτει διεπαφή για Ηλ. Υπολογιστή. Τα εμπορικά προϊόντα που υλοποιούν τη συγκεκριμένη λειτουργικότητα παρουσιάζουν πολλές παραλλαγές ή ευκολίες οι οποίες καθορίζουν και την κατηγοριοποίηση του είδους αυθεντικοποίησης που προσφέρουν. Συνεπώς, τα *OTP* τα οποία απλώς παράγουν ένα τυχαίο password ανήκουν στην κατηγορία της αυθεντικοποίησης «ενός – παράγοντα» (*one – factor authentication*), ενώ όσα *OTP* απαιτούν την εισαγωγή από το χρήστη του προσωπικού του PIN εξασφαλίζουν «ισχυρότερη» αυθεντικοποίηση (*two – factor authentication*) καθώς συνδυάζουν «κάτι που ο χρήστης γνωρίζει» (PIN) με «κάτι που ο χρήστης κατέχει» (το *OTP Token*), ώστε να επιτευχθεί αυθεντικοποίηση. Η μεμονωμένη χρήση καθενός στοιχείου (PIN & *OTP Token*) χωρίς το συνδυασμό του με το άλλο δεν μπορεί να έχει αποτέλεσμα.

Πηγή: [123, 149]

Εικόνα 3: Ενδεικτικές Συσκευές *One – Time Password Tokens*

3. *Soft Cryptographic Token*: Ένα κλειδί κρυπτογράφησης το οποίο είναι αποθηκευμένο σε κάποιο δίσκο ή σε άλλο ηλεκτρονικό μέσο. Η αυθεντικοποίηση υλοποιείται μόλις ο χρήστης επιδείξει την κατοχή και έλεγχο του συγκεκριμένου κλειδιού. Το *Soft Crypto Token* είναι προστατευμένο με κάποιας μορφής κρυπτογράφηση η οποία βασίζεται σε κωδική πληροφορία (πχ ένα password) την οποία γνωρίζει μόνο ο χρήστης. Συνεπώς, ο χρήστης αποκρυπτογραφεί το κλειδί με το password του και στη συνέχεια το κλειδί παρουσιάζεται στο σύστημα αυθεντικοποίησης ως απόδειξη της ταυτότητάς του. Για καθεμιά διαδικασία αυθεντικοποίησης ο χρήστης υποχρεούται να εισάγει τον προσωπικό του κωδικό και το αποκρυπτογραφημένο κλειδί καταστρέφεται μετά την ολοκλήρωση της διαδικασίας. Τα *Soft Crypto Tokens* μπορεί να είναι αποθηκευμένα στο σκληρό δίσκο του Ηλ. Υπολογιστή ενός χρήστη ή να υπάρχουν στο Server ενός Πληροφ. Συστήματος και να τα προσπελαύνει ο χρήστης με συγκεκριμένη ασφαλή διαδικασία.

4. *Hard Cryptographic Token*: Μία ηλεκτρονική συσκευή η οποία περιέχει ένα κλειδί κρυπτογράφησης. Η αυθεντικοποίηση επιτυγχάνεται με την απόδειξη από την πλευρά του χρήστη της κατοχής της συσκευής και του ελέγχου του κλειδιού. Η ενεργοποίηση της συσκευής ελέγχεται από προσωπικό, μυστικό κωδικό (PIN) που απομνημονεύει ο χρήστης ή από κάποιο βιομετρικό χαρακτηριστικό του χρήστη (πχ δακτυλικό αποτύπωμα). Οι συγκεκριμένες συσκευές μπορεί να είναι οι λεγόμενες «έξυπνες κάρτες» ("*Smart Cards*") ή η νεότερη εκδοχή τους, τα "*USB Tokens*" τα οποία παρέχουν τις λειτουργίες μία «έξυπνης κάρτας» και διαθέτουν τη διαδεδομένη διεπαφή σύνδεσης στον Ηλ. Υπολογιστή USB.

Πηγή: [2, 123, 149]

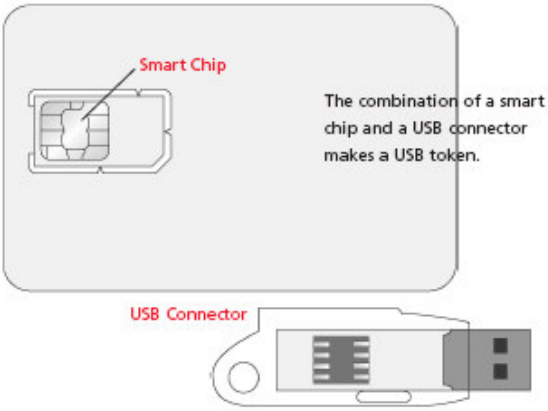
Εικόνα 4: Ενδεικτικές Συσκευές *Hard Crypto Tokens*

Οι εμπορικές εταιρίες συνεχώς παράγουν νέα προϊόντα αποθήκευσης πληροφοριών κρυπτογράφησης τα οποία μπορούν να χρησιμοποιηθούν σε συστήματα "*two – factor*" αυθεντικοποίησης, ταυτόχρονα με εξελιγμένα πακέτα λογισμικού τα οποία διευκολύνουν τη διαχείριση των συσκευών και την ενσωμάτωσή τους σε διαδεδομένα Λειτουργικά Συστήματα (πχ Windows και το Active Directory) [152]. Η εμπορική ανάπτυξη των συγκεκριμένων συσκευών αυθεντικοποίησης έχει οδηγήσει στην ανάπτυξη πολλών διαφορετικών τεχνολογιών και προτύπων τα οποία πολλές φορές δεν είναι συμβατά μεταξύ τους (*Proprietary Standards*). Μία προσπάθεια καθορισμού ενιαίων, ανοιχτών προτύπων συσκευών «ισχυρής» αυθεντικοποίησης είναι η συνολική πρόταση «ισχυρής» αυθεντικοποίησης χρηστών και συσκευών από τον οργανισμό "*OATH – Initiative for Open Authentication*". Ο *OATH* αποτελείται από εταιρίες παραγωγής προϊόντων και λογισμικού ασφαλείας (ενδεικτικά: VeriSign, SanDisk, Entrust, IBM – Tivoli κλπ) και αποσκοπεί στη διαμόρφωση ενιαίων, ανοιχτών προτύπων για «ισχυρή» αυθεντικοποίηση για οποιαδήποτε χρήση σύνδεσης χρηστών σε Εφαρμογές Ηλ. Υπολογιστών (εφαρμογές e-Commerce, δίκτυα VPN, ERP/CRM Πληρ. Συστήματα κλπ) [107].

Μεταξύ των *Hard Crypto Tokens* συσκευών οι Smart Cards είναι από τις πιο δημοφιλείς μαζί με τα USB Tokens. Με τον όρο "*Smart Card*" περιγράφεται ένα ευρύ σύνολο καρτών οι οποίες περιέχουν κάποιας μορφής ηλεκτρονική πληροφορία: Κάρτες Μαγνητικής Ταινίας (*Magnetic Stripe Cards* – οι γνωστές τραπεζικές Κάρτες), Οπτικές Κάρτες (*Optical Cards*), Κάρτες Αποθήκευσης Δεδομένων (*Memory Cards*), Κάρτες Μικροεπεξεργαστή (*Microprocessor Cards*) με ενσωματωμένο κύκλωμα ή chip το οποίο εκτός από αποθήκευση μπορεί να επεξεργάζεται δεδομένα και οι οποίες μπορούν να επικοινωνούν με τη συσκευή ανάγνωσης είτε άμεσα (*Contact Cards*) είτε από απόσταση με ραδιο-σήματα (*Contactless Cards*). Οι κάρτες που αναφέρονται στην παρούσα εργασία για χρήση στην αυθεντικοποίηση είναι οι *Microprocessor Cards* στις οποίες μπορούν να υλοποιηθούν πολύπλοκες πράξεις κρυπτογράφησης [142]. Τα USB Tokens αποτελούν την ενσωμάτωση του «έξυπνου» chip μίας Smart Card σε μία συσκευή με τη διαδεδομένη διεπαφή USB. Οι λειτουργικές τους δυνατότητες είναι ίδιες, ενώ διαφέρουν μόνο στο βαθμό ευχρηστίας τους, καθώς οι θύρες USB είναι συχνότερες στους σύγχρονους Ηλ. Υπολογιστές από τις συσκευές ανάγνωσης έξυπνων καρτών (*Smart Card Readers*) [118]. Τα πλεονεκτήματα των συγκεκριμένων συσκευών είναι [118, 142]:

- Διαθέτουν δυνατότητες αποθήκευσης πολλών πιστοποιητικών ασφαλείας και άλλων προσωπικών πληροφοριών των χρηστών (χωρητικότητα μέχρι 32Kb)
- Δεν μπορούν εύκολα να παραχαραχθούν ή αλλοιωθούν, ενώ ακόμα και σε περίπτωση απώλειας ή κλοπής προστατεύονται από το προσωπικό PIN του χρήστη.
- Είναι εύκολες στη χρήση και οικείες στους χρήστες καθώς παρόμοιες συσκευές χρησιμοποιούνται και σε άλλες ανάγκες της καθημερινότητας.
- Μπορούν να λειτουργήσουν με μεγάλη ποικιλία εφαρμογών και πρωτοκόλλων καθώς αυξάνει η διάδοσή τους στα συστήματα αυθεντικοποίησης.
- Η δυνατότητα αυθεντικοποίησης γίνεται μία «φορητή» διαδικασία καθώς τα απαραίτητα «πιστοποιητικά» των χρηστών μπορούν να μεταφέρονται μέσα στις συγκεκριμένες συσκευές.

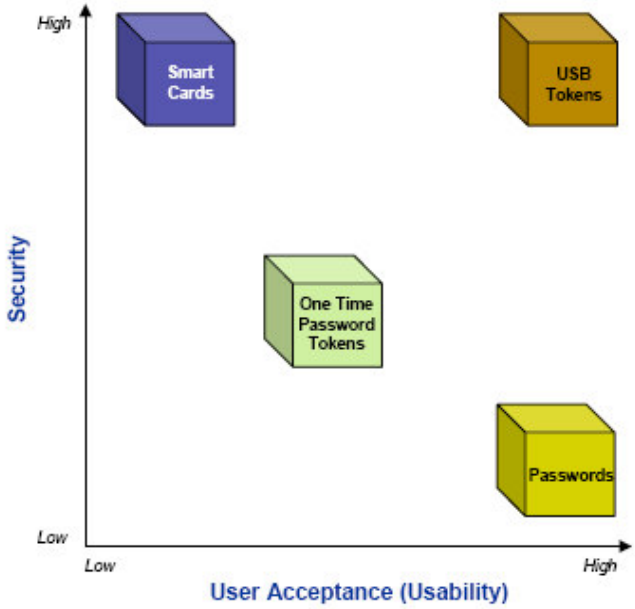
Πηγή: [118]



Εικόνα 5: Smart Card και USB Token

Μία προσεγγιστική σύγκριση των παραπάνω κατηγοριών *Tokens* σε σχέση με την ευκολία χρήσης τους (*Usability*) και την ασφάλεια (*Security*) που παρέχουν φαίνεται στο παρακάτω διάγραμμα:

Πηγή: [63]



Εικόνα 6: Σύγκριση κατά Προσέγγιση Διαφορετικών *Authentication Tokens*

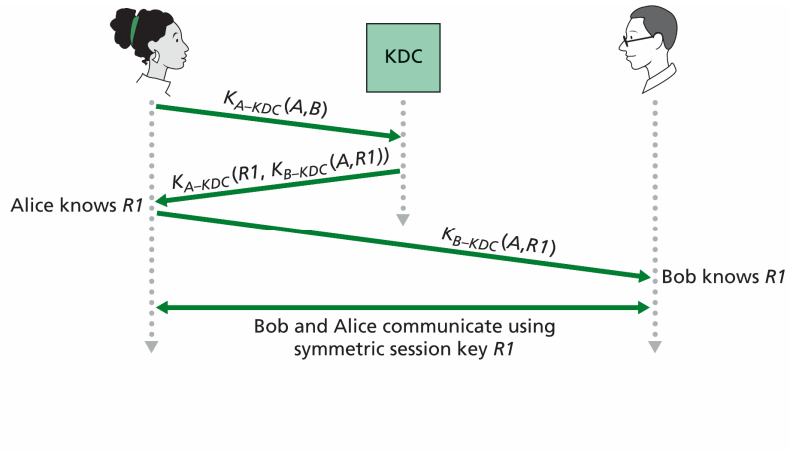
Από το διάγραμμα προκύπτει ότι τα USB Tokens καλύπτουν ικανοποιητικά και τις δύο απαιτήσεις, ενώ οι Smart Cards παρέχουν υψηλό επίπεδο ασφάλειας, αλλά παρουσιάζουν δυσκολίες στην εφαρμογή τους λόγω της εξάρτησής τους από συγκεκριμένο Hardware ανάγνωσής τους.

Τα *Tokens* των δύο τελευταίων κατηγοριών προστατεύουν κρυπτογραφικά κλειδιά ανάλογα με το πρωτόκολλο αυθεντικοποίησης που εφαρμόζεται. Στην περίπτωση πρωτοκόλλου που χρησιμοποιεί Συμμετρική Κρυπτογράφηση, περιέχουν κάποιο κοινό κλειδί κρυπτογράφησης για την ανταλλαγή μηνυμάτων με τον Server που υλοποιεί την αυθεντικοποίηση, ενώ στην περίπτωση Κρυπτογράφησης Δημοσίου Κλειδιού περιέχουν κλειδιά του ζευγαριού Δημόσιο / Ιδιωτικό Κλειδί που αντιστοιχεί στο συγκεκριμένο χρήστη. Η αυθεντικοποίηση με τη χρήση Δημοσίου / Ιδιωτικού κλειδιού μέσω ενός *Hard Crypto Token* μπορεί να γίνει με πολλούς τρόπους. Συνήθως στο *Token* βρίσκεται το Ιδιωτικό Κλειδί του χρήστη, οπότε η «server πλευρά» του πρωτοκόλλου μπορεί να αποκτήσει το Δημόσιο Κλειδί του χρήστη με τη μορφή ενός Ψηφιακού «Πιστοποιητικού» (μπορεί να περιέχεται και αυτό στο *Hard Crypto Token*), να κρυπτογραφήσει ένα τμήμα πληροφορίας (χρήσιμο ή όχι) με αυτό το Δημόσιο Κλειδί εξασφαλίζοντας έτσι ότι η αποκρυπτογράφηση της πληροφορίας μπορεί να γίνει μόνο από τον κάτοχο του αντίστοιχου, σωστού Ιδιωτικού Κλειδιού. Με αυτό τον τρόπο αυθεντικοποιείται ο χρήστης καθώς αποδεικνύει την κατοχή (*Proof of Possession*) και τον έλεγχο του σωστού Ιδιωτικού Κλειδιού [93, 128].

Το πρόβλημα που τίθεται και με τις δύο μεθόδους Κρυπτογράφησης είναι πως θα σιγουρευτούν τα δύο μέρη του πρωτοκόλλου ότι τα κλειδιά του άλλου μέρους είναι τα σωστά. Στην

περίπτωση της Συμμετρικής Κρυπτογράφησης οι δύο συναλλασσόμενοι θα πρέπει να εμπιστευτούν μία τρίτη οντότητα, το *Key Distribution Center - KDC* το οποίο έχει το ρόλο της δημιουργίας κλειδιών μίας χρήσης για καθένα ζευγάρι χρηστών που επιθυμεί να «συνομιλήσει» με ασφάλεια μέσω Συμμετρικής Κρυπτογράφησης. Η συνήθης διαδικασία φαίνεται στην παρακάτω Εικόνα [64]:

Πηγή: [64]

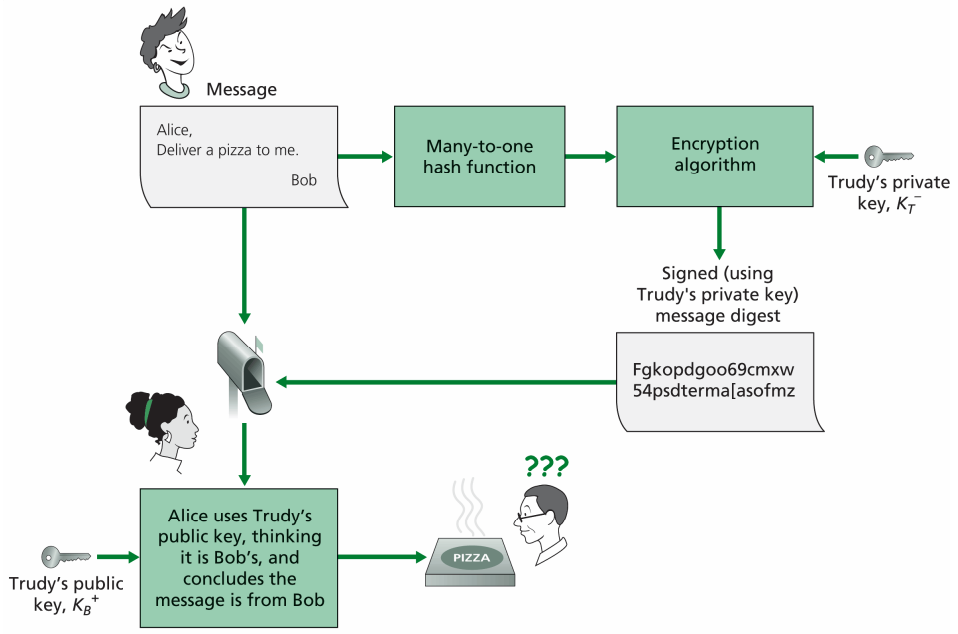


Εικόνα 7: Σχηματική Αναπαράσταση της Λειτουργίας των *KDC*

όπου καθένας χρήστης πρέπει καταρχάς να διατηρεί ένα μόνιμο κλειδί για την επικοινωνία του με το *KDC* ($K_{A\text{-}KDC}$, $K_{B\text{-}KDC}$). Ο χρήστης Α ζητάει από το *KDC* ένα μοναδικό, προσωρινό κλειδί για την επικοινωνία του με το χρήστη Β. Το *KDC* παράγει αυτό το κλειδί (*R1*) και το επιστρέφει στον Α μαζί με ένα τμήμα κρυπτογραφημένου μηνύματος που επίσης περιέχει το *R1* αλλά μπορεί να το διαβάσει μόνο ο χρήστης Β, καθώς είναι κρυπτογραφημένο με το κλειδί $K_{B\text{-}KDC}$. Ο Α αποστέλλει αυτή την κρυπτογραφημένη προσθήκη στον Β, χωρίς να την επεξεργαστεί, και ο Β αποκτά το δικό του αντίγραφο του κοινού κλειδιού *R1*.

Στην περίπτωση της Κρυπτογράφησης Δημοσίου Κλειδιού, το ερώτημα είναι πως μπορεί ένα πρωτόκολλο να εξασφαλίσει ότι το Δημόσιο Κλειδί που έχει στην κατοχή του ένας χρήστης ανήκει στο σωστό χρήστη – «συναλλασσόμενο» και όχι σε κάποιο «εισβολέα» ο οποίος υποδύεται το ρόλο του θεμιτού χρήστη. Το πρόβλημα που μπορεί να προκύψει έγινε σαφές στην «απειλή» "*Man – in – the – Middle*", αλλά φαίνεται επίσης παραστατικά στην παρακάτω Εικόνα:

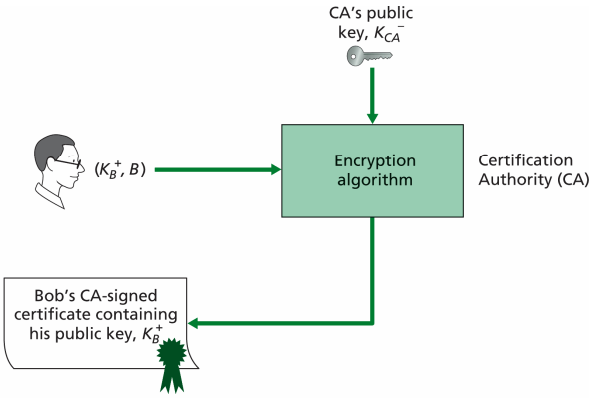
Πηγή: [64]



Εικόνα 8: Πρόβλημα στην Αυθεντικοποίηση με Κρυπτογράφηση Δημοσίου Κλειδιού

όπου η εισβολέας προωθεί το δικό της Δημόσιο Κλειδί ως αυτό του χρήστη Β και η χρήστης Α επιβεβαιώνει λανθασμένα την ταυτότητα του συνομιλητή της ως χρήστης Β. Η λύση σε αυτό το πρόβλημα είναι τα Ψηφιακά «Πιστοποιητικά» (*Digital Certificates*) τα οποία «εκδίδονται» από κοινώς αποδεκτούς και έμπιστους Οργανισμούς, παρέχουν ζεύγη Δημοσίου / Ιδιωτικού Κλειδιού στους ενδιαφερόμενους χρήστες και επικυρώνουν την ταυτότητα του κατόχου ενός Δημοσίου Κλειδιού. Οι συγκεκριμένοι οργανισμοί ονομάζονται *Certification Authorities* (*CA*), μπορεί να ανήκουν στον Ιδιωτικό ή Δημόσιο τομέα και θεωρείται ότι κάνουν τους απαραίτητους έλεγχους ταυτότητας των χρηστών που εξυπηρετούν, ώστε να επιβεβαιώνουν την ταυτοπροσωπία των Πιστοποιητικών που «εκδίδουν». Η διαδικασία είναι ότι ο καθένας χρήστης που αποκτά ένα ζεύγος Δημόσιου / Ιδιωτικού Κλειδιού αποκτά και ένα Ψηφιακό Πιστοποιητικό το οποίο περιέχει τα στοιχεία του, την ημερομηνία έκδοσης και ισχύος του, το *CA* που το εξέδωσε κλπ. Το συγκεκριμένο πιστοποιητικό περιέχει και το Δημόσιο Κλειδί του χρήστη το οποίο κρυπτογραφείται με το Ιδιωτικό Κλειδί του *CA* (K_{CA}^-) (βλ επόμενη Εικόνα). Το Δημόσιο Κλειδί ενός *CA* είναι εύκολα διαθέσιμο και για πολλούς είναι ήδη εγκατεστημένο στους Web Browsers των μοντέρνων Ηλ. Υπολογιστών, οπότε οποιοσδήποτε χρήστης δεχθεί το συγκεκριμένο πιστοποιητικό μπορεί να το αποκωδικοποιήσει με το Δημόσιο Κλειδί του *CA*, να γίνει κάτοχος του Δημοσίου Κλειδιού που περιέχει και να επιβεβαιώσει ότι ο χρήστης που αναγράφεται στο Πιστοποιητικό είναι όντως αυτός που κατέχει το συγκεκριμένο Δημόσιο Κλειδί, καθώς υπάρχει αυτονόητη εμπιστοσύνη στο *CA* που το εξέδωσε και το «υπέγραψε» ψηφιακά. Ταυτόχρονα, λαμβάνει χώρα και έλεγχος της εγκυρότητας του χρήστη καθώς υπάρχουν περιπτώσεις όπου η εμπιστοσύνη στις *CA* δεν είναι αυτονόητη και το σύστημα αυθεντικοποίησης δέχεται Πιστοποιητικά μόνο από συγκεκριμένες *CA* οπότε και φιλτράρονται οι «έμπιστοι» χρήστες [64].

Πηγή: [64]



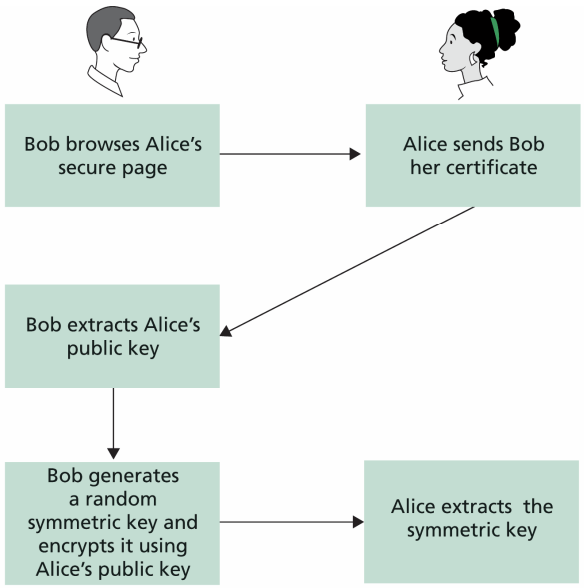
Εικόνα 9: Απόκτηση Ψηφιακού Πιστοποιητικού από *Certificate Authority*

Η δομή των Ψηφιακών Πιστοποιητικών είναι τυποποιημένη και ακολουθεί το πρότυπο X.509 της ITU-T. Τα Πιστοποιητικά X.509 προσδιορίζονται από μία σειρά RFC's (RFC 2459, RFC 3820, RFC 4325, RFC 4630) τα οποία καθορίζουν εκτός από τα ακριβή περιεχόμενα ενός Πιστοποιητικού, τη δομή και τις λειτουργίες μίας *Certificate Authority*. Προκύπτει, επομένως. ένα πλαίσιο εφαρμογής της Κρυπτογράφησης Δημοσίου Κλειδιού το οποίο καλείται *Public Key Infrastructure – PKI* και περιλαμβάνει όλες τις διαδικασίες και κανόνες διαχείρισης των Πιστοποιητικών και των Κλειδιών Κρυπτογράφησης. Επίσης, καθορίζονται οι τρόποι εντοπισμού του κατάλληλου *CA* από ένα χρήστη, στην περίπτωση όπου ένα συγκεκριμένο Πιστοποιητικό έχει εκδοθεί από κάποιο *CA* εκτός των προ-εγκατεστημένων (Ιεραρχίες των *Certification Authorities*) [42].

Ένας ακόμα τρόπος προστασίας της αυθεντικοποίησης με απλή χρήση username & password σε Web Εφαρμογές είναι η κωδικοποίηση της αποστελλόμενης πληροφορίας μέσω του λεγόμενου «ασφαλούς HTTP» πρωτοκόλλου, του HTTPS. Το συγκεκριμένο πρωτόκολλο είναι ουσιαστικά το βασικό πρωτόκολλο του World Wide Web, το HTTP, με τη χρήση του πρωτοκόλλου ασφαλούς μετάδοσης *Secure Sockets Layer / Transport Layer Security* (SSL/TLS). Το SSL/TLS είναι πρωτόκολλο που λειτουργεί πάνω από το πρωτόκολλο TCP και χρησιμοποιείται από τα πρωτόκολλα εφαρμογών του Internet (HTTP, FTP κλπ) για ασφαλή μετάδοση δεδομένων μεταξύ των Clients και Servers των βασικών εφαρμογών του Internet και την αποτροπή των «απειλών»: "*Eavesdropping*", "*Man – in – the middle*" (υπό ορισμένες προϋποθέσεις) και της αλλοίωσης του περιεχομένου των μηνυμάτων. Αρχικά δημιουργήθηκε το SSL από τη Netscape και μετά από διαδοχικές εξελίξεις η τρέχουσα έκδοσή του είναι το *TLS* v1.1 [18]. Η λειτουργία του απαιτεί την ύπαρξη ενός ζευγαριού Δημοσίου/Ιδιωτικού κλειδιού στον Web Server, η οποία πιστοποιείται με ένα Ψηφιακό Πιστοποιητικό μίας κοινώς αποδεκτής *CA* ή μίας *CA* που λειτουργεί στα πλαίσια του συγκεκριμένου Πληροφ. Συστήματος. Με αυτό τον τρόπο είναι δυνατή η αρχική αυθεντικοποίηση του SSL Server ώστε να είναι σίγουρος ο Client ότι «συνομιλεί» με το σωστό Server: μόλις ξεκινάει η επικοινωνία με τον Web Server αυτός αποστέλλει στον Client το πιστοποιητικό του το οποίο περιέχει το Δημόσιο κλειδί του, αλλά είναι κρυπτογραφημένο με το ιδιωτικό κλειδί του *CA* (ψηφιακή υπογραφή του *CA*). Οι Web Browsers διαθέτουν τα Δημόσια Κλειδιά των πιο γνωστών *CA's* άρα, εφόσον το συγκεκριμένο πιστοποιητικό είναι γνήσιο, μπορούν να το αποκρυπτογραφήσουν και να επιβεβαιώσουν την ταυτότητα του Web Server. Αυτό το βήμα αυθεντικοποίησης του Web Server απο-

τελεί και το πρώτο βήμα στη λειτουργία του SSL/TLS. Ο Web Browser, έχοντας στην κατοχή του το Δημόσιο Κλειδί του Web Server, δημιουργεί ένα τυχαίο κλειδί συνόδου (session key), για να χρησιμοποιηθεί στη μετέπειτα συμμετρική κρυπτογράφηση των δεδομένων μεταξύ του ίδιου και του Web Server. Το κλειδί αποστέλλεται στον Web Server κρυπτογραφημένο με το Δημόσιο Κλειδί του. Ο Web Server αποκρυπτογραφεί το μήνυμα με το Ιδιωτικό Κλειδί του και αποκτά έτσι το κοινό κλειδί συνόδου με το οποίο μπορεί από αυτή τη στιγμή να ανταλλάσσει κρυπτογραφημένα μηνύματα με τον Web Client. Με αυτό τον τρόπο μπορεί ο Client να αποστείλει τους προσωπικούς κωδικούς του χρήστη (PIN ή password) χωρίς να απειλούνται από υποκλοπή, τουλάχιστον όσο μεταδίδονται μέχρι τον Web Server. Αυτό αποτελεί μία έμμεση εφαρμογή του πρωτοκόλλου HTTPS (HTTP + SSL/TLS) στα συστήματα αυθεντικοποίησης [64].

Πηγή: [64]



Εικόνα 10: Αναπαράσταση των Βασικών, Αρχικών Βημάτων του SSL/TLS

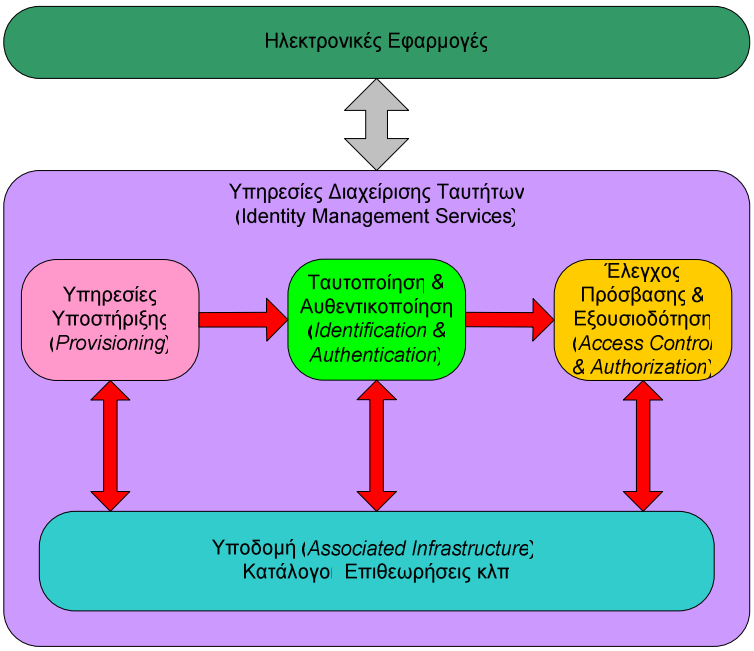
2.2 Αυθεντικοποίηση και Διαχείριση Ταυτοτήτων στο Διαδίκτυο

Η Διαχείριση Ταυτοτήτων (*Identity Management - IdM*) γενικά συνδυάζει τις διαδικασίες, τεχνολογίες και πολιτικές διαχείρισης των ψηφιακών ταυτοτήτων καθώς και του τρόπου χρήσης των ταυτοτήτων για τον έλεγχο πρόσβασης στους πόρους ενός πληροφοριακού συστήματος. Οι προσπάθειες ανάπτυξης συστημάτων Διαχείρισης Ταυτοτήτων καθίστανται ιδιαιτέρως πολύπλοκες στα πλαίσια ενός σύγχρονου οργανισμού λόγω: της ποικιλομορφίας των τεχνολογιών και προτύπων ταυτοτήτων, των πολλών απειλών της ασφάλειας των συστημάτων, της επέκτασης των δικτύων και της αύξησης των χρηστών, των σύγχρονων επιχειρηματικών δράσεων και αναγκών. Η ανάπτυξη διαφορετικών εφαρμογών σε διαφορετικές πλατφόρμες

με ιδιαίτερες απαιτήσεις διαχείρισης ταυτοτήτων (Portals, Web Applications, Client – Server εφαρμογές κλπ), οι αυξημένες ανάγκες εξυπηρέτησης συναλλασσομένων ή υπαλλήλων, ο κατακερματισμός των οργανισμών σε ποικίλα λειτουργικά ή γεωγραφικά υπο-συστήματα, οι επιχειρηματικές δράσεις στενής συνεργασίας και εμπιστοσύνης μεταξύ οργανισμών είναι μερικές από τις σύγχρονες πραγματικότητες που οδηγούν την εξέλιξη, τυποποίηση και οικοδόμηση των σύγχρονων συστημάτων Διαχείρισης Ταυτοτήτων [86].

Ένα γενικό σχεδιάγραμμα των υπηρεσιών που εξασφαλίζονται μέσω ενός συστήματος Διαχείρισης Ταυτοτήτων σε ένα Πληροφοριακό Σύστημα με προσανατολισμό την εξαγωγή υπηρεσιών στο διαδίκτυο φαίνεται στην παρακάτω Εικόνα.

Πηγή: [36]



Εικόνα 11: Βασικές Υπηρεσίες Συστήματος Διαχείρισης Ταυτοτήτων

Οι *Υποστηρικτικές Υπηρεσίες* (*Provisioning*) αφορούν [36]:

- Υπηρεσίες δημιουργίας Ταυτοτήτων (*Identity Creation Services*): είναι οι υπηρεσίες που ελέγχουν και επιβεβαιώνουν τα προσωπικά δεδομένα των χρηστών ώστε να εγκριθεί η δημιουργία ψηφιακής ταυτότητας γι αυτούς. Καθορίζουν τον τρόπο και τη μέθοδο με την οποία θα δημιουργούνται οι ψηφιακές ταυτότητες των χρηστών.

- Υπηρεσίες Εγγραφής Χρηστών (*Enrolment Services*): αποδίδουν στους χρήστες τα δικαιώματα πρόσβασής τους στις δικτυακές υπηρεσίες, ανάλογα με τα επίπεδα εξουσιοδότησης που έχουν καθοριστεί.

- Υπηρεσίες Διάχυσης Στοιχείων Ταυτοτήτων (*Dissemination Services*): εξασφαλίζουν την αυτόματη ενημέρωση όσων συστημάτων διατηρούν πληροφορίες ταυτοτήτων με όποια νέα δεδομένα δημιουργούνται ή αλλάζουν.

Η *Υποδομή* (*Associated Infrastructure*) που είναι απαραίτητη για την ανάπτυξη ενός συστήματος Διαχείρισης Ταυτοτήτων περιλαμβάνει τα δομικά συστατικά [36]:

- Υπηρεσίες Καταλόγου (*Directory Service*): είναι η δομή όπου αποθηκεύονται όλα τα δεδομένα των ταυτοτήτων του συστήματος. Πέρα από το τμήμα της απλής αποθήκευσης δεδομένων ταυτοτήτων, οι Υπηρεσίες Καταλόγου καθορίζουν την ποικιλία των χαρακτηριστικών γνωρισμάτων που είναι δυνατό να συνδεθούν με ένα χρήστη, τις δυνατότητες αποθήκευσης ψηφιακών πιστοποιητικών στους λογαριασμούς των χρηστών κλπ.

- Υπηρεσίες Ασφαλείας (*Security Services*): εξασφαλίζουν την ακεραιότητα και τον απαραβίαστο χαρακτήρα των μεταδιδόμενων πληροφοριών ταυτοτήτων, πχ με μεθόδους κρυπτογράφησης.

- Υπηρεσίες Εμπιστευτικότητας (*Confidentiality Services*): αποτρέπουν την παραχάραξη των ταυτοτήτων με τεχνικές κρυπτογράφησης.

- Υπηρεσίες Επιθεωρήσεων και Αναφορών (*Audit & Reporting Services*): παρέχουν ενημέρωση στους διαχειριστές των συστημάτων για τη χρήση των δεδομένων ταυτοτήτων.

- Υπηρεσίες Διαλειτουργικότητας (*Interoperability Services*): εξασφαλίζουν την μεταφορά ή διαμοίραση των δεδομένων των ταυτοτήτων σε άλλα συστήματα ή οργανισμούς, ανάλογα και με τα επιτρεπόμενα από το θεσμικό πλαίσιο για τα προσωπικά δεδομένα.

- Υπηρεσίες Πρόσβασης μέσω Κινητών Μέσων (*Mobile Services*): υποστηρίζουν την απομακρυσμένη πρόσβαση των χρηστών μέσω «κινητών» συσκευών (τηλεφώνων ή υπολογιστών) στις εφαρμογών των συστημάτων, εξασφαλίζοντας ομοιογένεια μεταξύ των διαφόρων προτύπων επικοινωνίας των συγκεκριμένων συσκευών.

- Υπηρεσίες Διαχείρισης Συστήματος (*System Management Services*): παρέχουν στους διαχειριστές και στο υποστηρικτικό προσωπικό τις κατάλληλες πληροφορίες, διαχειριστικές λειτουργίες και απαραίτητους ελέγχους λαθών.

Το σημαντικότερο για την παρούσα εργασία τμήμα του παραπάνω συστήματος Διαχείρισης Ταυτοτήτων είναι το υπο-σύστημα Ταυτοποίησης και Αυθεντικοποίησης (*Identification & Authentication*) των χρηστών [36]:

- Υπηρεσίες Αυθεντικοποίησης (*Authentication Services*): περιλαμβάνουν όλους τους μηχανισμούς και τα πρωτόκολλα επιβεβαίωσης της ταυτότητας των χρηστών του δικτύου. Σύμφωνα και με την προηγούμενη ενότητα είναι δυνατή η εφαρμογή ποικίλων μεθόδων αυθεντικοποίησης: η απλή εισαγωγή μία κωδικής λέξης (password), η εφαρμογή τεχνολογιών κρυπτογράφησης που βασίζονται σε *Public Key Infrastructure – PKI*, οι τεχνικές που βασίζονται στον έλεγχο βιομετρικών δεδομένων κλπ. Σε ένα Πληροφοριακό Σύστημα διαδικτυακών υπηρεσιών ορίζονται συνήθως διαφορετικά «επίπεδα» εγγύησης ασφαλείας (*Assurance Levels*) η οποία παρέχεται μέσω των εφαρμοζόμενων τεχνολογιών αυθεντικοποίησης. Για υπηρεσίες, δηλαδή, όπου δεν θεωρούνται ιδιαίτερα κρίσιμες μπορεί να εφαρμοστεί αυθεντικοποίηση χαμηλής εξασφάλισης ασφάλειας, σε σημαντικότερες υπηρεσίες ορίζεται η εφαρμογή αυθεντικοποίησης μεγαλύτερης εξασφάλισης κ.ο.κ.

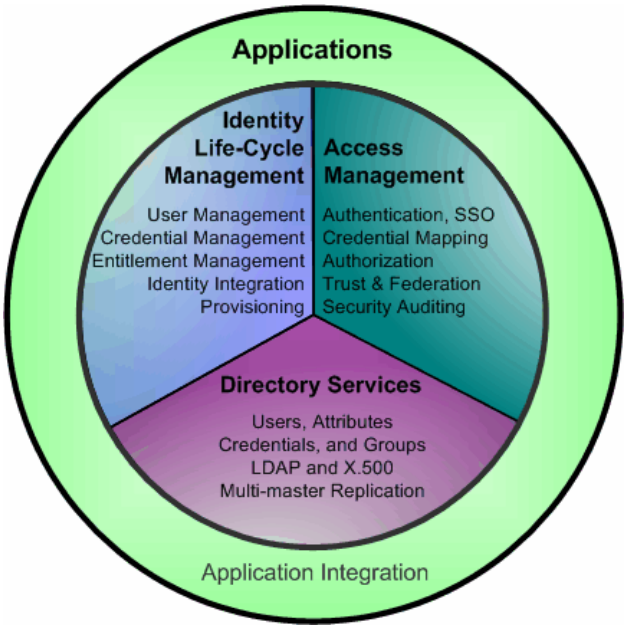
- *Single Sign – On*: στα πλαίσια ενός συστήματος πολλών δικτυακών υπηρεσιών ή ενός Portal είναι η απαραίτητη υπηρεσία μοναδικής αυθεντικοποίησης του χρήστη κατά την

πρώτη είσοδό του σε μία υπηρεσία και η διατήρηση της αυθεντικοποιημένης κατάστασής του κατά την πρόσβασή του σε άλλες υπηρεσίες του ίδιου συστήματος ή Portal. Με αυτό τον τρόπο δε χρειάζεται ο χρήστης να εισάγει τα «πιστοποιητικά» της ταυτότητάς του κάθε φορά που προσπελαύνει μία νέα υπηρεσία.

- Υπηρεσίες Διαχείρισης Πρόσθετων Ιδιοτήτων των Ταυτοτήτων (*Identity Attribute Provision Services*): είναι οι υπηρεσίες που πρέπει να παρέχονται σε όσες δικτυακές εφαρμογές απαιτούν τη γνώση πρόσθετων ιδιοτήτων ενός χρήστη, συνήθως για τις αποφάσεις εξουσιοδότησης και ενεργοποιούνται μετά την αυθεντικοποίηση του χρήστη.

Η Microsoft [86] παρουσιάζει μία αντίστοιχη κατανομή των εργασιών και υπο-συστημάτων Διαχείρισης Ταυτότητας. Οι διαδικασίες *Provisioning* των ταυτοτήτων και της όλης διαχείρισης του συστήματος ονομάζονται «Διαχείριση Κύκλου – Ζωής Ταυτοτήτων» ("*Identity Life – Cycle Management*"). Αποδίδεται ξεχωριστή θέση στις «Υπηρεσίες Καταλόγου» ("*Directory Services*") Η Αυθεντικοποίηση εντάσσεται στο γενικό υπο-σύστημα «Διαχείριση Πρόσβασης» ("*Access Management*"), ενώ όλο το σύστημα καταλήγει στις κατάλληλες, τυποποιημένες διεπαφές με τις «Εφαρμογές Λογισμικού» ("*Applications*") που είναι οι τελικοί «καταναλωτές» των πληροφοριών ταυτοτήτων (βλ. παρακάτω Εικόνα).

Πηγή: [86]



Εικόνα 12: Η Πρόταση της Microsoft για την Υποδομή Συστήματος Διαχείρισης Ταυτοτήτων και Πρόσβασης (*Microsoft Identity and Access Management Framework*)

Το υπο-σύστημα *Access Management* εκτός από τις βασικές διαδικασίες Αυθεντικοποίηση (*Authentication*), Αντιστοίχιση Πιστοποιητικών (*Credential Mapping*), Single Sign – On, Εξουσιοδότηση (*Authorization*) και Ελέγχων Ασφάλειας (*Security Auditing*) περιλαμβάνει δύο πρόσθετες έννοιες: *Trust & Federation* [86]:

- *Trust*: η έννοια *Trust* (*Εμπιστοσύνη*) αποκτά μεγάλη σημασία στους σύγχρονους οργανισμούς καθώς είναι έντονη η ανάγκη διαμοίρασης πόρων και υπηρεσιών μεταξύ τους. Οι

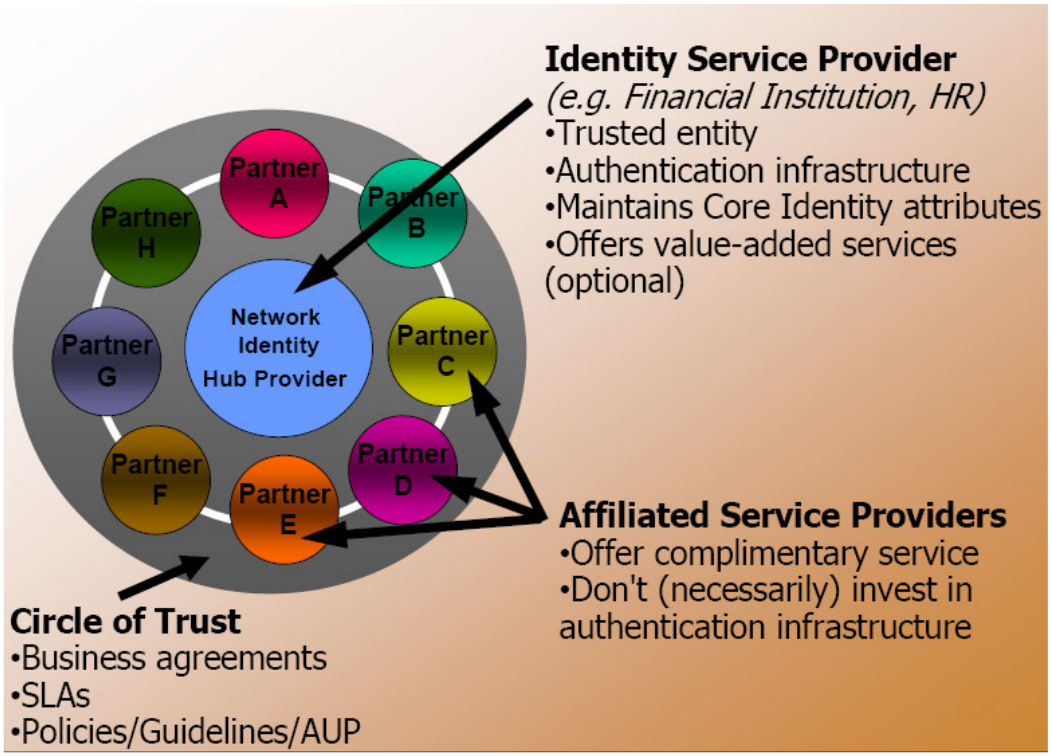
συνεργασίες, επομένως, μεταξύ οργανισμών, η επέκταση του e-Commerce και του e-Government έχει οδηγήσει σε πολύπλοκα σχήματα στα οποία είναι συχνή η απαίτηση κοινής χρήσης πόρων με διαφορετικές τεχνολογικές πλατφόρμες. Η εγκαθίδρυση «έμπιστης» σχέσης μεταξύ των οργανισμών αποτελεί την απαραίτητη προϋπόθεση για την ασφαλή αυθεντικοποίηση των χρηστών αυτόνομων πληροφοριακών συστημάτων με το λιγότερο δυνατό διαχειριστικό κόστος. Οι μηχανισμοί υλοποίησης της «έμπιστης» σχέσης μεταξύ οργανισμών περιλαμβάνουν πολλές εργασίες προς το σκοπό της ανάπτυξης ενός ασφαλούς μηχανισμού – διαύλου επικοινωνίας και οι οποίες εργασίες αφορούν τεχνολογικά προβλήματα αλλά και διοικητικά θέματα του τρόπου και του εύρους διάθεσης πόρων ενός οργανισμού στους υπόλοιπους «έμπιστους» οργανισμούς.

- *Federation*: είναι μία «συνομοσπονδία» οργανισμών οι οποίοι έχουν εγκαθιδρύσει μεταξύ τους «έμπιστη» σχέση (*Trust*) διαμοίρασης πόρων. Ανάλογα με το επίπεδο της εμπιστοσύνης είναι δυνατή η ασφαλής αυθεντικοποίηση και ο έλεγχος πρόσβασης χρηστών ενός οργανισμού της *Federation* σε δικτυακούς πόρους του άλλου. Για παράδειγμα ο χρήστης μίας εταιρίας Α μπορεί να προσπελάσει δεδομένα ή υπηρεσίες μίας εταιρίας Β χρησιμοποιώντας το μοναδικό λογαριασμό που διαθέτει στην εταιρία Α, γιατί οι δύο εταιρίες έχουν «έμπιστη» σχέση στα πλαίσια του *Federation*. Δημιουργούνται, επομένως, «συνομοσπονδίες» (*Federations*) οργανισμών και τεχνολογιών μέσα στα όρια των οποίων υπάρχει η ανάγκη μετάδοσης των δεδομένων ταυτοτήτων του καθένα οργανισμού, αλλά και των διαθέσιμων δικτυακών υπηρεσιών. Συνεπώς, μέσα στο «εκτεταμένο», «ομόσπονδο» μοντέλο διαχείρισης ταυτοτήτων κάθε οργανισμός καθορίζει έναν τυποποιημένο και ασφαλή τρόπο για τη δημοσίευση όχι μόνο των διαθέσιμων υπηρεσιών σε «έμπιστους» συνεργάτες και πελάτες, αλλά και των πολιτικών ασφαλείας που εφαρμόζει (τι είδους πιστοποιητικά δέχεται για την αναγνώριση των χρηστών, ποιους άλλους οργανισμούς και χρήστες «εμπιστεύεται» κλπ). Όλες αυτές οι ενέργειες και διαδικασίες σχηματίζουν ένα σύστημα Διαχείρισης Ταυτοτήτων εξειδικευμένο για τις *Federations*, ένα σύστημα *Federated Identity Management* [115].

Συνοπτικά, η *Trust* είναι το τεχνολογικό και διοικητικό υπόβαθρο με το οποίο εξασφαλίζεται ότι οι «έμπιστοι» οργανισμοί τηρούν συγκεκριμένα πρότυπα ασφαλείας των ταυτοτήτων που διαχειρίζονται, οπότε τα πιστοποιητικά των χρηστών που προέρχονται από αυτούς μπορούν να γίνουν δεκτά από τον αποδέκτη της «έμπιστης» σχέσης. *Federation* είναι η συνεργασία «έμπιστων» οργανισμών για την αμοιβαία αυθεντικοποίηση και εξουσιοδότηση χρηστών τους με ασφαλή, ομοιόμορφο και πρότυπο τρόπο ελάχιστου διαχειριστικού κόστους. Τεχνολογικά η *Trust* μεταξύ οργανισμών επιτυγχάνεται συνήθως με την εγκατάσταση ψηφιακών πιστοποιητικών σε *Public Key Infrastructure – PKI* [72, 86]. Οι *Trust* & *Federation* προέκυψαν από την εξάπλωση των «δικτύων αξιών» ("*Value Networks*") των οργανισμών (Ιδιωτικών ή Δημοσίων) τα οποία πια επεκτείνονται σε πολλούς πελάτες, προμηθευτές, εξωτερικούς συνεργάτες, άλλους ομότιμους οργανισμούς κλπ. Η ανάπτυξη των δικτυακών εφαρμογών e-Business και e-Government δημιούργησε την ανάγκη αυστηρού ελέγχου της ταυτότητας των χρηστών τους, των οποίων όμως ο αριθμός είναι μη ελεγχόμενος. Η απόπειρα κεντρικής διαχείρισης των ταυτοτήτων χρηστών όλου του περιγραφόμενου εύρους συνεργασιών προκαλεί μεγάλο διαχειριστικό κόστος και ελάχιστη ευελιξία στον οργανισμό. Από την άλλη πλευρά, οι προσπάθειες ad – hoc συνεργασιών οργανισμών, χωρίς συγκεκριμένες πρότυπες διαδικασίες μπορούν να απειλήσουν την ασφάλεια των δεδομένων ταυτοτήτων των οργανισμών ή να επιτρέψουν κενά ασφαλείας κατά την αυθεντικοποίηση των χρηστών [43].

Η έννοια του *Federation* συναντάται και με τον όρο «Κύκλος Εμπιστοσύνης» ("*Circle of Trust*") μεταξύ οργανισμών που διατηρούν τα δεδομένα ταυτοτήτων των χρηστών (*Identity Providers*) και των οργανισμών που παρέχουν τις δικτυακές υπηρεσίες (*Service Providers*). Οι συγκεκριμένοι *Providers* διατηρούν τεχνολογικές, διοικητικές και επιχειρηματικές σχέσεις εμπιστοσύνης έτσι ώστε οι χρήστες τους να έχουν τη δυνατότητα ομοιόμορφων και ασφαλών συναλλαγών χωρίς να αντιλαμβάνονται τις υποβόσκουσες λεπτομέρειες. Ο «κύκλος» έχει την έννοια ότι η εμπιστοσύνη δεν είναι απαραίτητο να υφίσταται απευθείας μεταξύ οποιωνδήποτε δύο οργανισμών, αλλά να «μεταβιβάζεται» μεταξύ δύο «έμπιστων» οργανισμών, οπότε κάθε οργανισμός στον «κύκλο» μπορεί να εμπιστευτεί κάποιο άλλο μέλος του «κύκλου». Μία σχηματική αναπαράσταση του "*Circle of Trust*" φαίνεται στην παρακάτω Εικόνα [71]:

Πηγή: [70]

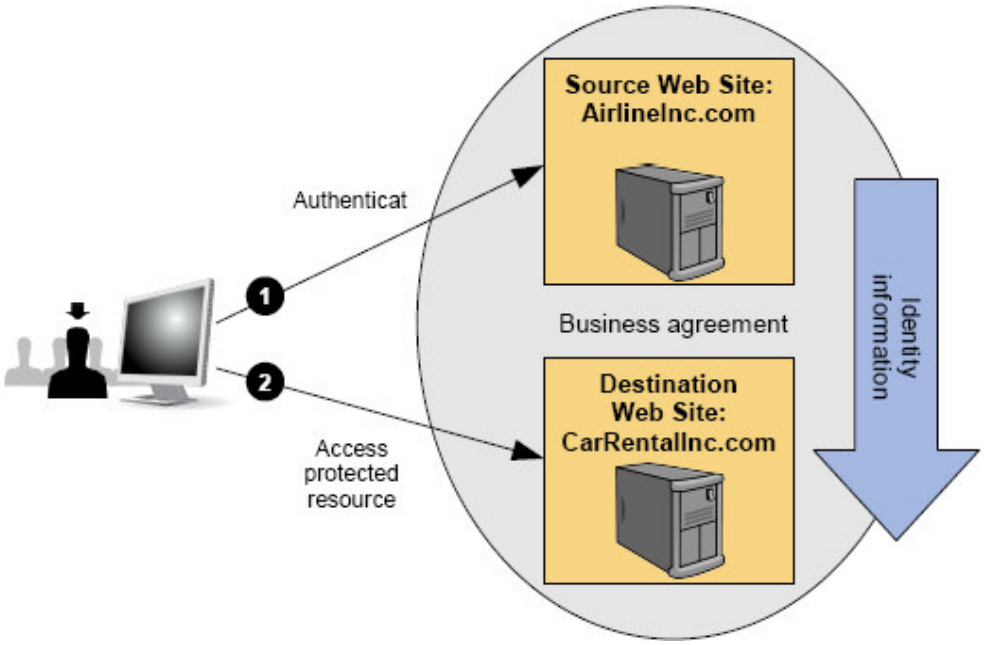


Εικόνα 13: «*Κύκλος Εμπιστοσύνης*» ("*Circle of Trust*")

Στη συγκεκριμένη αναπαράσταση το κέντρο του «κύκλου» είναι οι οργανισμοί που περιέχουν τα «έμπιστα» δεδομένα ταυτοτήτων των χρηστών, διαθέτουν υποδομή αυθεντικοποίησης και μπορούν να επιβεβαιώσουν την εγκυρότητα των πιστοποιητικών χρηστών στα υπόλοιπα συνεργαζόμενα μέλη. Οι οργανισμοί στην περιφέρεια του «κύκλου» διαθέτουν τις δικτυακές υπηρεσίες, αλλά πιθανώς καθόλου υποδομή αυθεντικοποίησης και όλες εμπιστεύονται είτε απευθείας τον κεντρικό οργανισμό του «κύκλου» είτε τις σχέσεις εμπιστοσύνης που διατηρούν συνεργαζόμενοι οργανισμοί με τον κεντρικό οργανισμό. Το υπόβαθρο όλου του «κύκλου» είναι οι επιχειρηματικές συμφωνίες, οι πολιτικές ασφαλείας, οι οδηγίες και οι Συμφωνίες Επιπέδου Υπηρεσιών (*Service Level Agreements – SLAs*) τα οποία διέπουν την έμπιστη σχέση των οργανισμών και αποσκοπούν στον ακριβή ορισμό των τηρουμένων διαδικασιών, των δεδομένων που μεταδίδονται μεταξύ των οργανισμών και της απαραίτητης ενημέρωσης των χρηστών για τις εφαρμοζόμενες συμφωνίες διαμοίρασης πόρων [68].

Συνεπώς, οι έννοιες *Trust & Federation* αποτελούν την εξέλιξη των διαδικασιών διαχείρισης ταυτοτήτων με την υπέρβαση των ορίων ενός αυτόνομου οργανισμού και παρέχουν όλα τα οφέλη της ασφαλούς αυθεντικοποίησης μεταξύ «έμπιστων», συνεργαζόμενων οργανισμών. Σε αυτό το περιβάλλον η ταυτότητα (*Identity*) ενός χρήστη και όλα τα δεδομένα που την πιστοποιούν αποκτούν νέο χαρακτηρισμό, αυτόν του *Federated Identity*. Ταυτόχρονα, οι διαδικασίες διαχείρισης των *Federated Identities* συγκροτούν τα πρότυπα *Federated Identity Management*. Ένα πρώτο όφελος του *Federated Identity Management* είναι η εφαρμογή της υπηρεσίας Single Sign – On, όταν ο χρήστης προσπελαύνει Δικτυακές Εφαρμογές ακόμα και διαφορετικών οργανισμών, οι οποίοι όμως διατηρούν «έμπιστη» σχέση στη μεταφορά δεδομένων ταυτοτήτων τους. Ένα σχετικό παράδειγμα φαίνεται στην παρακάτω Εικόνα [103]:

Πηγή: [103]



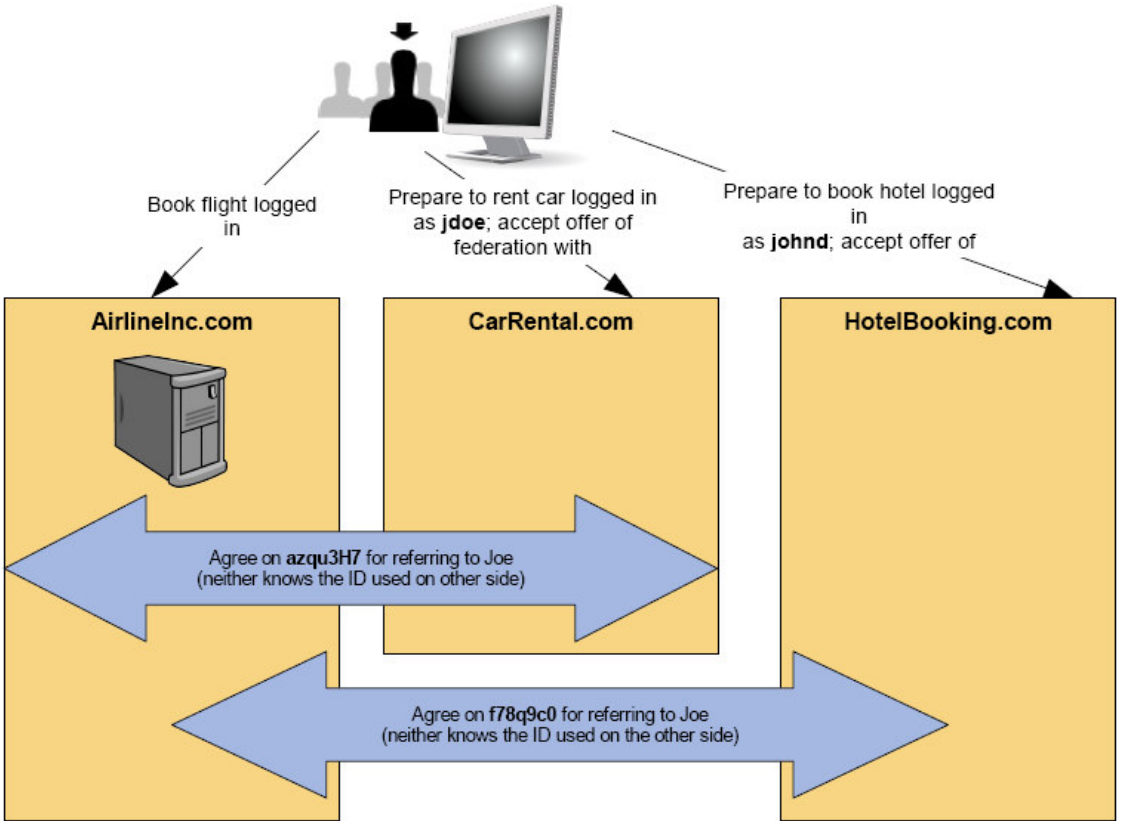
Εικόνα 14: Παράδειγμα Single Sign – On Μεταξύ Διαφορετικών Οργανισμών

Στο συγκεκριμένο παράδειγμα ο χρήστης προσπελαύνει αρχικά την υπηρεσία αεροπορικών κρατήσεων (*AirlineInc.com*) η οποία και τον αυθεντικοποιεί με βάση το λογαριασμό που διατηρεί γι αυτόν. Στη συνέχεια επιχειρεί να προσπελάσει (ενδεχομένως να υπάρχει σχετική σύνδεση στο Web Site της *AirlineInc.com*) το Web Site της εταιρίας ενοικίασης αυτοκινήτων (*CarRentalInc.com*). Μεταξύ των δύο εταιριών, όμως, υπάρχει επιχειρηματική συμφωνία και τεχνολογική «εμπιστοσύνη» διαμοίρασης των πόρων και των πληροφοριών ταυτοτήτων των χρηστών τους. Συνεπώς, η *AirlineInc.com* βεβαιώνει τη συνεργαζόμενη *CarRentalInc.com* για την εγκυρότητα της ταυτότητας του συγκεκριμένου χρήστη, ο οποίος αποκτά πρόσβαση στην υπηρεσία *CarRentalInc.com* μέσω της «ομόσπονδης» ταυτότητάς του (*Federated Identity*) χωρίς να διατηρεί λογαριασμό στην *CarRentalInc.com* και χωρίς να επαναληφθεί η διαδικασία αυθεντικοποίησής του [103].

Η έννοια της *Federated Identity* ξεπερνά τις ιδιότητες της συνήθους ταυτότητας ενός χρήστη στα πλαίσια ενός αυτόνομου οργανισμού. Ο ίδιος χρήστης, δηλαδή, μπορεί να διατηρεί λογαριασμούς σε πολλαπλές εφαρμογές, διαφορετικών εταιριών μέσα στο Internet και προφανώς

επιθυμεί να εισέρχεται σε κάθε υπηρεσία με τον τοπικό λογαριασμό καθεμιάς, ο οποίος μπορεί να συνδέεται και με πιθανό ιστορικό αγορών ή προσφορών κλπ. Η έννοια της *Federated Identity* παρέχει αυτή τη δυνατότητα σε ένα χρήστη: να προσπελαύνει υπηρεσίες διαφορετικών οργανισμών, οι οποίοι όμως έχουν προηγουμένως αναπτύξει τεχνολογική και διοικητική συμφωνία «έμπιστης» σχέσης, με τα στοιχεία ταυτότητας που διατηρεί στον καθένα οργανισμό. Ένα παράδειγμα αυτής της εφαρμογής *Federated Identity* φαίνεται στην παρακάτω Εικόνα [103]:

Πηγή: [103]



Εικόνα 15: Παράδειγμα *Federated Identity* Μεταξύ Διαφορετικών Οργανισμών

Στο συγκεκριμένο παράδειγμα ο χρήστης διατηρεί λογαριασμούς και στις τρεις δικτυακές υπηρεσίες *AirlineInc.com* (username: *johndoe*), *CarRental.com* (username: *jdoe*), *HotelBooking.com* (username: *johnd*). Ο χρήστης εισέρχεται πρώτα στην *AirlineInc.com* όπου και αυθεντικοποιείται ως *johndoe*. Στη συνέχεια ενεργοποιεί κάποια πιθανή σύνδεση που υπάρχει στην *AirlineInc.com* προς τις ενοικιάσεις αυτοκινήτων *CarRental.com*. Καθώς οι δύο οργανισμοί διαθέτουν «έμπιστη» σχέση, ο χρήστης ερωτάται αν επιθυμεί να συνδεθεί με κάποιο τοπικό λογαριασμό στην *CarRental.com*. Ο χρήστης μπορεί να επιλέξει τον τοπικό λογαριασμό του *jdoe* και τότε οι δύο λογαριασμοί συνδέονται με ένα «ψευδώνυμο», πχ το *azqu3H7*, με το οποίο αναφέρονται στο συγκεκριμένο χρήστη από αυτό το χρονικό σημείο και εξής, χωρίς να ξέρουν λεπτομέρειες της ταυτότητάς του σε καμία από τις δύο υπηρεσίες. Στο μέλλον, κάθε πρόσβαση του συγκεκριμένου χρήστη από τη μία υπηρεσία στην άλλη θα υλοποιείται μέσω του ψευδωνύμου και με μόνο μία αυθεντικοποίηση στην πρώτη κατά σειρά υπηρεσία. Το ίδιο συμβαίνει και μεταξύ των λογαριασμών του χρήστη στις υπηρεσίες *AirlineInc.com* και *Ho-*

telBooking.com οι οποίοι συνδέονται μέσω ενός τυχαίου ψευδωνύμου, πχ *f78q9C0*. Συνεπώς, ο χρήστης θα αυθεντικοποιείται κάθε φορά από την *AirlineInc.com* και μέσω των ψευδωνύμων που έχουν δημιουργηθεί αποκτά *Federated Identity* και στις δύο συνεργαζόμενες υπηρεσίες οι οποίες εμπιστεύονται την επιτυχή αυθεντικοποίηση της πρώτης υπηρεσίας [103].

Το παραπάνω παράδειγμα καταδεικνύει την τόνωση της επιχειρηματικής αξιοποίησης του Internet που προσφέρει το *Federated Identity Management* και πως μπορούν να ικανοποιηθούν ή ακόμα να προκύψουν πολλά σενάρια καθημερινής πρακτικής και χρήσης του Internet. Γι αυτό και τα θέματα του *Federated Identity Management* θεωρούνται ως η σύγχρονη πρόκληση ενίσχυσης του ρόλου του Internet και ότι μπορούν να σηματοδοτήσουν μία επαναστατική εκκίνηση διεύρυνσης της επιχειρηματικής (e-Business) και κυβερνητικής (e-Government) εκμετάλλευσής του [43]. Ταυτόχρονα, η συγκεκριμένη «σύγκλιση» του σύγχρονου Internet προς τα *Federated* «σενάρια» χρήσης καθιστά απαραίτητη την εφαρμογή των μεθόδων «ισχυρής» αυθεντικοποίησης της προηγούμενης ενότητας, καθώς η αυθεντικοποίηση υλοποιείται σε ένα μόνο σημείο του *Federation* και όλες οι άλλες οντότητες εμπιστεύονται τη συγκεκριμένη επιβεβαίωση εγκυρότητας.

Συμπερασματικά. γίνεται σαφές ότι η αυθεντικοποίηση είναι αναπόσπαστο μέρος ενός σύνθετου προβλήματος διαχείρισης ταυτοτήτων. Ειδικότερα σε ένα περιβάλλον e-Business ή e-Government προέχει η απλοποίηση της διαδικασίας αυθεντικοποίησης από τη μεριά του συναλλασσομένου, η μείωση του διαχειριστικού κόστους από τη μεριά των Portals – Web Applications και η ενίσχυση της ασφάλειας. Από την παρουσίαση των υπο-συστημάτων της διαχείρισης ταυτοτήτων προέκυψαν αυτόματα τα σημαντικότερα θέματα που αφορούν την αυθεντικοποίηση σε διαδικτυακές εφαρμογές ή Portals:

- Οι μηχανισμοί και τα πρωτόκολλα αυθεντικοποίησης.
- Οι Υπηρεσίες Καταλόγου (*Directory Services*).
- Η υπηρεσία Single Sign – On.
- Οι διαδικασίες *Federated Identity Management* και οι εφαρμογές τους σε πραγματικά σενάρια.

Η δομή της υπόλοιπης εργασίας ακολουθεί αυτές τις ενότητες, ενώ τα συμπληρωματικά ζητήματα *Provisioning* των ταυτοτήτων, υποδομής και διαχείρισης του συστήματος και Εξουσιοδότησης (*Authorization*) είναι εκτός του εύρους της εργασίας.

2.3 Πρωτόκολλα Σχετιζόμενα με Τεχνολογίες Αυθεντικοποίησης

2.3.1 Διαδικασία Αυθεντικοποίησης

Εξαιτίας της μεγάλης σημασίας της διαδικασίας ασφαλούς αυθεντικοποίησης χρηστών έχουν αναπτυχθεί πολλά πρωτόκολλα αυθεντικοποίησης μερικά από τα οποία έχουν εξειδικευμένες

εφαρμογές, ενώ άλλα χρησιμοποιούνται σε γενικότερες περιπτώσεις. Μία συνοπτική απαρίθμηση τέτοιων πρωτοκόλλων είναι [86, 108]:

- ***Kerberos***: διαδεδομένο πρωτόκολλο αυθεντικοποίησης σε δικτυακά περιβάλλοντα, παρουσιάζεται αναλυτικότερα σε επόμενη ενότητα.

- ***Security Assertion Markup Language – SAML***: πρότυπη γλώσσα περιγραφής και μετάδοσης «βεβαιώσεων» ταυτότητας ηλεκτρονικών χρηστών για εφαρμογές σε *Federated Identity Management*, παρουσιάζεται αναλυτικότερα σε επόμενη ενότητα.

- ***Simple Authentication and Security Layer – SASL***: διατυπώνει μεθόδους για προσθήκη υπηρεσιών αυθεντικοποίησης σε υπάρχοντα πρωτόκολλα βασισμένα σε σύνδεση (*connection – based protocols*), παρουσιάζεται αναλυτικότερα σε επόμενη ενότητα.

- ***Integrated Windows Authentication – IWA***: το λειτουργικό σύστημα Windows παρέχει εναλλακτικές μεθόδους – πρωτόκολλα αυθεντικοποίησης, κάποια από τα οποία είναι γενικότερα πρότυπα και κάποια αποτελούν αποκλειστικά πρωτόκολλα των Windows. Αναλυτικότερη παρουσίαση των διαφορετικών λύσεων γίνεται σε επόμενη ενότητα.

- ***(Point – to – Point) Challenge-Handshake Authentication Protocol – CHAP***: πρωτόκολλο αυθεντικοποίησης για τη σύνδεση ενός χρήστη σε έναν παροχέα πρόσβασης στο Internet. Έχει ευρεία εφαρμογή στις Dial – up συνδέσεις στο Internet [76, 129].

- ***MS-CHAP v1 & v2***: είναι η Microsoft «διάλεκτος» του PPP CHAP προτύπου για την παροχή των μεθόδων αυθεντικοποίησης της Microsoft σε δίκτυα με απομακρυσμένους σταθμούς εργασίας [162, 163].

- ***Password Authentication Protocol – PAP***: πρωτόκολλο αυθεντικοποίησης το οποίο σχεδιάστηκε για χρήση με το πρωτόκολλο σύνδεσης *Point – to – Point (PPP)*, κυρίως για τη Dial – up σύνδεση Clients στο Internet. Δεν εφαρμόζει κάποια κρυπτογράφηση των αποστελλόμενων passwords και δε θεωρείται ιδιαίτερα ασφαλές [76, 129].

- ***Extensible Authentication Protocol – EAP***: χρησιμοποιείται σε Client/Server συνδέσεις για τη διαπραγμάτευση προσδιορισμού του πρωτοκόλλου αυθεντικοποίησης που θα χρησιμοποιηθεί μεταξύ του συνδεόμενου Client και του Server [1].

- ***Hypertext Transfer Protocol – HTTP*** [26]: βασικό πρωτόκολλο μετάδοσης «ιστοσελίδων» του Internet το οποίο παρέχει ένα βασικό μηχανισμό αυθεντικοποίησης username/ password. Χρησιμοποιείται συχνά σε συνδυασμό με το πρωτόκολλο ασφαλούς μετάδοσης SSL/TLS [17] για την κρυπτογραφημένη αποστολή των passwords πάνω από το δίκτυο. Το SSL/TLS μπορεί να χρησιμοποιήσει πιστοποιητικά Δημοσίου Κλειδιού και να παρέχει PKI αυθεντικοποίηση του Client στο Server και αντίστροφα. Ο συνδυασμός των HTPP και SSL/TLS χαρακτηρίζεται "*secure HTTP – HTTPS*".

- ***S/Key***: παλαιότερος μηχανισμός αυθεντικοποίησης ο οποίος στηρίζεται στη μέθοδο Hashing του password, ώστε να αποτρέπονται οι «επιθέσεις» *Replay Attacks* [39, 40].

Τα πρωτόκολλα που ανήκουν στο πεδίο ενδιαφέροντος της παρούσας εργασίας είναι όσα παρουσιάζουν χρησιμότητα για την αυθεντικοποίηση χρηστών σε δικτυακές εφαρμογές και μεγάλη διάδοση στα συστήματα Διαχείρισης Ταυτοτήτων:

2.3.1.1 Kerberos

Το *Kerberos* είναι μία γενική, κατανεμημένη υπηρεσία αυθεντικοποίησης η οποία επιτρέπει σε μία διεργασία πελάτη (*client*) που εκτελείται για λογαριασμό μίας κύριας οντότητας (*principal* – ένας χρήστης ή ένας server) να αποδείξει την ταυτότητά της (αυθεντικοποιηθεί) σε μία οντότητα επιβεβαίωσης (έναν άλλο server). Το πρωτόκολλο *Kerberos* αναπτύχθηκε στα μέσα του 1980 ως μέρος του έργου "*Athena*" του Massachusetts Institute of Technology (M.I.T.), ενώ η τρέχουσα έκδοση του *Kerberos* είναι η v5 η οποία περιγράφεται στο RFC 4120 [96]. Ο πρώτιστος στόχος του πρωτοκόλλου ήταν η ενίσχυση της διαδικασίας αυθεντικοποίησης σε ένα ανοιχτό δίκτυο client – server με κρυπτογραφικές μεθόδους έναντι της συνήθους χρήσης των απλών passwords τα οποία όταν μεταφέρονται αυτούσια στο δίκτυο είναι εύκολος στόχος σε κάθε «ακροατή» του δικτύου [95]. Η γενική ιδέα είναι ότι μέσα στα πλαίσια ενός δικτύου η αυθεντικοποίηση κάθε χρήστη δε θα πρέπει να γίνεται από καθένα server δικτυακής υπηρεσίας ξεχωριστά, αλλά από ένα έμπιστο, «τρίτο μέρος» μέσα στο ίδιο δίκτυο, το *Key Distribution Center* (*KDC*). Το *KDC* περιέχει τα μυστικά κλειδιά των χρηστών και των servers του δικτύου τα οποία έχουν καταχωρηθεί σε αυτό με αυστηρά ασφαλή διαδικασία (είτε εκτός δικτύου από διαχειριστές των συστημάτων είτε από ασφαλή γραμμή). Ο χρήστης, επομένως, αποδεικνύει την ταυτότητά του σε ένα server με την παρουσίαση ενός «εισιτηρίου» ("ticket") το οποίο έχει πάρει από τον *KDC* και περιέχει ένα προσωρινό κλειδί με το οποίο μπορούν ο χρήστης και ο server να κωδικοποιούν τα μηνύματα που ανταλλάσσουν για όσο διαρκέσει η επικοινωνία τους [62]. Το *Kerberos* χρησιμοποιεί κρυπτογράφηση «Συμμετρικού Κλειδιού», καθώς σε κάθε επικοινωνία χρησιμοποιείται ένα μοναδικό, αμοιβαίως γνωστό κλειδί για την κωδικοποίηση/αποκωδικοποίηση των μηνυμάτων, ενώ για την κρυπτογράφηση των μηνυμάτων χρησιμοποιείται το πρότυπο *Data Encryption Standard* (*DES*) [91, 95]. Αναλυτικότερα, τα βασικά χαρακτηριστικά του πρωτοκόλλου είναι [62, 95, 96, 133]:

- Το *KDC* του *Kerberos* διατηρεί τα προσωπικά κλειδιά όλων των μερών του δικτύου (clients & servers). Για τους χρήστες, το συγκεκριμένο κλειδί μπορεί να θεωρηθεί ότι είναι το password τους. Το τμήμα του *KDC* το οποίο διαχειρίζεται την αρχική κλήση ενός client για αυθεντικοποίηση ονομάζεται *Authentication Server* (*AS*).

- Κάθε χρήστης (client) ο οποίος θέλει να χρησιμοποιήσει μία δικτυακή υπηρεσία σε έναν server (ή αλλιώς verifier) αποστέλλει ένα μήνυμα στον *AS* του *Kerberos*. Το μήνυμα περιέχει το όνομα του client, το όνομα του server και ένα "*nonce*", μία «χρονοσφραγίδα» (*timestamp*) ή μία οποιαδήποτε άλλη τιμή που μπορεί να προσδιορίσει μοναδικά τη συγκεκριμένη κλήση (μήνυμα 1 στην Εικόνα 16).

- Με τη λήψη της αίτησης του client ο *AS* δημιουργεί ένα τυχαίο κλειδί κρυπτογράφησης ($K_{c,v}$) το οποίο θα έχει προσωρινή ισχύ για την επικοινωνία του client και του verifier, γι αυτό και ονομάζεται κλειδί συνόδου (*session key*). Ο *AS* δημιουργεί ένα μήνυμα απάντησης προς τον client το οποίο αποτελείται από δύο τμήματα. Το πρώτο τμήμα περιέχει το *session key* ($K_{c,v}$) και τα υπόλοιπα δεδομένα της αρχικής αίτησης του client (το "*nonce*", το όνομα του verifier κλπ) και αποστέλλεται κρυπτογραφημένο με το κλειδί του client (K_c). Το δεύτερο τμήμα περιέχει το αποκαλούμενο "εισιτήριο" ("*ticket*") του client για την πρόσβαση στον verifier ($T_{c,v}$), το οποίο περιέχει το *session key* και τις ημερομηνίες έναρξης και λήξης ισχύος του "*ticket*". Το "*ticket*" $T_{c,v}$ αποστέλλεται στον client κρυπτογραφημένο με το μυστικό κλειδί του verifier (K_v) το οποίο «γνωρίζει» μόνο ο verifier και ο *AS*. Με αυτό τον τρόπο δεν είναι δυνατή η αποκρυπτογράφηση και ανάγνωση του περι-

εχομένου του "*ticket*" από κάποιον τρίτο, άρα και η «πλαστογράφηση» της ταυτότητας του client (μήνυμα 2 στην Εικόνα 16).

- Με την παραλαβή της απάντησης του *AS* ο client αποκρυπτογραφεί το πρώτο τμήμα με τη χρήση του δικού του κλειδιού και αφού ελέγξει την ορθότητα του "*nonce*" που λαμβάνει σε σχέση με αυτό που είχε στείλει, αποθηκεύει το *session key* και το κρυπτογραφημένο "*ticket*" του δευτέρου τμήματος της απάντησης. Στη συνέχεια ο client αποστέλλει την καθεαυτού αίτηση αυθεντικοποίησης στον verifier – server. Η αίτηση περιλαμβάνει αυτούσιο το κρυπτογραφημένο "*ticket*" $T_{c,v}$ του προηγούμενου βήματος και ένα τμήμα κρυπτογραφημένο με το κοινό *session key*. Το συγκεκριμένο τμήμα ονομάζεται *authenticator* και περιλαμβάνει πληροφορίες για την ταυτότητα του client: ένα καινούριο *timestamp*, ένα προαιρετικό – εναλλακτικό *session key* και ένα checksum[ii] όλων αυτών (μήνυμα 3 στην Εικόνα 16).

- Ο verifier – server παραλαμβάνει το παραπάνω μήνυμα και αποκρυπτογραφεί πρώτο το κρυπτογραφημένο "*ticket*" με τη χρήση του μυστικού κλειδιού του (K_v). Από το περιεχόμενο του "*ticket*" διαβάζει το *session key* και την ταυτότητα του client. Με την εφαρμογή του *session key* ο verifier αποκρυπτογραφεί το τμήμα *authenticator* του μηνύματος όπου με τη βοήθεια του checksum ελέγχει την ακεραιότητα του μηνύματος, άρα και την ορθότητα του *session key* με το οποίο γίνεται η αποκρυπτογράφηση, αλλά και με τη βοήθεια του *timestamp* ελέγχει αν το μήνυμα είναι πρόσφατο. Συνήθως, υπάρχει ένα χρονικό «παράθυρο» των πέντε λεπτών από την τρέχουσα ώρα του verifier μέσα στο οποίο πρέπει να ανήκει το *timestamp*. Σε αυτό το σημείο ο verifier έχει επιβεβαιώσει ότι ο client ο οποίος ονοματίζεται στο κρυπτογραφημένο "*ticket*" κατέχει το ίδιο *session key* που επίσης περιέχεται στο "*ticket*". Ο μόνος τρόπος για να συμβεί αυτό είναι ο client να μπορέσει να αποκρυπτογραφήσει με το μυστικό κλειδί του την απάντηση του *AS* στο μήνυμα 2 παραπάνω. Εφόσον το μυστικό κλειδί που χρησιμοποιεί ο client είναι ίδιο με αυτό που διατηρεί ο *AS* για το συγκεκριμένο όνομα client, ο verifier λογικά μπορεί να εμπιστεύεται τον client που του έστειλε τη συγκεκριμένη αίτηση αυθεντικοποίησης.

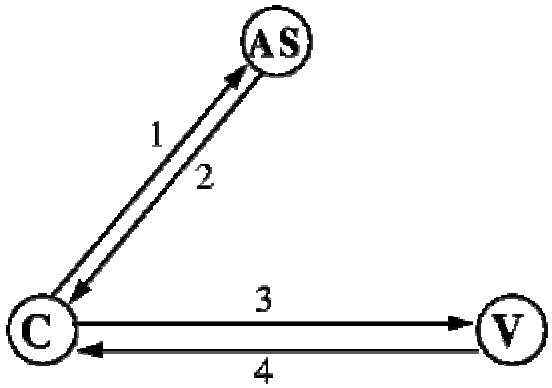
  Προαιρετικά, ο client μπορεί να ζητήσει την αυθεντικοποίηση και του verifier – server, οπότε ο verifier αποστέλλει με τη σειρά του μήνυμα (μήνυμα 4) το οποίο περιέχει βασικά το *timestamp* που είχε στείλει ο client στο μήνυμα 3 και το κρυπτογραφεί με το *session key*. Ο client, στη συνέχεια, αποκρυπτογραφεί το μήνυμα του verifier με τη χρήση του *session key* και ελέγχοντας την ορθότητα του *timestamp* που περιέχεται σε σχέση με αυτό που είχε στείλει μπορεί να είναι σίγουρος για την ταυτότητα του verifier, γιατί το *session key* θα μπορούσε να εξαχθεί από τον verifier στο μήνυμα 3 παραπάνω μόνο αν αυτός διέθετε το μυστικό κλειδί το οποίο διατηρεί ο «έμπιστος» *AS* για τον συγκεκριμένο verifier.

- Στην παρακάτω εικόνα οι συμβολισμοί είναι:
  - *c, v*: τα δικτυακά ονόματα των client και verifier, αντίστοιχα.
  - K_c, K_v, $K_{c,v}$: το κλειδί του client, του verifier και το session key client – verifier, αντίστοιχα.

[ii] Μία μορφή ελέγχου της ορθής μετάδοσης δεδομένων. Αποτελεί επιπλέον πληροφορία πέρα από το κυρίως πακέτο των δεδομένων και προκύπτει από την εφαρμογή πράξεων στα bits που αντιστοιχούν στα δεδομένα. Η ίδια πράξη εφαρμόζεται στα δεδομένα κατά την παραλαβή τους και το συγκεκριμένο αποτέλεσμα συγκρίνεται με αυτό που μεταδόθηκε μαζί με τα δεδομένα.

- $\{\ldots\}K_c$: κρυπτογραφημένο τμήμα δεδομένων με χρήση του κλειδιού K_c.
- $T_{c,v}$: "ticket" το οποίο περιέχει τα απαραίτητα στοιχεία κρυπτογραφημένης επικοινωνίας client – verifier.
- *ts, ck*: *timestamp* και checksum, αντίστοιχα.

Πηγή: [95]



1. as_req: c, v, $time_{exp}$, n
2. as_rep: $\{K_{c,v}, v, time_{exp}, n, \ldots\}K_c$, $\{T_{c,v}\}K_v$
3. ap_req: $\{ts, ck, K_{subsession}, \ldots\}K_{c,v}$ $\{T_{c,v}\}K_v$
4. ap_rep: $\{ts\}K_{c,v}$ (optional)

$T_{c,v} = K_{c,v}$, c, $time_{exp}$ ...

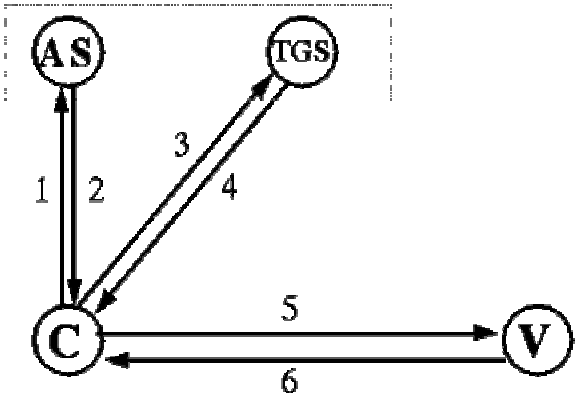
Εικόνα 16: Βασική (Απλοποιημένη) Λειτουργία του Πρωτοκόλλου *Kerberos*

- Στο *Kerberos* η μετάδοση όλων των μηνυμάτων μεταξύ των clients και του *KDC* γίνεται με TCP/IP πακέτα ή UDP/IP πακέτα και οι *KDC* servers περιμένουν αιτήσεις συνήθως στο port 88.

- Η παραπάνω βασική λειτουργικότητα του πρωτοκόλλου έχει το μειονέκτημα ότι ο χρήστης (client) πρέπει να εισάγει και χρησιμοποιήσει το προσωπικό του κλειδί – password (K_c) προς τον *AS* κάθε φορά που επιχειρεί την προσπέλαση ενός server μέσα στο δίκτυο. Η συγκεκριμένη επανάληψη περιέχει κινδύνους για την ασφάλεια του κλειδιού και δυσχεραίνει την ευχρηστία του πρωτοκόλλου. Γι αυτό το λόγο το πρωτόκολλο προβλέπει έναν ακόμα server, τον *Ticket Granting Server – TGS* ο οποίος έχει πρόσβαση στη Βάση Δεδομένων των κλειδιών του *KDC* και αναγνωρίζει κάθε χρήστη με ένα ειδικό *Ticket - Granting Ticket – TGT* και όχι με το μυστικό κλειδί K_c. Η αλλαγή, επομένως, στη βασική λειτουργία του πρωτοκόλλου είναι ότι ο client επικοινωνεί μόνο μία φορά με τον *AS*, κατά την πρώτη προσπάθεια επικοινωνίας με κάποιον verifier. Από αυτή την επικοινωνία ο client αποκτά ένα κλειδί επικοινωνίας με τον *TGS* το οποίο μαζί με τα στοιχεία του εσωκλείονται στο *TGT*. Το καθένα *TGT* έχει περιορισμένη χρονική ισχύ, συνήθως 8 ώρες. Από αυτή τη στιγμή και μετά ο client επικοινωνεί με τον *TGS* κάθε φορά που πρόκειται να προσπελάσει ένα νέο verifier και με το κοινό *session key* που περιέχεται στο *TGT* διαβάζει την κρυπτογραφημένη απάντηση του *TGS* στην οποία περιέχεται το *session key* της επικοινωνίας του με τον συγκεκριμένο verifier. Με αυτό τον τρόπο δε χρησιμοποιείται το

μυστικό κλειδί του client παρά μόνο κατά την πρώτη σύνδεσή του. Η πλήρης λειτουργικότητα, επομένως, του *Kerberos* περιγράφεται σχηματικά στην παρακάτω Εικόνα, στην οποία τα μηνύματα 1 & 2 ανταλλάσσονται μόνο κατά την πρώτη είσοδο του client στο σύστημα, τα μηνύματα 3 & 4 ανταλλάσσονται κάθε φορά που ο client πρόκειται να αυθεντικοποιηθεί από ένα νέο verifier, το μήνυμα 5 αποστέλλεται προκειμένου να αυθεντικοποιηθεί τελικά ο client από τον verifier, ενώ το μήνυμα 6 αποστέλλεται προαιρετικά όταν απαιτηθεί και η αυθεντικοποίηση του verifier. Στην παρακάτω εικόνα οι νέοι συμβολισμοί είναι το $T_{c,tgs}$: το *Ticket-Granting Ticket*, και το $K_{c,tgs}$: το *session key* επικοινωνίας client – *TGS*.

Πηγή: [95]



1. as_req: c, tgs, $time_{exp}$, n
2. as_rep: $\{K_{c,tgs}, tgs, time_{exp}, n, ...\}K_c$, $\{T_{c,tgs}\}K_{tgs}$
3. tgs_req: $\{ts, ...\}K_{c,tgs}$ $\{T_{c,tgs}\}K_{tgs}$, v, $time_{exp}$, n
4. tgs_rep: $\{K_{c,v}, v, time_{exp}, n, ...\}K_{c,tgs}$, $\{T_{c,v}\}K_v$
5. ap_req: $\{ts, ck, K_{subsession}, ...\}K_{c,v}$ $\{T_{c,v}\}K_v$
6. ap_rep: $\{ts\}K_{c,v}$ (optional)

Εικόνα 17: Πλήρης (Απλοποιημένη) Λειτουργία του Πρωτοκόλλου *Kerberos*

- Το δίκτυο το οποίο ελέγχεται από μία εγκατάσταση του *Kerberos* αποτελεί μία αυτόνομη περιοχή ευθύνης (*realm*) του *Kerberos*. Είναι δυνατή η αυθεντικοποίηση ενός client από έναν *Kerberos* server σε ένα άλλο *realm* εκτός του δικού του, εφόσον οι *TGS* των δύο *realms* έχουν προ-ρυθμισμένα *inter-realm* κλειδιά. Όταν ο client επιχειρεί να προσπελάσει έναν server σε ένα απομακρυσμένο *realm* μπορεί να αποκτήσει ένα *TGT* από το δικό του *realm* το οποίο όμως θα είναι κρυπτογραφημένο και με το *inter-realm* κλειδί το οποίο «γνωρίζουν» μόνο οι δύο *TGS* των δύο *realms*. Με αυτό τον τρόπο ο απομακρυσμένος *TGS* επιβεβαιώνει ότι ο συγκεκριμένος client προέρχεται από ένα «έμπιστο» *realm* και του επιστρέφει ένα *session key* επικοινωνίας με τον απομακρυσμένο server. Σε περίπτωση που δύο *realms* δεν μοιράζονται αμοιβαία *inter-realm* κλειδιά είναι δυνατή η αυθεντικοποίηση χρηστών ενός από το άλλο, εφόσον υπάρχουν ενδιάμεσα *realms* τα οποία διατηρούν *inter-realm* κλειδιά με τα συγκεκριμένα *realms*. Με αυτό τον τρόπο δημιουργείται ένα μονοπάτι αυθεντικοποίησης από «έμπιστα» *realms* τα οποία μεταβιβάζουν την εμπιστοσύνη τους από το αρχικό *realm* στο τελικό. Επιπροσθέτως, πολλά *realms* μπορούν να οργανωθούν ιεραρχικά, ώστε καθένα από αυτά να διατηρεί ένα *inter-realm* κλειδί με τον «πατέρα» του και διαφορετικά κλειδιά για καθέναν από τους άμεσους απογόνους του. Συ-

νεπώς, είναι πιο εύκολος ο προσδιορισμός του μονοπατιού αυθεντικοποίησης κάθε φορά που απαιτείται επικοινωνία μεταξύ των *realms*. Η συγκεκριμένη ιδιότητα του πρωτοκόλλου *Kerberos* χρησιμοποιείται για την οικοδόμηση «έμπιστων» σχέσεων (*Trust*) μεταξύ ταυτοτήτων διαφορετικών οργανισμών.

- Το *Kerberos* καθορίζει μία διαδικασία αποκλειστικά για αυθεντικοποίηση και όχι για κανόνες – δικαιώματα πρόσβασης στις δικτυακές υπηρεσίες (*authorization*). Είναι δυνατή, όμως, η συνεργασία του με εξωτερικές εφαρμογές ελέγχου πρόσβασης. Επιπροσθέτως, το *Kerberos* αποτυγχάνει να εξασφαλίσει ασφαλή αυθεντικοποίηση όταν η Βάση Δεδομένων του *KDC* δεν είναι αρκετά προστατευμένη και τα passwords των χρηστών δεν είναι εμπιστευτικά ή είναι πολύ μικρά ή αυτονόητα, οπότε ένας έμπειρος «εισβολέας» μπορέσει και τα αναπαράγει.

- Μία επέκταση του πρωτοκόλλου, όπως εφαρμόζεται από τα "server" λειτουργικά συστήματα της Microsoft (Windows 2000, Windows Server 2003 κλπ), μπορεί να συνδυάσει τη βασική λειτουργία του *Kerberos* με Κρυπτογράφηση Δημοσίου Κλειδιού και τη χρήση *Hard Crypto Tokens* όπως μία Smart Card. Συγκεκριμένα, ο χρήστης κατά την έναρξη της διαδικασίας αυθεντικοποίησής του εισάγει την Smart Card του στον ανάλογο Card Reader και εισάγει τον προσωπικό του κωδικό (PIN). Το λειτουργικό σύστημα «διαβάζει» από την κάρτα το Πιστοποιητικό του Δημόσιου Κλειδιού που διατηρεί ο χρήστης και το αποστέλλει στο *KDC* του *Kerberos*. Το *KDC* εντοπίζει το χρήστη, μέσω του κωδικού του ονόματος στο Πιστοποιητικό, μέσα στην υπηρεσία καταλόγου που διατηρεί και ελέγχει την αξιοπιστία του *CA* που «υπογράφει» το Πιστοποιητικό. Εφόσον εντοπιστεί το Δημόσιο Κλειδί του *CA* εξάγεται το Δημόσιο Κλειδί του χρήστη από το Πιστοποιητικό, το *KDC* δημιουργεί ένα προσωρινό *session key* και ένα *TGT* για το συγκεκριμένο χρήστη, τα οποία και κωδικοποιεί με το Δημόσιο Κλειδί του χρήστη. Με αυτό τον τρόπο εξασφαλίζεται ότι μόνο ο κάτοχος του αντίστοιχου Ιδιωτικού Κλειδιού, δηλαδή ο έγκυρος χρήστης, θα μπορέσει να αποκρυπτογραφήσει το συγκεκριμένο μήνυμα άρα και να εξάγει το προσωρινό *session key*. Συνεπώς, το *KDC* αποστέλλει το κρυπτογραφημένο μήνυμα στον client (Smart Card) όπου αποκρυπτογραφείται και προκύπτει το *session key* και το *TGTs* τα οποία χρησιμοποιεί ο χρήστης για να επικοινωνήσει με το *Kerberos* και να αυθεντικοποιηθεί στην επιθυμητή εφαρμογή με τα επόμενα κλασικά βήματα του πρωτοκόλλου [14].

2.3.1.2 Integrated Windows Authentication – IWA

Η μέθοδος αυθεντικοποίησης *Integrated Windows Authentication – IWA* είναι μία από τις ενσωματωμένες μεθόδους του λειτουργικού συστήματος Microsoft *Windows* και το προηγούμενο όνομά της ήταν *NTLM* (*Windows **NT** **L**an **M**anager*), το οποίο είναι γνωστό και ως *Windows NT Challenge/Response Authentication Protocol* [84]. Η μέθοδος *IWA* δεν αποτελεί συγκεκριμένο πρωτόκολλο, αλλά προτεινόμενη επιλογή αυθεντικοποίησης ενός web site το οποίο λειτουργεί σε περιβάλλον Windows κατά τη ρύθμιση των υπηρεσιών Web Server των Windows, τις *Internet Information Services – IIS* [83]. Το *IWA* καθορίζει μία συγκεκριμένη διαδικασία αυθεντικοποίησης ενός χρήστη, ο οποίος επιχειρεί πρόσβαση σε προστατευόμενους πόρους, με πρώτη προτεραιότητα την εφαρμογή του πρωτοκόλλου *Kerberos 5* για την αυθεντικοποίηση του χρήστη. Στην περίπτωση όπου δεν υπάρχει εγκατάσταση του πρωτοκόλλου *Kerberos 5* στο σύστημα ή οι παράμετροι των συστημάτων δεν επιτρέπουν την πλήρη λειτουργία του πρωτοκόλλου, τότε το *IWA* επιλέγει ως πρωτόκολλο αυθεντικοποίησης το

NTLM (*Windows* ***NT Lan Manager***). Η διαδικασία του ελέγχου της παρούσας κατάστασης του συστήματος και της επιλογής του κατάλληλου τρόπου αυθεντικοποίησης γίνεται μέσω του μηχανισμού «διαπραγμάτευσης» "***S****imple and* ***P****rotected GSSAPI*[iii] ***Nego****tiation Mechanism – SPNEGO*" (RFC 4178 [161]). Το *IWA* ξεκινάει τη λειτουργία του με τον έλεγχο από την πλευρά του server της ύπαρξης κατάλληλων αρχείων του λειτουργικού συστήματος Windows στο σταθμό του client. Σε περίπτωση επιτυχίας, αυτές οι πληροφορίες χρησιμοποιούνται για την αυθεντικοποίηση του χρήστη χωρίς την προτροπή στο χρήστη για την εισαγωγή username & password του. Ειδικότερα, στην περίπτωση όπου ο χρήστης έχει εισέλθει στο σύστημα ως εγκεκριμένος χρήστης του *Domain*, τότε είναι αναγνωρίσιμος από το *IWA* χωρίς την επανάληψη εισαγωγής των στοιχείων του κάθε φορά που χρησιμοποιεί έναν πόρο του συστήματος (Single Sign-On). Στην περίπτωση που δεν υπάρχουν στον client προσωρινά αποθηκευμένα δεδομένα χρήστη για την αναγνώρισή του, προβάλλεται στο χρήστη σχετικό παράθυρο εισαγωγής των σωστών username & password του. Τα γενικότερα χαρακτηριστικά της λειτουργίας του *IWA* είναι [84]:

- Το πρωτόκολλο *Kerberos 5* σε ένα περιβάλλον Windows απαιτεί την εγκατάσταση του server τμήματος του πρωτοκόλλου (*KDC*) στον *Domain Controller*, ενώ τα στοιχεία και τα απαραίτητα μυστικά κλειδιά των χρηστών και υπηρεσιών του δικτύου είναι εγκατεστημένα στο *Active Directory* του *Domain*. Το δεύτερο γεγονός καθιστά δύσκολη την εφαρμογή του πρωτοκόλλου σε υπηρεσίες που προσπελαύνονται από χρήστες του Internet, καθώς κάθε χρήστης ή υπηρεσία στο δίκτυο πρέπει να αποκτήσει ένα λογαριασμό (*User Principal Name - UPN* ή *Service Principal Name – SPN*, αντίστοιχα) στο *Active Directory*.

- Τόσο ο client όσο και server οι οποίοι πρόκειται να επικοινωνήσουν πρέπει να έχουν ασφαλή πρόσβαση στο *KDC* του *Kerberos* και να είναι συστήματα συμβατά με το *Active Directory*.

- Το πρωτόκολλο *NTLM* αποκαλείται "*Challenge/Response*" πρωτόκολλο και χρησιμοποιείται για συμβατότητα του *IWA* με συστήματα που έχουν λειτουργικό σύστημα Windows NT 4.0 και παλαιότερο ή για συστήματα που λειτουργούν αυτόνομα (*stand-alone*). Τα στοιχεία του χρήστη που απαιτεί το *NTLM* είναι το *Domain Name*, το username και το password. Ο χρήστης επιχειρεί σύνδεση είτε απευθείας στον *Domain Controller* είτε σε ένα server του δικτύου οπότε ο *Domain Controller* αναλαμβάνει την αυθεντικοποίηση εκ μέρους του συγκεκριμένου server. Τα βήματα της αυθεντικοποίησης σύμφωνα με το *NTLM* είναι:

  1. Στον client του χρήστη υπολογίζεται μία «*ψηφιακή σύνοψη*» ("*Hash*")[iv] του password του χρήστη και αυτή η τιμή χρησιμοποιείται στο εξής για την αυθεντικοποίηση του χρήστη, με αποτέλεσμα το αυτούσιο password να μην είναι απαραίτητο να διατηρείται στη μνήμη του client Ηλ. Υπολογιστή.

[iii] *Generic Security Services Application Programming Interface – GSSAPI* (RFC2743 [75]): είναι ένα πρότυπο API με βάση το οποίο μπορούν να υλοποιηθούν πρωτόκολλα αυθεντικοποίησης. Οι ακριβείς λεπτομέρειες της διαδικασίας αυθεντικοποίησης «κρύβονται» από το γενικό API και μία εφαρμογή που καλεί τις υπηρεσίες ασφάλειας μέσω του *GSSAPI* δεν χρειάζεται να ξαναγραφεί όταν αλλάζουν οι λεπτομέρειες αυτών των υπηρεσιών. Γνωστότερη υλοποίησή του είναι το *Kerberos*. Δεν υποστηρίζει Εξουσιοδότηση (authorization) και προϋποθέτει client/server περιβάλλον. Η έκδοση του πρωτοκόλλου στα λειτουργικά συστήματα της Microsoft ονομάζεται "*Security Support Provider Interface – SSPI*" [86].

[iv] Ο συγκεκριμένος υπολογισμός γίνεται με τη μέθοδο Hashing. Στην έκδοση *NTLMv2* χρησιμοποιούνται οι αλγόριθμοι *LANMAN Hash* και *HMAC-MD5 Hash*

2. Ο client στέλνει στον server το username του χρήστη χωρίς κρυπτογράφηση.
3. Ο server δημιουργεί έναν τυχαίο αριθμό 16-byte ο οποίος καλείται «*πρόκληση*» ("*challenge*") ή "*nonce*" και το στέλνει πίσω στον client.
4. Ο client κρυπτογραφεί το *challenge* με κλειδί το *Hash* του βήματος 1 και στέλνει το αποτέλεσμα στον server. Το συγκεκριμένο αποτέλεσμα ονομάζεται «*απάντηση*» ("*response*").
5. Ο server αποστέλλει στον *Domain Controller* (εφόσον είναι διαφορετικοί) το username του client, το *challenge* που στάλθηκε στον client και την απάντηση που δέχθηκε από τον client.
6. Ο *Domain Controller* χρησιμοποιεί το username του client για να ανασύρει το υπολογισμένο *Hash* του password του client από τη Βάση Δεδομένων του υποσυστήματος *Security Account Manager*. Με το συγκεκριμένο *Hash* ως κλειδί κρυπτογραφεί το *challenge* που έστειλε ο server στο βήμα 3.
7. Το αποτέλεσμα της παραπάνω κρυπτογράφησης συγκρίνεται με την «*απάντηση*» που έστειλε ο client στο βήμα 4. Στην περίπτωση που η σύγκριση οδηγήσει σε ισότητα, τότε ο client θεωρείται έγκυρος και επιτρέπεται η είσοδός του στο σύστημα.

Το *NTLM* θεωρείται λιγότερο ασφαλές σε σχέση με το *Kerberos* ως πρωτόκολλο αυθεντικοποίησης στα πλαίσια ενός *Domain*, καθώς το δεύτερο εφαρμόζει την αρχή της αυθεντικοποίησης μέσω μίας τρίτης, «έμπιστης αρχής», αλλά το *NTLM* βρίσκει ακόμα πολλές εφαρμογές σε διαφορετικές συνθέσεις τοπικών δικτύων [28].

❖ Δύο σημαντικά μειονεκτήματα του *IWA* είναι:

1. Η εφαρμογή του *IWA* απαιτεί έκδοση Internet Explorer 2 και μετά.
2. Το *IWA* δεν μπορεί να λειτουργήσει πάνω από συνδέσεις μέσω Proxy.

Εξαιτίας των παραπάνω λόγων και του γεγονότος ότι το πρωτόκολλο *Kerberos 5* λειτουργεί με λογαριασμούς του *Active Directory*, άρα όλοι οι χρήστες πρέπει να έχουν το δικό τους *Active Directory* λογαριασμό, το *IWA* εφαρμόζεται για αυθεντικοποίηση στα πλαίσιο ενός Windows Intranet, όπου οι παραπάνω απαιτήσεις είναι εφικτές και ελεγχόμενες.

Τα λειτουργικά συστήματα Windows προτείνουν εκτός από το μηχανισμό *IWA* και άλλες μεθόδους αυθεντικοποίησης χρηστών από τον *IIS*, με εφαρμογές όμως κυρίως σε τοπικά Intranet [84]:

❖ <u>*Digest Authentication*</u>: αποτελεί εξέλιξη της βασικής διαδικασίας εισαγωγής username & password του client, καθώς το password του χρήστη δεν μεταδίδεται αυτούσιο στον server αλλά αυτό που μεταδίδεται είναι η «*ψηφιακή σύνοψη*» ("*Hash*" ή "*Message Digest*") των στοιχείων του χρήστη με βάση τον Hashing αλγόριθμο *MD5* (RFC 1321 [116]). Τα στοιχεία που συνδυάζονται για την παραγωγή του *Hash* είναι τα username, password και το όνομα του Domain. Σύμφωνα με τον αλγόριθμο *MD5* το παραγόμενο *Hash* των αρχικών στοιχείων είναι τέτοιο ώστε είναι αδύνατη η αντίστροφη αναπαραγωγή του αρχικού μηνύματος. Τα στοιχεία του καθενός χρήστη πρέπει να είναι αποθηκευμένα μη – κρυπτογραφημένα σε αντίστοιχους *Active Directory* λογαριασμούς, ώστε με την παραλαβή των κρυπτογραφημένων στοιχείων του client ο server εφαρμόζει την ίδια ενέρ-

γεια στα στοιχεία που διατηρεί στο *Active Directory* και αποφασίζει για την αυθεντικότητα του χρήστη ανάλογα με το αποτέλεσμα της σύγκρισης των δύο κρυπτογραφήσεων.

- *Advanced Digest Authentication*: αποτελεί επέκταση της παραπάνω διαδικασίας η οποία ισχύει μόνο στον Windows Server 2003. Η βασική διαφορά των δύο διαδικασιών είναι ότι στην *Advanced* τα στοιχεία των χρηστών αποθηκεύονται στο *Active Directory* του Windows Server 2003 με προεπιλεγμένη την εφαρμογή αλγορίθμου *Hashing*. Επομένως, στο *Active Directory* αποθηκεύονται οι *MD5* τιμές που προκύπτουν από τα προσωπικά στοιχεία των χρηστών, έτσι ώστε να είναι αδύνατη η αναπαραγωγή των αρχικών στοιχείων, ακόμα και αν υποκλαπούν τα δεδομένα του *Active Directory*.

- *.NET Passport Authentication*: κάθε νέο web site μπορεί να προγραμματιστεί, μέσω της πλατφόρμας *.NET*, ώστε να συνδέεται με την κεντρική υπηρεσία *Microsoft Passport Network* για την αυθεντικοποίηση των χρηστών του. Μόλις, επομένως, ο χρήστης εισέρχεται σε τέτοιο web site, ο έλεγχος μεταφέρεται στην κεντρική υπηρεσία του *Microsoft Passport Network* όπου ο χρήστης εισάγει τα προσωπικά του στοιχεία όπως τα έχει καταχωρήσει κατά την εγγραφή του στην υπηρεσία *Microsoft Passport*. Οι χρήστες με αυτό τον τρόπο διατηρούν έναν ενιαίο τρόπο πρόσβασης σε όλα τα sites τα οποία προτείνουν ως μέθοδο αυθεντικοποίησης το *.NET Passport*. Επίσης, μετά την πρώτη είσοδο του χρήστη σε μία τέτοια υπηρεσία, δεν είναι απαραίτητη η επαν-εισαγωγή των στοιχείων του κάθε φορά που εισέρχεται σε μία άλλη υπηρεσία που χρησιμοποιεί το *.NET Passport*, καθώς δημιουργείται στον client ένα προσωρινό Cookie[v] το οποίο χρησιμοποιείται για την αυθεντικοποίησή του (Single Sign-On). Η αποστολή των στοιχείων του χρήστη κατά την αυθεντικοποίησή του στην ειδική φόρμα του *Microsoft Passport Network* γίνεται σε «ασφαλές κανάλι» με τη χρήση του πρωτοκόλλου SSL/TLS.

- *Forms Based Authentication*: λειτουργεί κατά τον ίδιο με τον παραπάνω τρόπο με τη διαφορά ότι ο προγραμματιστής του site πρέπει να δημιουργήσει ο ίδιος την κατάλληλη φόρμα καταχώρησης των προσωπικών στοιχείων του χρήστη στη θέση της κεντρικής υπηρεσίας *Microsoft Passport Network*. Επίσης, είναι ευθύνη του ίδιου του site η προστασία της αποστολής των προσωπικών στοιχείων χρηστών με ασφαλείς μεθόδους, ο τρόπος αποθήκευσης και διαχείρισης των προσωπικών στοιχείων των χρηστών και ο τρόπος ελέγχου – σύγκρισης των καταχωρημένων στοιχείων. Η πλατφόρμα *.NET* παρέχει πολλές διευκολύνσεις στους προγραμματιστές για την εισαγωγή της συγκεκριμένης μεθόδου αυθεντικοποίησης στα sites τα οποία αναπτύσσουν στο περιβάλλον των Windows [82].

2.3.1.3 Security Assertion Markup Language – SAML

Η γλώσσα *SAML – Security Assertion Markup Language* αναπτύχθηκε από την Επιτροπή *Security Services Technical Committee* του Οργανισμού *OASIS - Organization Advancement of Structured Information Standards*[vi] και αποτελεί ένα μηχανισμό βασισμένο σε XML για την

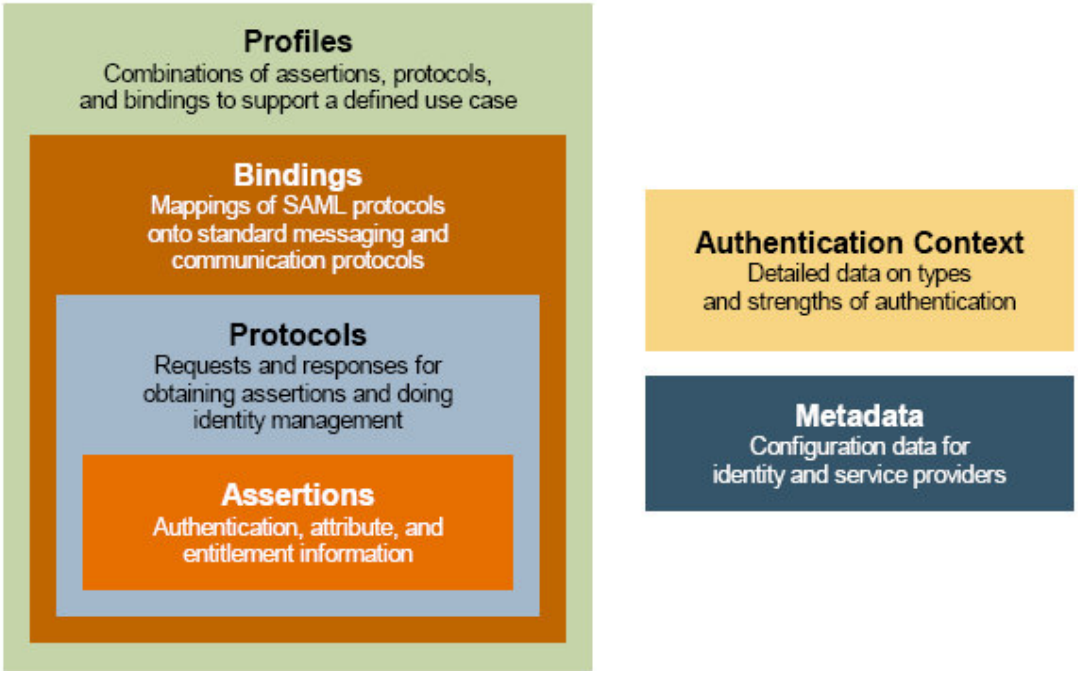
[v] *Cookie*: Ένας γενικός μηχανισμός με τον οποίο το server τμήμα μίας web σύνδεσης μπορεί να χρησιμοποιήσει για την αποθήκευση και ανάκτηση πληροφοριών σχετικών με το client μέρος της σύνδεσης. Ένα μικρό αρχείο δεδομένων κατάστασης του client στο οποίο ο server μπορεί να καταγράψει ό,τι πληροφορία είναι χρήσιμη στη λειτουργικότητα μιας συγκεκριμένης web εφαρμογής ή υπηρεσίας [94].

[vi] Ο Οργανισμός *OASIS* [100] είναι μία σύμπραξη εταιριών και οργανισμών με αντικείμενο την ανάπτυξη, δημοσίευση και υποστήριξη τεχνολογικών προτύπων για το e-Business.

επικοινωνία πληροφοριών αυθεντικοποίησης και δικαιωμάτων. Η *SAML* επιδιώκει να απομονώσει με πρότυπο τρόπο τις ενδεχομένως διαφορετικές τεχνολογίες Διαχείρισης Ταυτοτήτων σε συνεργαζόμενους οργανισμούς και να πραγματοποιήσει την ανταλλαγή αυτών των πληροφοριών υλοποιώντας *Federated Identity Management* «σενάρια». Διατυπώθηκε ως πρότυπο του *OASIS* το Νοέμβριο 2002 με την έκδοση *SAML V1.0* και το Σεπτέμβριο 2003 δημοσιεύτηκε η έκδοση *SAML V1.1*, ενώ η τρέχουσα έκδοση *SAML V2.0* αποσκοπεί στην πλήρη σύγκλιση και ικανοποίηση των απαιτήσεων για "*Identity Federations*" μεταξύ οργανισμών [104].

Η *SAML* ορίζει δομικά τμήματα (modules) τα οποία, όταν συνδυαστούν κατάλληλα, μπορούν να υποστηρίξουν πολλές περιπτώσεις αυθεντικοποίησης. Οι συγκεκριμένες δομές αφορούν στη μετάδοση δεδομένων ταυτοτήτων, αυθεντικοποίησης, εξουσιοδότησης χρηστών μεταξύ οργανισμών οι οποίοι έχουν εγκαθιδρύσει σχέση εμπιστοσύνης (*Trust*). Ο οργανισμός που βεβαιώνει (*assert*) τα στοιχεία ταυτότητας κάποιας οντότητας – αντικειμένου (*Principal*) ονομάζεται *Asserting Party*, ενώ ο οργανισμός που εμπιστεύεται (*rely*) αυτή τη βεβαίωση προς επεξεργασία ονομάζεται *Relying Party*. Ένας *Principal*, τα στοιχεία του οποίου μεταφέρονται μεταξύ των δύο *Parties,* μπορεί να είναι ένας χρήστης ή ένας υπολογιστής. Ανάλογα με το είδος της πληροφορίας που μεταδίδεται, τα *Parties* που επικοινωνούν αποκτούν διακριτούς ρόλους οι οποίοι καθορίζουν τους τύπους των μηνυμάτων που θα μεταδοθούν καθώς και το ακριβές περιεχόμενό τους. Για παράδειγμα, σε ένα σενάριο αυθεντικοποίησης χρήστη υπάρχουν δύο ρόλοι: αυτός του *Identity Provider* (*IdP*) για το *Asserting Party*, ο οποίος κατέχει τα δεδομένα της ταυτότητα ενός χρήστη, και αυτός του *Service Provider* (*SP*) για το *Relying Party*, ο οποίος κατέχει τις προσπελάσιμες υπηρεσίες. Τα δομικά συστατικά της *SAML* φαίνονται στην παρακάτω Εικόνα και είναι [104]:

Πηγή: [104]



Εικόνα 18: Δομικά Συστατικά της *SAML*

- *Assertions*: Η βασική δομή της *SAML* είναι η *Assertion* με την οποία δηλώνονται όλες οι βασικές πληροφορίες που αφορούν ένα *Principal* και πρόκειται να αποσταλούν από ένα *Asserting Party* μετά από κλήση ενός *Relying Party*. Το περιεχόμενο ενός *Assertion* ορίζεται από το αντίστοιχο XML Σχήμα της *SAML* και συνήθως είναι δεδομένα για το *Principal*, τις *προϋποθέσεις* (*conditions*) κάτω από τις οποίες μπορεί να επικυρωθεί η *Assertion* και συγκεκριμένες *δηλώσεις* (*statements*) οι οποίες μπορεί να είναι τριών ειδών:
  - *Δηλώσεις Αυθεντικοποίησης (Authentication Statements)*: δημιουργούνται από το *Asserting Party* το οποίο έχει ήδη αυθεντικοποίηση το *Principal*, οπότε και αναφέρει τη μέθοδο της αυθεντικοποίησης και το χρόνο πραγματοποίησής της.
  - *Δηλώσεις Ιδιοτήτων (Attribute Statements)*: περιλαμβάνουν χαρακτηριστικά γνωρίσματα ή ιδιότητες του *Principal* (πχ ο χρήστης «Χ» έχει βαθμίδα πιστωτικής κάρτας «Χρυσή»)
  - *Δηλώσεις για Αποφάσεις Εξουσιοδότησης (Authorization decision statements)*: Προσδιορίζουν όσα ο *Principal* έχει δικαίωμα να εκτελέσει - πραγματοποιήσει (πχ ο χρήστης «Χ» επιτρέπεται να αγοράσει το αντικείμενο «Υ»)
- *Protocols*: Η *SAML* ορίζει μία σειρά από πρωτόκολλα *αίτησης/απάντησης* (*request/response*) σύμφωνα με τα οποία υλοποιείται η ανταλλαγή των *Assertions* μεταξύ των *Parties*:
  - *Authentication Request Protocol*: ορίζει τον τρόπο με τον οποίο ένας *Principal* ή ένα *Relying Party* μπορεί να ζητήσει *Assertion* με δεδομένα αυθεντικοποίησης ή/και εξουσιοδότησης.
  - *Single Logout Protocol*: ορίζει το μηχανισμό τερματισμού όλων των sessions που συνδέονται με κάποιον *Principal* και ουσιαστικά την αποσύνδεσή του από τα *Parties* που είχε συνδεθεί.
  - *Assertions Query and Request Protocol*: ορίζει ένα σύνολο ερωτημάτων (queries) με βάση τα οποία μπορούν να αναζητηθούν *Assertions*. Με τη φόρμα *Request Form* του πρωτοκόλλου μπορεί να ερωτηθεί ένα *Asserting Party* για ένα *Assertion* με βάση το ID του *Assertion*, ενώ με τη φόρμα *Query Form* του πρωτοκόλλου ένα *Relying Party* μπορεί αναζητήσει *Assertions* με βάση συγκεκριμένο θέμα ή τύπο εντολών.
  - *Artifact Resolution Protocol*: ορίζει το μηχανισμό επικοινωνίας μεταξύ *Parties* με τον οποίο αυτό που μεταδίδεται είναι μόνο μία αναφορά σε ένα *SAML* μήνυμα (*artifact*) χωρίς να μεταφέρεται το ίδιο αυτούσιο. Ο παραλήπτης της αναφοράς χρησιμοποιεί το πρωτόκολλο *Artifact Resolution Protocol* για να ζητήσει από τον αποστολέα να αποστείλει το πλήρες μήνυμα που αντιστοιχεί στη συγκεκριμένη αναφορά (*artifact*).
  - *Name Identifier Management Protocol*: ορίζει το μηχανισμό για την αλλαγή του προσδιοριστικού ονόματος ενός *Principal* και η συγκεκριμένη αίτηση μπορεί να ξεκινήσει από οποιοδήποτε *Party*.
  - *Name Identifier Mapping Protocol*: ορίζει το μηχανισμό της αντιστοίχισης ενός ονόματος *SAML Principal* σε ένα άλλο με βάση συγκεκριμένους κανόνες. Για παράδειγμα, είναι δυνατό ένας *Service Provider* να ζητήσει από έναν *Identity Provider* να του δώσει στοιχεία για ένα χρήστη τα οποία μπορεί να χρησιμοποιήσει για την πρό-

σβαση του χρήστη σε έναν άλλο *Service Provider* με άλλο όνομα χρήστη, επομένως αυτό το εναλλακτικό όνομα πρέπει να συνδεθεί με αυτό που ήδη διατηρεί.

- *Bindings*: καθορίζουν τον τρόπο με τον οποίο θα μεταδοθούν τα μηνύματα των διάφορων *SAML* πρωτοκόλλων μέσω των πρωτοκόλλων μετάδοσης σε χαμηλότερο επίπεδο. Για την έκδοση *SAML V2.0* ισχύει:
  - *HTTP Redirect Binding*: μετάδοση *SAML* μηνυμάτων μέσω της λειτουργίας ανακατεύθυνσης (*Redirect*) του πρωτοκόλλου HTTP.
  - *HTTP Post Binding*: μετάδοση *SAML* μηνυμάτων μέσω του περιεχομένου ενός αντικειμένου φόρμας (*control*) του πρωτοκόλλου HTTP.
  - *HTTP Artifact Binding*: μετάδοση ενός *artifact* του πρωτοκόλλου *Artifact Resolution Protocol* με τη χρήση HTTP μηχανισμών, είτε ως περιεχόμενο ενός αντικειμένου φόρμας (*control*), είτε ως παράμετρος στη διεύθυνση URL του Web Browser του χρήστη.
  - *SAML SOAP Binding*: μετάδοση μέσω πρωτοκόλλου SOAP 1.1[vii]
  - *Reverse SOAP (PAOS) Binding*: εξειδικευμένη περίπτωση στην οποία ορίζεται ο τρόπος για έναν HTTP client να μπορεί να λειτουργήσει και με βάση το πρωτόκολλο SOAP.
  - *SAML URI Binding*: ορίζει τον τρόπο απόκτησης ενός *SAML Assertion* μέσω της ανάλυσης ενός ονόματος σύμφωνου με την προδιαγραφή URI[viii].
- *Profiles*: καθορίζουν τον τρόπο με τον οποίο *SAML Assertions*, *Protocols* και *Bindings* μπορούν να συνδυαστούν για την ικανοποίηση συγκεκριμένων «σεναρίων» χρήσης. Για την έκδοση *SAML V2.0* ισχύει:
  - *Web Browser SSO Profile*: ορίζει τον τρόπο χρήσης του *Authentication Request Protocol* και των μηνυμάτων *SAML Response* και *Assertions* για την επίτευξη Single Sign-On σε έναν απλό Web Browser. Καθορίζει τον τρόπο χρήσης των μηνυμάτων σε σχέση και με τα *Bindings*: *HTTP Redirect*, *HTTP POST* και *HTTP Artifact*.
  - *Enhanced Client and Proxy (ECP) Profile*: ορίζει ένα εξειδικευμένο SSO *Profile* όπου γίνεται χρήση του *Reverse SOAP (PAOS) Binding*.
  - *Identity Provider Discovery Profile*: ορίζει ένα μηχανισμό όπου ένας *Service Provider* μπορεί να μάθει τους *Identity Providers* τους οποίους ένας χρήστης έχει προηγουμένως επισκεφτεί.
  - *Single Logout Profile*: ορίζει το μηχανισμό χρήσης των *Bindings*: *SOAP*, *HTTP Redirect*, *HTTP POST* και *HTTP Artifact* με το πρωτόκολλο *SAML Single Logout Protocol*.

[vii] *Simple Object Access Protocol – SOAP*: είναι ένα W3C πρωτόκολλο μετάδοσης πληροφοριών σε ένα κατανεμημένο περιβάλλον. Βασίζεται στην XML και κάθε μήνυμα αποτελείται από τρία μέρη: έναν «φάκελο» ο οποίος ορίζει το πλαίσιο για την περιγραφή του περιεχομένου του μηνύματος, κανόνες περιγραφής τύπων δεδομένων της εφαρμογής που αποστέλλει το μήνυμα και μία σύμβαση για την αναπαράσταση Απομακρυσμένων Κλήσεων Υπο-προγραμμάτων (*Remote Procedure Calls*) [154].

[viii] *Uniform Resource Identifier – URI*: είναι μία σειρά από χαρακτήρες η οποία προσδιορίζει μόναδικά έναν πόρο συνήθως μέσα στο World Wide Web (RFC 3986 [9])

- *Assertion Query/Request Profile*: ορίζει το μηχανισμό χρήσης του πρωτοκόλλου *SAML Query and Request Protocol* για την απόκτηση *Assertions,* μέσω του *SOAP Binding*.
- *Artifact Resolution Profile*: ορίζει το μηχανισμό χρήσης του πρωτοκόλλου *Artifact Resolution Protocol* για την απόκτηση ενός μηνύματος το οποίο αναφέρεται από ένα *artifact*, μέσω του *SOAP Binding*.
- *Name Identifier Management Profile*: ορίζει τον τρόπο χρήσης του πρωτοκόλλου *Name Identifier Management Protocol* με τα *Bindings*: *SOAP*, *HTTP Redirect*, *HTTP POST* και *HTTP Artifact*.
- *Name Identifier Mapping Profile*: ορίζει τον τρόπο χρήσης του πρωτοκόλλου *Name Identifier Mapping Protocol* με το *SOAP Binding*.

❖ *Metadata*: αποτελεί συμπληρωματικό τμήμα μίας *SAML* επικοινωνίας καθώς περιγράφει τον τρόπο με τον οποίο δύο οντότητες θα ορίσουν και θα επικοινωνήσουν τις πληροφορίες διαμόρφωσης της μελλοντικής ανταλλαγής *SAML* μηνυμάτων. Παραδείγματα τέτοιων πληροφοριών παραμετροποίησης είναι η υποστήριξη από μία οντότητα ενός συγκεκριμένου *SAML Binding*, η υποστήριξη συγκεκριμένης *Public Key Infrastructure* (*PKI*) τεχνολογίας κλπ. Τα *metadata* ορίζονται με τη μορφή σχήματος της XML.

❖ *Authentication Context*: περιλαμβάνει τον προαιρετικό ορισμό λεπτομερειών για τις τεχνολογίες αυθεντικοποίησης που χρησιμοποιεί ο *Identity Provider*, οι οποίες λεπτομέρειες είναι πιθανό να ζητηθούν από τον *Service Provider*, επιπρόσθετα του *Assertion*, προκειμένου να ελέγξει το επίπεδο ασφάλειας των τεχνικών που εμπιστεύεται. Η συγκεκριμένη προδιαγραφή ορίζει το XML Schema περιγραφής όλων των πιθανών πληροφοριών σχετικά με το μηχανισμό αυθεντικοποίησης που χρησιμοποιείται. Η *SAML* δεν απαιτεί τη χρήση κάποιου συγκεκριμένου μηχανισμού, πρωτοκόλλου ή μεθόδου αυθεντικοποίησης των χρηστών, αλλά παρέχει τη δυνατότητα στην καθεμιά υλοποίησή της να μεταφέρει πληροφορίες για τους εφαρμοζόμενους μηχανισμούς αυθεντικοποίησης, μέσα σε ένα *Assertion* (πχ κάποιος μηχανισμός *multi-factor authentication*), ώστε ο *Resource Provider* να τις συνυπολογίσει στη λήψη της απόφασης αποδοχής ή όχι του χρήστη. Οι πληροφορίες που μπορεί η *SAML* να περιγράψει για τις εφαρμοζόμενες τεχνολογίες αυθεντικοποίησης χωρίζονται στις κατηγορίες:

- *Identification*: πληροφορίες που περιγράφουν τους μηχανισμούς και διαδικασίες που χρησιμοποιεί το σύστημα αυθεντικοποίησης για την αρχική σύνδεση μίας οντότητας με μία ταυτότητα (πχ με φυσική παρουσία του *Principal* κατά τη διαδικασία κλπ).
- *Technical Protection*: πληροφορίες που περιγράφουν τους τρόπους με τους οποίους τα «μυστικά» δεδομένα της αυθεντικοποίησης (όσα πρέπει να γνωρίζει ή κατέχει ο *Principal* για να αυθεντικοποιηθεί) προστατεύονται ώστε να παραμένουν μυστικά (πχ που είναι αποθηκευμένο το κάθε κλειδί, πως προστατεύεται το Δημόσιο Κλειδί, πως προστατεύεται το Ιδιωτικό Κλειδί, αν το κλειδί απαιτεί ενεργοποίηση κλπ)
- *Operational Protection*: πληροφορίες που περιγράφουν τους τρόπους με τους οποίους η αρχή αυθεντικοποίησης ελέγχει την ασφάλεια των εφαρμοζόμενων διαδικασιών (πχ καταγραφή συμβάντων, audits ασφαλείας κλπ).
- *Authentication Method*: πληροφορίες που περιγράφουν τους μηχανισμούς με τους οποίους ο χρήστης που περιέχεται στο καθένα *Assertion* αυθεντικοποιείται από την

αρχή αυθεντικοποίησης (πχ χρήση password, Smart Card, άλλου Hardware *Token* κλπ).

- *Governing Agreements*: πληροφορίες που περιγράφουν το νομικό πλαίσιο που ενδεχομένως να συνοδεύει τη διαδικασία αυθεντικοποίησης ή/και τη σχετιζόμενη τεχνολογική υποδομή της αυθεντικοποίησης.

Συμπερασματικά, τα *Assertions* είναι τα τμήματα της *SAML* τα οποία περιέχουν την ουσιώδη πληροφορία, ενώ τα υπόλοιπα τμήματα αφορούν τις τεχνολογίες μετάδοσης των μηνυμάτων. Ένα τυπικό παράδειγμα *Assertion* σύμφωνο με το XML Σχήμα της *SAML* φαίνεται στην παρακάτω Εικόνα:

Πηγή: [104]

```
 1: <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
 2:   Version="2.0"
 3:   IssueInstant="2005-01-31T12:00:00Z">
 4:   <saml:Issuer Format=urn:oasis:names:SAML:2.0:nameid-format:entity>
 5:     http://www.example.com
 6:   </saml:Issuer>
 7:   <saml:Subject>
 8:     <saml:NameID
 9:       Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">
10:         j.doe@example.com
11:     </saml:NameID>
12:   </saml:Subject>
13:   <saml:Conditions
14:     NotBefore="2005-01-31T12:00:00Z"
15:     NotOnOrAfter="2005-01-31T12:10:00Z">
16:   </saml:Conditions>
17:   <saml:AuthnStatement
18:     AuthnInstant="2005-01-31T12:00:00Z" SessionIndex="67775277772">
19:     <saml:AuthnContext>
20:       <saml:AuthnContextClassRef>
21:         urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
22:       </saml:AuthnContextClassRef>
23:     </saml:AuthnContext>
24:   </saml:AuthnStatement>
25: </saml:Assertion>
```

Εικόνα 19: Ενδεικτικό Παράδειγμα *Assertion* της *SAML*

- Στην πρώτη γραμμή δηλώνεται το XML Namespace του *SAML Assertion* με το πρόθεμα "*saml*".

- Οι γραμμές 2 έως 6 παρέχουν πληροφορίες για τη χρησιμοποιούμενη έκδοση της *SAML*, την ημερομηνία έκδοσης του *Assertion* και αυτόν που το εξέδωσε.

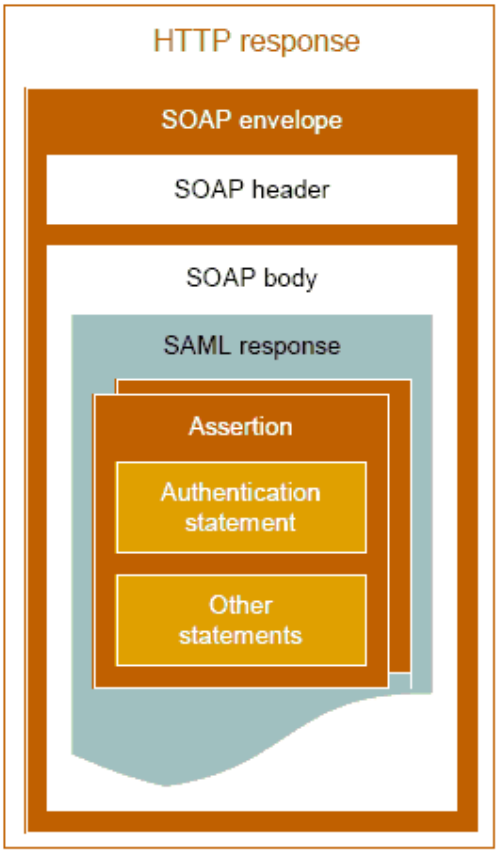
- Οι γραμμές 7 έως 12 περιέχουν πληροφορίες για το *Subject* (*principal*) του *Assertion*. Στη γραμμή 10 ορίζεται η τιμή του ονόματος του *Subject* ("*j.doe@example.com*"), το οποίο όπως δηλώνεται στη γραμμή 9 είναι τύπου "*emailAddress*". Η *SAML* περιέχει πολλούς εναλλακτικούς τύπους ονομάτων για τα *Subjects*, όπως: e-mail διεύθυνση, πιστοποιητικά του X.509, ονόματα σύμφωνα με την ονοματολογία των Windows Domains, ονόματα σύμφωνα με το *Kerberos* κλπ

- Στις γραμμές 14 έως 15 δηλώνεται η περίοδος ισχύος του *Assertion*.

- Στις γραμμές 17 έως 24 προσδιορίζεται ο τρόπος και ο χρόνος αυθεντικοποίησης του *Subject*: χρήση password το οποίο στάλθηκε με προστατευμένο τρόπο μέσω του πρωτοκόλλου SSL. Η *SAML* περιέχει τρόπους περιγραφής μεγάλου αριθμού προκαθορισμένων μηχανισμών αυθεντικοποίησης (*Authentication Contexts*) οι οποίοι περιέχουν διαφορετικούς συνδυασμούς μεθόδων, πρωτοκόλλων και συσκευών αυθεντικοποίησης.

Μετά το σχηματισμό του *Assertion* το καθένα *Party* ετοιμάζει το μήνυμα που θα μεταδοθεί στο άλλο *Party*. Στις περιπτώσεις όπου τα δύο *Parties* υποστηρίζουν το πρωτόκολλο SOAP τότε επιλέγεται το *Binding SOAP-over HTTP* για την ανταλλαγή των μηνυμάτων. Στο κυρίως *Assertion* προστίθενται πληροφοριακά δεδομένα που απαιτεί η *SAML* με αποτέλεσμα το σχηματισμό του *SAML* μηνύματος (*Request* ή *Response*). Αυτό το μήνυμα ενσωματώνεται στο τμήμα *Body* ενός SOAP μηνύματος το οποίο μαζί με ένα SOAP *Header* συνιστούν το *Envelope* του SOAP μηνύματος. Όλο το SOAP μήνυμα ενσωματώνεται για την τελική μετάδοση σε μία απάντηση HTTP, η οποία φαίνεται σχηματικά στην παρακάτω Εικόνα.

Πηγή: [104]



Εικόνα 20: Σχηματική Παράσταση *SAML* μηνύματος *Απάντησης* (*Response*) που μεταδίδεται μέσα σε ένα SOAP μήνυμα

Η ενδεικτική σύνταξη ενός SOAP μηνύματος που περιέχει μία *SAML Απάντηση* (*Response*) φαίνεται στην παρακάτω Εικόνα.

Πηγή: [104]

```
 1: <?xml version="1.0" encoding="UTF-8"?>
 2: <env:Envelope  xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
 3:   <env:Body>
 4:     <samlp:Response
 5:       xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
 6:       xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
 7:       Version="2.0"
 8:       ID="i92f8b5230dc04d73e93095719d191915fdc67d5e"
 9:       IssueInstant="2005-11-10T06:47:42.000Z"
10:       InResponseTo="f0485a7ce95939c093e3de7b2e2984c0">
11:       <saml:Issuer>http://www.AirlineInc.com</saml:Issuer>
12:       <samlp:Status>
13:         <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
14:       </samlp:Status>
15:                    ...SAML assertion...
16:     </samlp:Response>
17:   </env:Body>
18: </env:Envelope>
```

Εικόνα 21: XML Σύνταξη *SAML* μηνύματος *Απάντησης* (*Response*) που μεταδίδεται μέσα σε ένα SOAP μήνυμα

Η ασφαλής μετάδοση των *SAML* μηνυμάτων είναι υψίστης σημασίας καθώς το *Relying Party* εμπιστεύεται κάθε φορά χωρίς περαιτέρω έλεγχο κάθε *Assertion* που δέχεται από το *Asserting Party*. Αυτό σημαίνει ότι τα μηνύματα πρέπει να προστατεύονται τόσο από πιθανή «υποκλοπή» όσο και από "*Man-in-the-middle*" *Attack*. Η *SAML* προϋποθέτει ότι μεταξύ των *Parties* υπάρχει ήδη εγκατεστημένος μηχανισμός «εμπιστοσύνης» ο οποίος στηρίζεται συνήθως σε *Public Key Infrastructure* (*PKI*) και προτείνει, χωρίς να επιβάλει, συγκεκριμένους μηχανισμούς προστασίας των μηνυμάτων στον ορισμό κάθε *SAML Binding*, ενδεικτικά:

- Στις περιπτώσεις όπου απαιτείται ακεραιότητα και προστασία των μηνυμάτων, προτείνεται η χρήση του HTTP πάνω από το SSL/TLS (HTTPS).
- Στις περιπτώσεις όπου ένα *Relying Party* ζητάει ένα *Assertion* από ένα *Asserting Party*, απαιτείται η αυθεντικοποίηση και των δύο μερών με τη χρήση των SSL/TLS ή με τη χρήση ψηφιακών υπογραφών.
- Στις περιπτώσεις όπου ένα *SAML* μήνυμα με ένα *Assertion* μεταφέρεται στο *Relying Party* μέσω του Web Browser ενός χρήστη (για παράδειγμα, με το *Binding HTTP POST*), απαιτείται η εξασφάλιση της ακεραιότητας του μηνύματος με την εφαρμογή ψηφιακών υπογραφών σύμφωνα με την προδιαγραφή XML Signature[ix]

2.3.1.4 Simple Authentication and Security Layer – SASL

Το *SASL* (*Simple Authentication and Security Layer*) (RFC 4422 [78]) δεν αποτελεί πρωτόκολλο αλλά ένα πλαίσιο παροχής υπηρεσιών αυθεντικοποίησης στα προσανατολισμένα σε σύνδεση (connection – oriented) πρωτόκολλα μετάδοσης δεδομένων στο Internet, μέσω των τρεχόντων μηχανισμών αυθεντικοποίησης. Παρέχει, επομένως, μία δομημένη διεπαφή μεταξύ των πρωτοκόλλων και των μηχανισμών αυθεντικοποίησης, όπως φαίνεται στην παρακάτω

[ix] Προδιαγραφή *XML-Signature Syntax and Processing* του W3C η οποία καθορίζει το συντακτικό και τους κανόνες επεξεργασίας των Ψηφιακών Υπογραφών με γλώσσα XML [153].

εικόνα, ενώ υποστηρίζει και την περαιτέρω ασφαλή μετάδοση των δεδομένων, μετά την αρχική αυθεντικοποίηση.

Πηγή: [78]

```
SMTP        LDAP     XMPP    Other protocols
   \          |        |        /
    \         |        |       /
       SASL abstraction layer
    /         |        |       \
   /          |        |        \
EXTERNAL    GSSAPI   PLAIN   Other mechanisms
```

Εικόνα 22: Σχηματική Αναπαράσταση Λειτουργίας του *SASL*

Με το *SASL*, συνεπώς, υλοποιείται η απαραίτητη «αφαίρεση» των λεπτομερειών πρωτοκόλλων και μηχανισμών, ώστε τα νέα πρωτόκολλα να χρησιμοποιούν τους υπάρχοντες μηχανισμούς και οι νέοι μηχανισμοί να μπορούν να χρησιμοποιηθούν από υπάρχοντα πρωτόκολλα. Το επίπεδο «αφαίρεσης» δεν λειτουργεί, όμως, στις λεπτομέρειες του καθενός μηχανισμού αυθεντικοποίησης με αποτέλεσμα τα δεδομένα που απαιτεί κάθε μηχανισμός να διαφέρουν.

Για την «αφαίρεση» των διαδικασιών αυθεντικοποίησης το *SASL* προϋποθέτει ότι η πολύ γενική αλληλουχία μηνυμάτων κατά τη φάση αυθεντικοποίησης σε ένα client/server περιβάλλον είναι [78]:

Client: Αίτηση ανταλλαγής μηνυμάτων αυθεντικοποίησης
Server: Αρχική «Πρόκληση»
Client: Αρχική «Απάντηση»
<Εναλλαγή επιπρόσθετων μηνυμάτων «Πρόκλησης»/«Απάντησης»>
Server: Αποτέλεσμα αυθεντικοποίησης

Επομένως, η υλοποίηση του *SASL* από τη μεριά ενός πρωτοκόλλου απαιτεί τον καθορισμό συγκεκριμένων παραμέτρων τις οποίες πρέπει να γνωρίζει το *SASL* για να επικοινωνεί με το συγκεκριμένο πρωτόκολλο, όπως η εφαρμοζόμενη μέθοδος προσδιορισμού του μηχανισμού αυθεντικοποίησης, η μέθοδος ανταλλαγής των μηνυμάτων «Πρόκλησης»/«Απάντησης» με το server, η μέθοδος ενημέρωσης για το αποτέλεσμα της αυθεντικοποίησης κλπ. Από την πλευρά των μηχανισμών, πρέπει να καθοριστεί ένα σύνολο από «Προκλήσεις»/«Απαντήσεις» με τις οποίες παρέχει ο μηχανισμός τις υπηρεσίες αυθεντικοποίησης.

Η τρέχουσα υλοποίηση του *SASL* υποστηρίζει τους μηχανισμούς αυθεντικοποίησης [78]:

- *GSSAPI* (RFC 2743 [75])
- *EXTERNAL* (RFC 4422 [78])
- *CRAM-MD5* (RFC 2195 [61])
- *ANONYMOUS* (RFC 4505 [155])
- *One Time Password* (RFC 2444 [97])

- *GSS-SPNEGO* (RFC 4178 [161])
- *PLAIN* (RFC 4616 [160])
- *SECURID* (RFC 2808 [99])
- *NTLM* των Microsoft Windows
- *Novell Modular Authentication Services LOGIN*
- *Novell Modular Authentication Services AUTHEN*
- *DIGEST-MD5* (RFC 2831 [66])
- *9798-U-RSA-SHA1-ENC* (RFC 3163 [164])
- *9798-M-RSA-SHA1-ENC* (RFC 3163 [164])
- *9798-U-DSA-SHA1* (RFC 3163 [164])
- *9798-M-DSA-SHA1* (RFC 3163 [164])
- *9798-U-ECDSA-SHA1* (RFC 3163 [164])
- *9798-M-ECDSA-SHA1* (RFC 3163 [164])
- *KERBEROS_V5*

Τα πρωτόκολλα ανωτέρου επιπέδου τα οποία υποστηρίζουν το *SASL* είναι τα [78]:

- *BEEP - Blocks Extensible Exchange Protocol* (RFC 3080 [117])
- *IMAP - Internet Message Access Protocol* (RFC 3501 [15])
- *LDAP – Lightweight Directory Access Protocol* (RFC 4510 [156])
- *POP – Post Office Protocol* (RFC 1939 [90])
- *SMTP - Simple Mail Transfer Protocol* (RFC 2821 [60])
- *XMPP - Extensible Messaging and Presence Protocol* (RFC 3920 [121])

2.3.2 Ηλεκτρονικοί Κατάλογοι Χρηστών

Οι Κατάλογοι (*Directories*) γενικά είναι συλλογές όμοιων πληροφοριών οργανωμένων με τρόπο λογικό και ιεραρχικό. Για παράδειγμα, ο τηλεφωνικός κατάλογος περιέχει ένα σύνολο ονομάτων οργανωμένων με αλφαβητική ταξινόμηση, για καθένα από τα οποία υπάρχει κατα-

χωρημένος ένας αριθμός τηλεφώνου, μία διεύθυνση και πιθανώς μία ιδιότητα. Οι ηλεκτρονικοί κατάλογοι είναι γενικά μία παρόμοια δομή σε ηλεκτρονική μορφή με τη διαφορά ότι εκτός από ανθρώπους – χρήστες καταχωρούνται στον κατάλογο και διάφοροι πόροι Πληροφοριακών Συστημάτων (servers, Η/Υ, routers, web services, εκτυπωτές κλπ).

2.3.2.1 Lightweight Directory Access Protocol – LDAP

Το πρώτο πρότυπο Ηλεκτρονικού Καταλόγου είναι το Χ.500 της *ITU* (*International Telecommunication Union*)[x] το οποίο μαζί με άλλα πρότυπα της σειράς Χ.500 κάλυπταν όλες τις παραμέτρους των Ηλεκτρονικών Καταλόγων. Παρ' όλη την πληρότητα της σειράς Χ.500 η εφαρμογή της δεν ήταν εύκολη καθώς οι απαιτήσεις σε υπολογιστική ισχύ ήταν μεγάλες. Γι αυτό το λόγο, στα τέλη του '90, προτάθηκε μία μικρότερη («ελαφρύτερη») έκδοση του Χ.500, το *Lightweight Directory Access Protocol – LDAP* το οποίο υλοποιούσε ένα υποσύνολο των προδιαγραφών του Χ.500. Η τρέχουσα έκδοση του *LDAP* είναι η v3 η οποία περιγράφεται από μία σειρά RFC's που απαριθμούνται στο RFC 4510 [156] και είναι[xi]:

- RFC 4511 - *LDAP*: The Protocol [124].
- RFC 4512 - *LDAP*: Directory Information Models [157].
- RFC 4513 - *LDAP*: Authentication Methods and Security Mechanisms [41].
- RFC 4514 - *LDAP*: String Representation of Distinguished Names [158].
- RFC 4515 - *LDAP*: String Representation of Search Filters [130].
- RFC 4516 - *LDAP*: Uniform Resource Locator [131].
- RFC 4517 - *LDAP*: Syntaxes and Matching Rules [67].
- RFC 4518 - *LDAP*: Internationalized String Preparation [159].
- RFC 4519 - *LDAP*: Schema for User Applications [122].

Το *LDAP* λειτουργεί με βάση το μοντέλο Client/Server, όπου κάθε client ο οποίος επιθυμεί την εκτέλεση μίας λειτουργίας καταλόγου, συνδέεται στον *LDAP* server, αποστέλλει το μήνυμα – αίτησή του και ο server εκτελεί την ενέργεια επιστρέφοντας προαιρετικά κάποιο αποτέλεσμα. Για την μετάδοση των μηνυμάτων στον server χρησιμοποιείται το TCP πρωτόκολλο και κατά σύμβαση το port 389. Οι εγγραφές του καταλόγου οργανώνονται ιεραρχικά σε δεντρική μορφή συνιστώντας το *Directory Information Tree – DIT*, όπου κάθε κόμβος αποτελεί και μία εγγραφή. Οι συνδέσεις των κόμβων μέσα στο δέντρο καθορίζουν τις σχέσεις μεταξύ των εγγραφών του καταλόγου (οι σχέσεις παιδιού/γονέα στο δέντρο χρησιμοποιούνται για την εξαγωγή συμπερασμάτων για τα αντικείμενα που αντιπροσωπεύουν).

[x] ITU: ο παλαιότερος διεθνής οργανισμός, ιδρύθηκε την 17/05/1865 στο Παρίσι και ο κύριος σκοπός του είναι η διατύπωση διεθνών προτύπων στην τηλεπικοινωνία [56].
[xi] Η σύντομη περιγραφή του *LDAP* στην παρούσα εργασία βασίζεται στα συγκεκριμένα RFC's

Κάθε εγγραφή (*entry*) του καταλόγου είναι ένα σύνολο από τιμές ιδιοτήτων (*attributes*) τα οποία περιγράφουν την αναπαριστώμενη οντότητα. Το καθένα *attribute* χαρακτηρίζεται από μία περιγραφή, δηλαδή έναν τύπο ο οποίος καθορίζει το πλήθος και το είδος των τιμών που μπορούν να του αποδοθούν και έναν αριθμό προαιρετικών επιλογών για το συγκεκριμένο *attribute*. Επομένως, ανάλογα με τον τύπο ενός *attribute* αυτό μπορεί να δεχθεί περισσότερες της μίας τιμές, όλες όμως πρέπει να είναι διαφορετικές μεταξύ τους. Το όνομα κάθε εγγραφής είναι πάντα σχετικό με τα ονόματα των ανωτέρω εγγραφών της (πρόγονοι). Το σχετικό όνομα, επομένως, μίας εγγραφής, το οποίο καλείται *Relative Distinguished Name – RDN* είναι ένα μη ταξινομημένο σύνολο από *attributes* της εγγραφής μαζί με τη μοναδική τιμή τους. Ενδεικτικά παράδειγμα *RDN's* είναι τα παρακάτω (με πλάγια γραφή είναι τα ονόματα των *attributes*):

1. *UID*=12345

2. *OU*=Engineering

3. *CN*=Kurt Zeilenga+*L*=Redwood Shores

όπου το *UID* είναι το *attribute* που αντιστοιχεί στο username ενός χρήστη, το *OU* είναι το *attribute* που αντιστοιχεί στο τμήμα που απασχολείται ένας χρήστης, το *CN* αντιστοιχεί στο πλήρες όνομα του χρήστη και το *L* αντιστοιχεί σε πληροφορία τοποθεσίας. Το *RDN* κάθε κόμβου που έχει τον ίδιο «πατέρα» στο δέντρο του καταλόγου πρέπει να είναι μοναδικό. Κάθε εγγραφή έχει επίσης ένα μοναδικό σε όλον τον κατάλογο όνομα το οποίο καλείται *Distinguished Name – DN* και είναι η συνένωση του *RDN* της εγγραφής με το *DN* του κόμβου – «πατέρα» του στο δέντρο. Ενδεικτικά παραδείγματα από *DN* εγγραφών είναι (με πλάγια γραφή είναι τα ονόματα των *attributes*):

1. ***UID*=nobody@example.com**,*DC*=example,*DC*=com

2. ***CN*=John Smith,OU=Sales**,*O*=ACME Limited,*L*=Moab,*ST*=Utah,*C*=US

όπου τα τμήματα με τους έντονους χαρακτήρες είναι τα *RDN's* των αντίστοιχων κόμβων. Συνεπώς, μία πλήρης εγγραφή σε έναν *LDAP* κατάλογο μπορεί να έχει τη μορφή:

dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 555 6789
telephoneNumber: +1 555 1234
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top

όπου το *objectClass* είναι η κλάση στην οποία ανήκει η συγκεκριμένη εγγραφή και καθορίζει τα *attributes* που μπορεί να δεχθεί η εγγραφή. Οι κλάσεις έχουν ιεραρχική δομή η οποία καθορίζει και κληρονομικότητα των *attributes*. Όπως φαίνεται και στο παραπάνω παράδειγμα, η

συγκεκριμένη εγγραφή, εκτός από τα πολύ γενικά χαρακτηριστικά της βασικής κλάσης "*top*", έχει όλα τα χαρακτηριστικά της κλάσης "*person*", της ειδικότερης («διάδοχης») κλάσης "*organizationalPerson*"και της περαιτέρω ειδικότερης κλάσης "*inetOrgPerson*".

Οι βασικότερες λειτουργίες που προβλέπονται στον *LDAP* κατάλογο είναι:

- *Bind*: είναι η κλήση αυθεντικοποίησης από τον client προς τον server. Υπάρχει η «Απλή» μορφή της εντολής ("*Simple Bind*"), κατά την οποία αποστέλλονται στον server τα username και password του χρήστη και ο server ελέγχει το *attribute userPassword* της εγγραφής του χρήστη για την τελική απόφαση αυθεντικοποίησής του. Στην «Απλή» μορφή της *Bind* περιλαμβάνονται και οι μορφές: *Anonymous Authentication* (χωρίς username και password) και *Unauthenticated Authentication* (μόνο username χωρίς password). Η άλλη μορφή της *Bind* είναι η αυθεντικοποίηση με τη χρήση του *SASL* ("*SASL Authentication Method*"). Το *LDAP* έχει κατοχυρωθεί ως χρήστης του *SASL* και μπορεί μέσω αυτού να υλοποιήσει κάθε μηχανισμό αυθεντικοποίησης που υποστηρίζεται από το *SASL*. Με την εντολή *Bind* ο client δηλώνει, επίσης, την έκδοση του *LDAP* που επιθυμεί να χρησιμοποιήσει.

- *Start TLS*: δηλώνει την έναρξη χρήσης του πρωτοκόλλου *Transport Layer Security – TLS* για την προστασία των μηνυμάτων που θα ανταλλαγούν στα πλαίσια της τρέχουσας σύνδεσης.

- *Search*: αναζήτηση ή/και ανάκτηση συγκεκριμένων εγγραφών του καταλόγου.

- *Compare*: έλεγχος αν μία εγγραφή περιέχει μία συγκεκριμένη τιμή *attribute*.

- *Add*: προσθήκη νέας εγγραφής καταλόγου.

- *Delete*: διαγραφή μίας εγγραφής καταλόγου.

- *Modify*: ενημέρωση στοιχείων μίας εγγραφής καταλόγου.

- *Modify DN*: μετακίνηση ή μετονομασία μίας εγγραφής καταλόγου.

- *Abandon*: ακύρωση ενός προηγούμενου αιτήματος.

- *Extended Operation*: γενική λειτουργία με την οποία είναι δυνατός ο ορισμός νέων λειτουργιών.

- *Unbind*: κλείσιμο της τρέχουσας σύνδεσης.

Το πρωτόκολλο *LDAP* δεν επιβάλλει συγκεκριμένους κανόνες ασφάλειας των μηνυμάτων που αποστέλλονται ή των δεδομένων που αποθηκεύονται στον κατάλογο. Για παράδειγμα, το περιεχόμενο μίας εντολής *Bind* αποστέλλεται χωρίς ιδιαίτερη προστασία σύμφωνα με τις προδιαγραφές του πρωτοκόλλου. Συνιστώνται, όμως, πολλοί μηχανισμοί προστασίας των παραπάνω ευαίσθητων δεδομένων. Συνεπώς, είναι καθήκον της καθεμιάς υλοποίησης του πρωτοκόλλου να καθορίσει ποια μηνύματα *Simple Bind* περιέχουν κρίσιμα δεδομένα (πχ passwords) και να τα προστατέψει με την εντολή *Start TLS*, ώστε να σχηματισθεί ασφαλές κανάλι επικοινωνίας client/server. Εναλλακτικά, προφέρεται στους προγραμματιστές της καθεμιάς υλοποίησης του *LDAP* η επιλογή της εφαρμογής του *SASL Bind* και του καταλληλότερου μη-

χανισμού αυθεντικοποίησης που μπορεί να υποστηρίξει το *SASL*. Με αυτό τον τρόπο τα θέματα προστασίας των μεταδιδόμενων μηνυμάτων καθορίζονται από τις προδιαγραφές του *SASL* και του επιλεγμένου μηχανισμού αυθεντικοποίησης. Κατά παρόμοιο τρόπο, είναι στην διάθεση των προγραμματιστών της καθεμιάς *LDAP* υλοποίησης να καθορίσουν ποιοι χρήστες έχουν δικαιώματα μετατροπής των εγγραφών του καταλόγου, ώστε να προστατευτούν τα περιεχόμενά του από μη εγκεκριμένες επεμβάσεις.

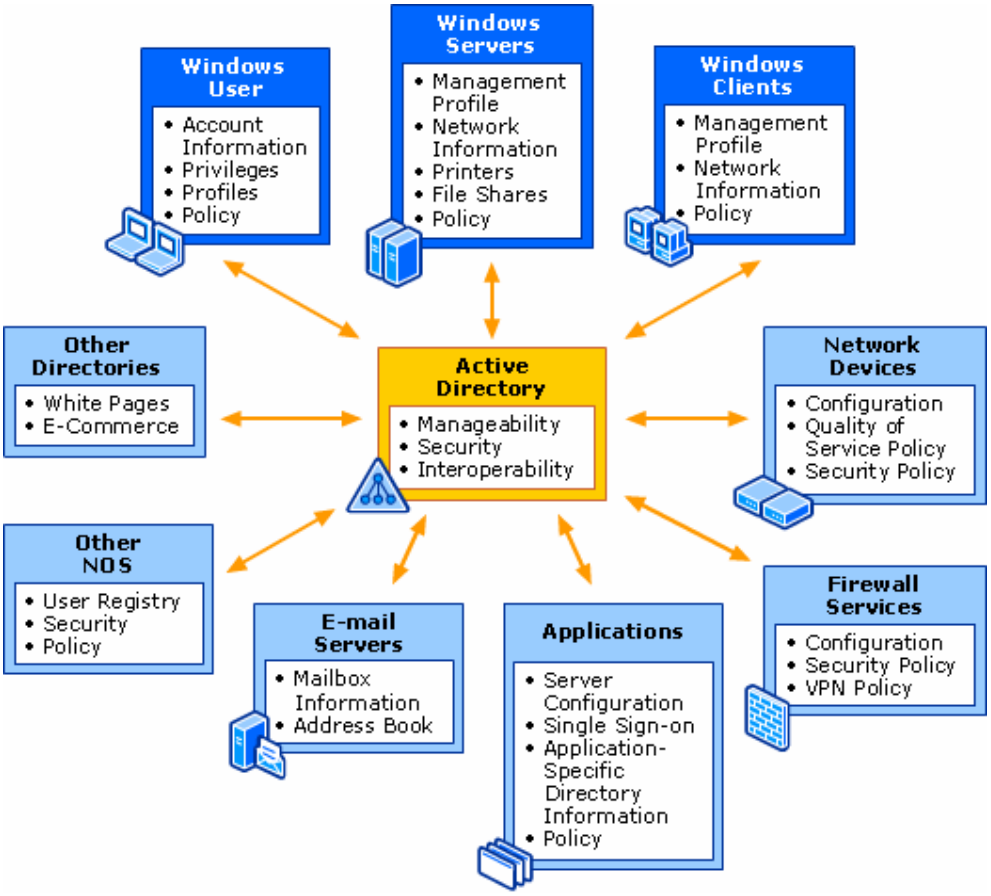
2.3.2.2 Active Directory του Microsoft Windows Server 2003

Η υπηρεσία *Active Directory* εγκαθίσταται στο λειτουργικό σύστημα *Microsoft Windows Server 2003* και χρησιμοποιείται για την ενιαία αποθήκευση πληροφοριών για τα δικτυακά αντικείμενα του δίκτυο που ελέγχεται από κάθε εγκατάσταση του συγκεκριμένου λειτουργικού συστήματος (*Windows Domain*[xii]). Τα δικτυακά αντικείμενα είναι πρωτίστως οι λογαριασμοί χρηστών του δικτύου, αλλά και οι servers, εκτυπωτές, προσωπικοί υπολογιστές κ.α. Όλες οι πληροφορίες που αφορούν αυτά τα αντικείμενα αποθηκεύονται σε μία ενιαία, ιεραρχική δομή καταλόγου, ώστε: να είναι δυνατή μία ομοιόμορφη διαδικασία αυθεντικοποίησης, οι διαχειριστές των δικτύων να ελέγχουν, οργανώνουν τους πόρους του δικτύου και να εφαρμόζουν πολιτικές δικαιωμάτων χρήσης των πόρων, ενώ οι χρήστες ανάλογα με τα δικαιώματα που τους έχουν δοθεί να εκμεταλλεύονται τους ανάλογους πόρους [80].

Ως υπηρεσία καταλόγου, το *Active Directory* είναι τόσο ένα σύστημα Βάσης Δεδομένων όσο και ένα σύνολο υπηρεσιών με τις οποίες γίνεται ασφαλής προσθήκη, επεξεργασία, διαγραφή και προσπέλαση δεδομένων μέσα στον αποθηκευτικό χώρο του καταλόγου. Αποτελεί το κομβικό σημείο για τη διαχείριση ταυτοτήτων και την διαμοίραση των κατανεμημένων πόρων ενός δικτύου το οποίο λειτουργεί υπό το λειτουργικό σύστημα *Microsoft Windows Server 2003* [79]:

[xii] Σχετικές με τη λειτουργία του *Active Directory* είναι οι έννοιες των *Domains, Trees* και *Forests* στην ορολογία των σύγχρονων "Server" λειτουργικών συστημάτων της Microsoft (Windows 2000, Windows Server 2003), οι οποίες και επεξηγούνται στο ΠΑΡΑΡΤΗΜΑ Α.

Πηγή: [79]



Εικόνα 23: Το Active Directory σε ένα Δίκτυο Windows Server 2003

Το Active Directory χρησιμοποιείται συνήθως για έναν από τους παρακάτω σκοπούς [79]:

- *Εσωτερικός Κατάλογος (Internal Directory)*: Εφαρμόζεται στο εσωτερικό ενός οργανισμού για τη διαχείριση πληροφοριών των χρηστών και πόρων του δικτύου. Είναι προσπελάσιμος μόνο από τους χρήστες του οργανισμού και από ένα ενδεχόμενο δίκτυο εκτός του εταιρικού μέσω μίας ασφαλούς σύνδεσης, όπως ένα *VPN (Virtual Private Network)*.

- *Εξωτερικός Κατάλογος (External Directory)*: Εφαρμόζεται σε «περιφερειακά» δίκτυα ή τις «Αποστρατικοποιημένες Ζώνες» (***De**Militarized **Z**ones - DMZ*) ενός οργανισμού, δηλαδή στο μικρό συνήθως δίκτυο των servers που βρίσκονται ανάμεσα στο τοπικό δίκτυο του οργανισμού και στο Internet. Ο κατάλογος, επομένως, περιέχει πληροφορίες εξωτερικών χρηστών (πελάτες και εμπορικούς συνεργάτες) οι οποίοι προσπελαύνουν δημοσιευμένα δεδομένα και υπηρεσίες.

- *Κατάλογος Εφαρμογών (Application Directory)*: Εφαρμόζεται για την αποθήκευση «ιδιωτικών» δεδομένων που χρειάζεται μόνο η δικτυακή εφαρμογή η οποία λειτουργεί στον ίδιο συνήθως server με τον κατάλογο. Τα συγκεκριμένα δεδομένα δεν έχουν κάποια ιδιαίτερη χρησιμότητα πέρα από τη δεδομένη εφαρμογή γι αυτό και δεν είναι απαραίτητο να μεταφέρονται μέσω δικτύου στους ελεγκτές του δικτύου (*Domain Controllers*).

Επιπροσθέτως, υπάρχει μία ειδική έκδοση του *Active Directory* η οποία ονομάζεται *Active Directory Application Mode – ADAM*. Το *ADAM* παρέχει υπηρεσίες καταλόγου σε περιπτώσεις όπου δεν είναι επιθυμητή η πλήρης εφαρμογή των σεναρίων εγκατάστασης του *Active Directory* με τη δημιουργία *Trees* και *Forests*. Συνήθως αυτές οι περιπτώσεις αφορούν συγκεκριμένες εφαρμογές οι οποίες απαιτούν τη σύνδεση με μία ευέλικτη υπηρεσία καταλόγου. Η τυπική εγκατάσταση του *Active Directory* γίνεται σε κάποιον *Domain Controller* γεγονός που πιθανώς αποτελεί πρόβλημα για συγκεκριμένες δικτυακές εφαρμογές οι οποίες επιθυμούν προσπέλαση σε πολλαπλά στιγμιότυπα (*instances*) ενός ηλεκτρονικού καταλόγου. Το *ADAM* είναι η περισσότερο ευέλικτη έκδοση του *Active Directory*, βασισμένη στο πρωτόκολλο *LDAP*, ώστε να ικανοποιούνται οι απαιτήσεις τέτοιων εφαρμογών [79].

Το *Active Directory* αυθεντικοποιεί και εξουσιοδοτεί (*authenticates* & *authorizes*) χρήστες, ομάδες χρηστών και υπολογιστές μέσω του υποσυστήματος *Local Security Authority (LSA)* το οποίο διαχειρίζεται τις κλήσεις για επιδιωκόμενες προσπελάσεις δικτυακών αντικειμένων. Οι μέθοδοι που εφαρμόζει είναι [79, 80]:

- *Αυθεντικοποίηση*: Το *LSA* του *Active Directory* αυθεντικοποιεί χρήστες και υπολογιστές με τα πρωτόκολλα *Kerberos V5* ή *NTLM*. Κατά την εφαρμογή του *Kerberos V5* σε περιβάλλον Windows Server λειτουργικού συστήματος το *KDC* του πρωτοκόλλου είναι ενσωματωμένο στο *Active Directory* το οποίο και διατηρεί τα κλειδιά καταχωρημένων χρηστών και servers. Το πρωτόκολλο *NTLM* (*Windows **NT** **L**an **M**anager*) εφαρμόζεται σε περιπτώσεις μικτών συστημάτων, σε δίκτυα δηλαδή όπου υπάρχει τουλάχιστον μία εγκατάσταση των Windows NT (client ή server) και επιχειρείται προσπέλαση προς ή από άλλο σύστημα με άλλη έκδοση των Windows. Μόλις επιβεβαιωθεί η ταυτότητα του χρήστη, το *LSA* δημιουργεί στον *Domain Controller* που υλοποιεί την αυθεντικοποίηση ένα *User Access Token* και συσχετίζει με το χρήστη ένα *Security ID (SID)* το οποίο και αποθηκεύει μέσα στο *User Access Token*. Το *SID* είναι ένας μοναδικός κωδικός ο οποίος αποδίδεται σε κάθε αντικείμενο που δημιουργείται στο *Active Directory* και μπορεί να συνδεθεί με πληροφορίες ασφαλείας. Η επιλογή του κατάλληλου πρωτοκόλλου αυθεντικοποίησης γίνεται μέσω του μηχανισμού «διαπραγμάτευσης» "***S**imple and **P**rotected GSSAPI **Nego**tiation Mechanism – SPNEGO*" (βλ. παράγραφο 2.3.1.2).

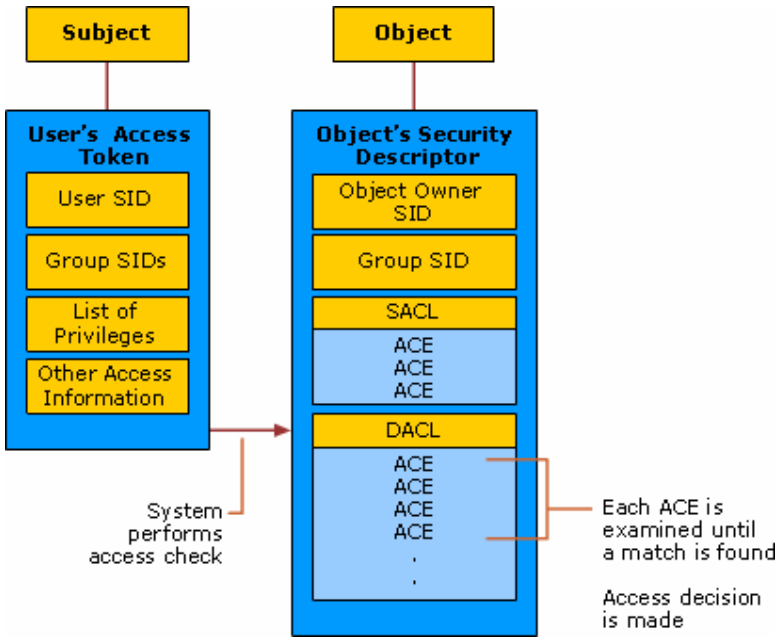
  Μόλις ένας χρήστης αυθεντικοποιηθεί σε ένα *Domain* που ελέγχεται από το *Active Directory* η υπηρεσία *LSA* αποθηκεύει προσωρινές πληροφορίες της ταυτότητας του χρήστη στον τοπικό του Ηλ. Υπολογιστή. Με αυτό τον τρόπο επιτυγχάνεται Single Sign – On στα πλαίσια των πόρων του *Domain*, καθώς κάθε επόμενη απόπειρα σύνδεσης του χρήστη σε κάποιο άλλο πόρο του *Domain*, η οποία απαιτεί αυθεντικοποίηση, θα υλοποιηθεί χωρίς επανεισαγωγή των μυστικών κωδικών του χρήστη. Οποιαδήποτε μέθοδος και αν χρησιμοποιήθηκε αρχικά, τα Windows εντοπίζουν τις πληροφορίες ταυτότητας του χρήστη από την προηγούμενή του αυθεντικοποίηση και του επιτρέπουν την πρόσβαση.

- *Εξουσιοδότηση – Έλεγχος Πρόσβασης*: Το *Active Directory* παρέχει τη δυνατότητα ελέγχου πρόσβασης σε κάθε δικτυακό αντικείμενο με την απόδοση συγκεκριμένων επιπέδων πρόσβασης ή εξουσιοδοτήσεων όπως: "*Full Control*", "*Write*", "*Read*", ή "*No Access*". Μέσα στο *Active Directory* προσδιορίζονται για καθένα διαμοιρασμένο αντικείμενο οι χρήστες και τα ακριβή δικαιώματά τους πάνω στο συγκεκριμένο αντικείμενο και οι πληροφορίες αυτές διατηρούνται ως ιδιότητες του αντικειμένου. Συγκεκριμένα, καθένα αντικείμενο του *Active Directory* διατηρεί δύο λίστες πληροφοριών πρόσβασης: την "*Discretionary Access Control List – DACL*" και την "*System Access Control List – SACL*". Η λί-

στα *DACL* περιέχει τους χρήστες ή τα groups και τα δικαιώματα που τους έχουν επιτραπεί ή απαγορευτεί πάνω στο αντικείμενο. Οι καταχωρήσεις της ονομάζονται "*Access Control Entries - ACEs*" και είναι ουσιαστικά τα *SIDs* των χρηστών ή groups όπως τα διατηρεί το *Active Directory*. Η λίστα *SACL* περιέχει τους χρήστες ή τα groups τα οποία ο διαχειριστής επιθυμεί να παρακολουθεί όταν επιτυγχάνουν ή αποτυγχάνουν να προσπελαύνουν το συγκεκριμένο αντικείμενο. Οι καταχωρήσεις της *SACL* είναι παρόμοιας μορφής με αυτές της *DACL*. Κάθε χρήστης που έχει αυθεντικοποιηθεί από τον *Active Directory* έχει στη διάθεσή του ένα *User Access Token* το οποίο περιέχει το δικό του *SID* και του group στο οποίο ανήκει. Κάθε φορά που επιχειρείται κάποια ενέργεια σε ένα διαμοιρασμένο αντικείμενο από έναν χρήστη το σύστημα (συγκεκριμένα ο *Windows Object Manager*) αναζητεί το *SID* που υπάρχει στο *User Access Token* του χρήστη μέσα στην *DACL* του αντικειμένου και αναλόγως επιτρέπει ή όχι την εκτέλεση της ενέργειας. Η διαδικασία περιγράφεται και στην παρακάτω Εικόνα 24.

Τα δεδομένα ταυτότητας των χρηστών και ελέγχου πρόσβασης των αντικειμένων είναι δυνατό να μεταφερθούν και σε άλλες πλατφόρμες μέσω της συμμόρφωσης του *Active Directory* με το πρωτόκολλο *LDAP*. Το *Active Directory*, δηλαδή, έχει «χτιστεί» με βάση την υποστήριξη όλων των προδιαγραφών του *LDAP v3*, επομένως θεωρείται ότι «συμμορφώνεται» στις απαιτήσεις του *LDAP v3* και μπορεί να υποστηρίξει όλες τις *LDAP* λειτουργίες πρόσβασης, ανάγνωσης και διαχείρισης ενός καταλόγου. Αυτό σημαίνει ότι μία εφαρμογή στο δίκτυο μπορεί να λειτουργήσει ως *LDAP* client προσπελαύνοντας πληροφορίες καταλόγου στο *Active Directory* ο οποίος μπορεί να ανταποκριθεί ως *LDAP* server. Το πρωτόκολλο *LDAP* είναι ο πυρήνας του *Active Directory* και είναι ο συνήθης και προτιμητέος τρόπος αλληλεπίδρασης ενός client με το *Active Directory* [81].

Πηγή: [79]



Εικόνα 24: Πληροφορίες Ταυτότητας και Διαδικασία Ελέγχου Πρόσβασης στον Active Directory

2.4 Single Sign-On (SSO) και *Federated Identity Management*

Ο όρος Single Sign – On (SSO) περιγράφει γενικά μία υπηρεσία η οποία παρέχεται από τα συστήματα Διαχείρισης Ταυτοτήτων επιπλέον της κύριας διαδικασίας αυθεντικοποίησης. Μέσα σε ένα περιβάλλον πολλών διαθέσιμων εφαρμογών λογισμικού η αυθεντικοποίηση ενός χρήστη για πρόσβαση σε μία από αυτές συνοδεύεται από την εξασφάλιση ότι εφόσον ο ίδιος χρήστης επιχειρήσει πρόσβαση σε κάποια άλλη εφαρμογή, η αυθεντικοποίησή του θα ολοκληρωθεί επιτυχώς χωρίς την επανάληψη από μέρους του των ενεργειών που απαιτεί ο εφαρμοζόμενος μηχανισμός αυθεντικοποίησης (πχ πληκτρολόγηση username & password, εισαγωγή Smart Card ή USB Token κλπ) (βλ. παράγραφο 2.2). Ανάλογα με το περιβάλλον και το είδος των εφαρμογών λογισμικού η υπηρεσία SSO διακρίνεται στις κατηγορίες [86, 120]:

- <u>*Desktop Single Sign – On*</u>: αφορά την εφαρμογή SSO σε επίπεδο δικτυακών Λειτουργικών Συστημάτων όπου οι χρήστες εισέρχονται σε ένα τοπικό δίκτυο το οποίο συνθέτει ένα *Domain* ή *Realm* και η μετέπειτα χρήση των πόρων που ελέγχονται από το Λειτουργικό Σύστημα δεν απαιτεί ξανά την αυθεντικοποίηση του χρήστη. Παράδειγμα εφαρμογής της συγκεκριμένης υπηρεσίας αποτελεί το Λειτουργικό Σύστημα Microsoft Windows Server 2003 στο οποίο η εγκατάσταση του *Active Directory* και η αυθεντικοποίηση των χρηστών βάσει αυτού εξασφαλίζει μοναδική αυθεντικοποίηση του χρήστη κατά την πρώτη είσοδό του στο *Domain* και αυτόματη, μετέπειτα πρόσβαση στους δικτυακούς πόρους του *Domain* (δικτυακούς εκτυπωτές, «μοιρασμένα» αρχεία ή προγράμματα, υπηρεσίες e-mail ή Διαχείρισης Βάσεων Δεδομένων κλπ).

- <u>*Enterprise Single Sign – On* (*ESSO*)</u>: αφορά την εφαρμογή SSO μεταξύ διαφορετικών εφαρμογών λογισμικού που εκτελούνται, όμως, μέσα στα πλαίσια μίας επιχείρησης (*Enterprise*). Η συγκεκριμένη υπηρεσία αποσκοπεί κυρίως στους υπαλλήλους επιχειρήσεων οι οποίοι χρησιμοποιούν συγκεκριμένα προγράμματα, πιθανώς διαφορετικών τεχνολογιών (ERP, CRM, άλλες client/server εφαρμογές κλπ). Εκτός από τη διευκόλυνση της πρόσβασης στις ποικίλες «εταιρικές» εφαρμογές υπάρχει η ανάγκη ενιαίας διαχείρισης των ταυτοτήτων των «εταιρικών» χρηστών που δημιουργούνται μέσα στα πλαίσια των διαφορετικών εφαρμογών. Το ESSO απαιτεί κάποιας μορφής «αντιστοίχιση ταυτοτήτων» καθώς πρέπει οι διαφορετικές ταυτότητες των ίδιων χρηστών στα διάφορα συστήματα να αντιστοιχιστούν σε μία ταυτότητα, η εγκυρότητα της οποίας να ελέγχεται κατά την αυθεντικοποίηση. Τα συστήματα, επομένως, που παρέχουν ESSO υπηρεσίες εγκαθίστανται παράλληλα στα συστήματα Διαχείρισης Ταυτοτήτων των ετερογενών εφαρμογών και προσπαθούν να εξάγουν τις ταυτότητες των χρηστών, ώστε να ταυτίσουν αυτές που ανήκουν στον ίδιο χρήστη και να προκύψει μία νέα, μοναδική ταυτότητα για καθένα χρήστη η οποία θα διατηρείται στο δικό τους Κατάλογο (*Active Directory*, οποιοσδήποτε άλλος *LDAP* κατάλογος, απλή Βάση Δεδομένων λογαριασμών χρηστών κλπ). Το ESSO είναι φλέγον ζήτημα για τις σύγχρονες επιχειρήσεις γι αυτό και έχουν δημιουργηθεί πολλά εμπορικά πακέτα εξασφάλισης υπηρεσιών ESSO και πολλών άλλων υπηρεσιών που σχετίζονται με τη διαχείριση χρηστών στα πλαίσια επιχειρήσεων. Ενδεικτικά αναφέρονται τα (αλφαβητική σειρά): Centrify *DirectControl* [12], Evidian *WiseGuard* [24], Microsoft

SharePoint και Microsoft *BizTalk* [85], Oracle *Enterprise Single Sign-On* [112], Passlogix *v-GO* [113], RSA *Sign-On Manager* [119] κλπ

- *Web Single Sign – On* (*Web SSO*): αφορά την εφαρμογή του SSO ειδικά στη διαδικασία πρόσβασης και εκτέλεσης εφαρμογών μέσω ιστοσελίδων του World Wide Web στο Διαδίκτυο (Internet). Οι συγκεκριμένες εφαρμογές είναι συνήθως οργανωμένες στα πλαίσια μία Δικτυακής Πύλης (Portal). Μέσω του Web SSO ο χρήστης εκτελεί τη διαδικασία αυθεντικοποίησης της ταυτότητάς του στην αρχή της εισόδου στο Portal και η ενδεχόμενη έγκριση εισόδου του ισχύει για όλες τις εφαρμογές που διατίθενται στο συγκεκριμένο δικτυακό χώρο. Η διαδικασία του Web SSO έχει αρχίσει να γίνεται αρκετά πολύπλοκη όσο αυξάνεται το μέγεθος και η ποικιλομορφία των Portals, γι αυτό και η υλοποίησή του αναλαμβάνεται από ξεχωριστά τμήματα λογισμικού τα οποία παίρνουν τη μορφή αυτόνομων υπηρεσιών που συνεργάζονται με το λογισμικό των Portals. Συγκεκριμένα, η υπηρεσία Web SSO υλοποιείται εγκαθιστώντας επιπρόσθετο λογισμικό στον Web Server ή Application Server που ελέγχει τις δικτυακές υπηρεσίες και την πρόσβαση των χρηστών σε αυτές [57]. Λόγω των διαφορετικών τεχνολογιών που εφαρμόζονται στις Internet Web Applications και στις απλές δικτυακές εφαρμογές ενός LAN, υπάρχει μεγάλη διαφορά στην τεχνολογική υλοποίηση του Web SSO από αυτή του *Domain* SSO ή του ESSO.

  Πολλά δείγματα υλοποίησης αυτών των υπηρεσιών προήλθαν από ερευνητικές προσπάθειες κυρίως μεγάλων Πανεπιστημίων και προσφέρονται ως «ανοιχτές» λύσεις (open – source Solutions) για ελεύθερη ενσωμάτωση κατά την ανάπτυξη Web Sites. Οι πιο διαδεδομένες open – source λύσεις Web SSO είναι: "*CoSign*" (University of Michigan), "*CAS*" (Yale University), "*WebAuth*" (Stanford University), "*Pubcookie*" (University of Washington). Επίσης, στην ίδια κατηγορία ανήκουν το "*WebAuth*" (Duke University) [19] και τα μη ακαδημαϊκά προϊόντα που βασίζονται στην Java: "*JOSSO*" – Java Open SSO Project [58], "*OpenSSO*" – Open Access / Open Federation το οποίο προέκυψε από το «άνοιγμα» του πηγαίου κώδικα του προϊόντος "*System Access Manager*" της εταιρίας Sun [111]. Εκτός από τις open – source λύσεις Web SSO υπάρχουν επίσης πολλά εμπορικά προϊόντα υλοποίησης των συγκεκριμένων υπηρεσιών τα οποία σε γενικές γραμμές ανήκουν στις ίδιες εταιρίες που αναφέρθηκαν στην προηγούμενη παράγραφο προϊόντων ESSO.

- *Federated Single Sign – On*: αφορά την επέκταση της υπηρεσίας Web SSO σε «σενάρια» χρήσης *Federations* μεταξύ οργανισμών. Οι χρήστες, επομένως, που αυθεντικοποιούνται με τη *Federated* ταυτότητά τους σε υπηρεσίες άλλου οργανισμού από αυτό που ανήκουν μπορούν να προσπελάσουν και άλλες υπηρεσίες συνεργαζόμενων οργανισμών χωρίς να επαναλάβουν τη διαδικασία της αυθεντικοποίησης (βλ παράγραφο 2.2).

Η υπηρεσία SSO φαίνεται αρχικά ότι επιχειρεί να διευκολύνει το χρήστη κατά την μετακίνησή του από μία εφαρμογή σε μία άλλη, αλλά τα οφέλη που προσφέρει είναι πολύ σημαντικότερα [120, 134]:

- Οι χρήστες υποβάλλουν τα «πιστοποιητικά» της ταυτότητάς τους μόνο μία φορά, γεγονός το οποίο ενισχύει την ασφάλεια της διαδικασίας αυθεντικοποίησης σε περιβάλλοντα δικτύου δεδομένων, καθώς δεν υπάρχει συνεχής μετάδοσή των «πιστοποιητικών» και δεν καθίστανται ευάλωτα σε «επιθέσεις».

- Οι χρήστες έχουν μόνο ένα μυστικό αναγνωριστικό με το οποίο αποδεικνύουν την ταυτότητά τους σε όλες τις προστατευόμενες υπηρεσίες, άρα διευκολύνονται οι ίδιοι, αλλά και ενισχύεται η ασφάλεια όλου του συστήματος με τον περιορισμό των διαφορετικών ή απολεσθέντων κωδικών πρόσβασης.

- Μειώνεται δραστικά το κόστος διαχείρισης των λογαριασμών των χρηστών, καθώς όλα τα δεδομένα ταυτοτήτων τους συγκεντρώνονται στο μοναδικό σημείο διεξαγωγής της αυθεντικοποίησής τους. Ταυτόχρονα, απαλείφονται οι διαδικασίες τήρησης πολλών αντιγράφων των ταυτοτήτων των χρηστών, οι οποίες είναι απαραίτητες στην περίπτωση ξεχωριστής αυθεντικοποίησης για καθεμιά υπηρεσία.

- Γίνεται εφικτή η εφαρμογή ενιαίας μεθόδου αυθεντικοποίησης σε όλες τις ελεγχόμενες υπηρεσίες με ενίσχυση της ασφάλειάς της στο μοναδικό σημείο όπου ελέγχονται οι χρήστες και όχι σε καθεμιά υπηρεσία ξεχωριστά. Είναι δυνατή, επομένως, η εφαρμογή μεθόδων «ισχυρής» αυθεντικοποίησης οι οποίες είναι πιο πολύπλοκες και σχεδόν απαγορευτικές στις περιπτώσεις ξεχωριστής αυθεντικοποίησης για καθεμιά ελεγχόμενη υπηρεσία.

- Εκτός από την είσοδο στις υπηρεσίες, η έξοδος και η λήξη των συναλλαγών που πιθανώς έχει ενεργοποιήσει ταυτόχρονα ο χρήστης υλοποιείται επίσης αυτόματα χωρίς να είναι απαραίτητη η έξοδος από καθεμιά «ανοιχτή» υπηρεσία ξεχωριστά.

- Από την πλευρά της εμπορικής και διοικητικής αξιοποίησης του Internet, οι Web Applications γίνονται περισσότερο απλές και ελκυστικές με αποτέλεσμα την διεύρυνση της χρήσης του Internet σε περισσότερους σκοπούς. Η απλούστευση αλλά ταυτόχρονα και οχύρωση των διαδικασιών αυθεντικοποίησης αποτελεί σημαντικό παράγοντα ανάπτυξης νέων μοντέλων λειτουργίας των εμπορικών ή κυβερνητικών Portals.

Οι κατηγορίες SSO που εμπίπτουν στο εύρος της παρούσας εργασίας είναι οι Web SSO και *Federated* SSO. Από τις υπάρχουσες υλοποιήσεις των συγκεκριμένων υπηρεσιών θα παρουσιαστούν παρακάτω οι πιο αντιπροσωπευτικές με βασικά κριτήρια επιλογής: τον «ανοιχτό» χαρακτήρα της εφαρμοζόμενης λύσης, ώστε να είναι πλησιέστερη στην Ακαδημαϊκή φιλοσοφία ανάπτυξης προϊόντων, το σχετικό βαθμό διάδοσης μέσα στο χώρο εφαρμογών παρόμοιων λύσεων και το βαθμό καινοτομίας που παρουσιάζουν στην υλοποίησή τους σε σχέση με τις υπόλοιπες.

2.4.1 "*CoSign*" – Open Source Web SSO (University of Michigan)

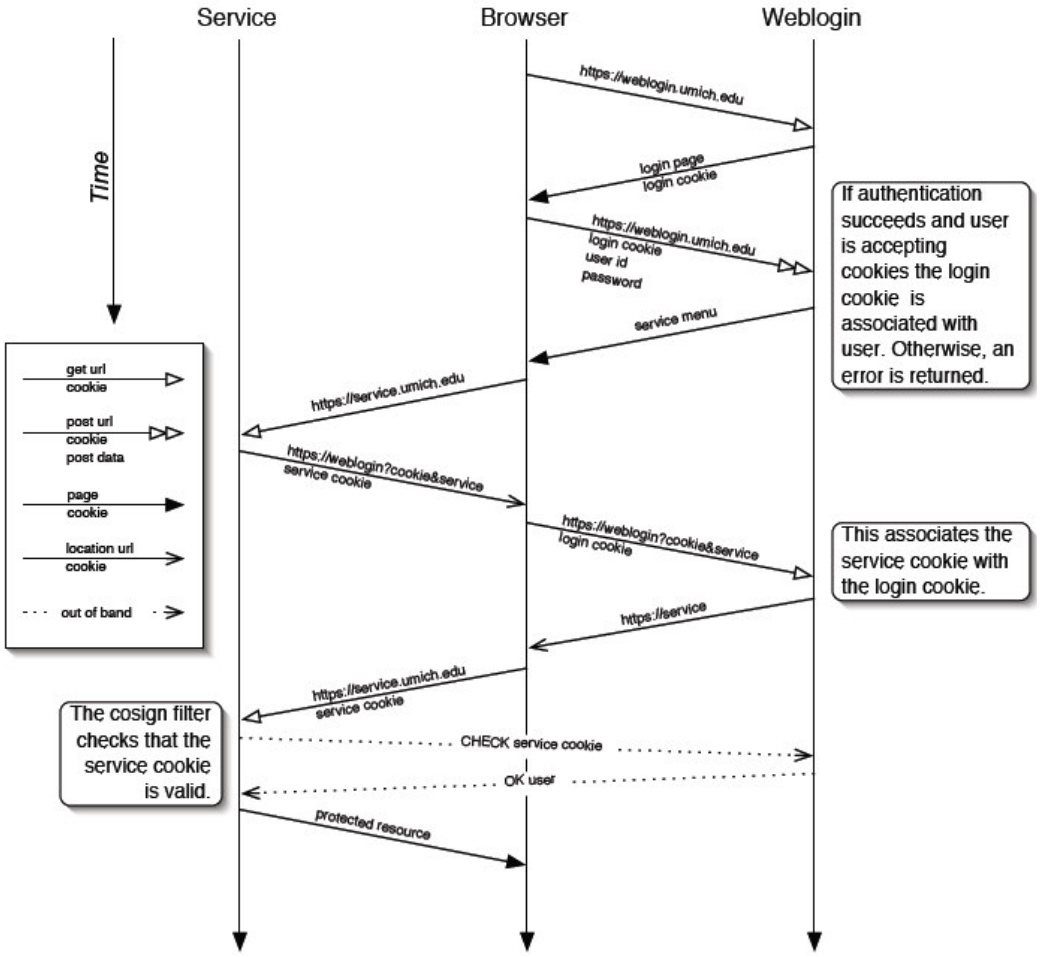
Η λύση Web SSO *CoSign* αναπτύχθηκε από το Πανεπιστήμιο του Michigan το 2002, αρχικά για την εξυπηρέτηση των αναγκών του ίδιου του Πανεπιστημίου. Το πρόγραμμα που υλοποιεί το *CoSign* είναι γραμμένο στη γλώσσα προγραμματισμού C και η λειτουργία του βασίζεται στο μηχανισμό των Cookies. Το μοντέλο αυθεντικοποίησης που εφαρμόζει χρησιμοποιεί δύο ειδών Cookies: το *Login Cookie* και το *Service Cookie*. Στη γενική αρχιτεκτονική την οποία προϋποθέτει το *CoSign* υπάρχει ένας σταθμός εξυπηρέτησης (server) στον οποίο έχει εγκατασταθεί το λογισμικό του *CoSign* και θεωρείται ο "*WebLogin Server*", ένας Application Server στον οποίο υπάρχουν οι υπηρεσίες (applications) που επιθυμεί να προσπελάσει ο χρήστης και στον οποίο έχει εγκατασταθεί λογισμικό – «φίλτρο» του *CoSign* για να ελέγχεται ποιες υπηρεσίες απαιτούν την αυθεντικοποίηση *CoSign*. Η αρχιτεκτονική ολοκληρώνεται με τον ίδιο

το χρήστη ο οποίος χρησιμοποιεί το τοπικό του λογισμικό πρόσβασης στο Internet (Web Browser). Υπάρχουν δύο «σενάρια» λειτουργίας της αυθεντικοποίησης [147]:

- Πρώτο «σενάριο»: ο χρήστης προσπελαύνει τη σελίδα αυθεντικοποίησης του *CoSign* (υπηρεσία *WebLogin*). Αν στον Browser του χρήστη δεν υπάρχει ένα *Login Cookie* τότε το *WebLogin* εμφανίζει την κατάλληλη οθόνη εισαγωγής των στοιχείων αυθεντικοποίησης του χρήστη (συνήθως username & password). Στην περίπτωση που ο έλεγχος των στοιχείων του χρήστη είναι επιτυχημένος και ο Browser του χρήστη αποδέχεται τα Cookies τότε δημιουργείται το απαραίτητο *Login Cookie* και συνδέεται με το συγκεκριμένο χρήστη. Στη συνέχεια αποστέλλεται στο χρήστη οποιαδήποτε οθόνη περιέχει τις δικτυακές υπηρεσίες (applications). Μόλις ο χρήστης επιλέξει την είσοδό του σε μία υπηρεσία τότε δημιουργείται το αντίστοιχο *Service Cookie* το οποίο αποστέλλεται στον *WebLogin server* ο οποίος συσχετίζει το συγκεκριμένο *Service Cookie* με το *Login Cookie* του χρήστη. Όταν αρχίσει η είσοδος του χρήστη σε τμήμα των υπηρεσιών του συγκεκριμένου web site, το «φίλτρο» του *CoSign*, που είναι εγκατεστημένο στον Application Server του site, θα ζητήσει και θα λάβει από τον Browser του χρήστη τα δύο απαραίτητα Cookies (*Login & Service*). Τα δύο Cookies στέλνονται στη συνέχεια από το «φίλτρο» στον *WebLogin Server* ο οποίος ελέγχει τη συσχέτισή τους και επιστρέφεται στο «φίλτρο» η έγκριση για την πρόσβαση του συγκεκριμένου χρήστη στη συγκεκριμένη υπηρεσία (βλ. Εικόνα 25) [27].

- Δεύτερο «σενάριο»: υπάρχει περίπτωση ο χρήστης να καλέσει απευθείας τη σελίδα της επιθυμητής δικτυακής υπηρεσίας. Η συγκεκριμένη υπηρεσία δημιουργεί το *Service Cookie* και το αποστέλλει στον *WebLogin Server*. Από τη στιγμή που δεν υπάρχει *Login Cookie* ο *WebLogin Server* ανακατευθύνει το χρήστη στη σελίδα εισαγωγής των στοιχείων ταυτότητάς του. Σε περίπτωση που ο χρήστης αυθεντικοποιηθεί επιτυχημένα, τα δύο συσχετισμένα Cookies (*Service & Login*) αποστέλλονται πίσω στο χρήστη. Στη συνέχεια, όπως και στο πρώτο «σενάριο», το «φίλτρο» του *CoSign* θα απαιτήσει από τον *WebLogin Server* επιβεβαίωση για το συγκεκριμένο ζευγάρι Cookies ώστε ο χρήστης να εκτελέσει τη συγκεκριμένη υπηρεσία (βλ. Εικόνα 26) [27].

Πηγή: [147]

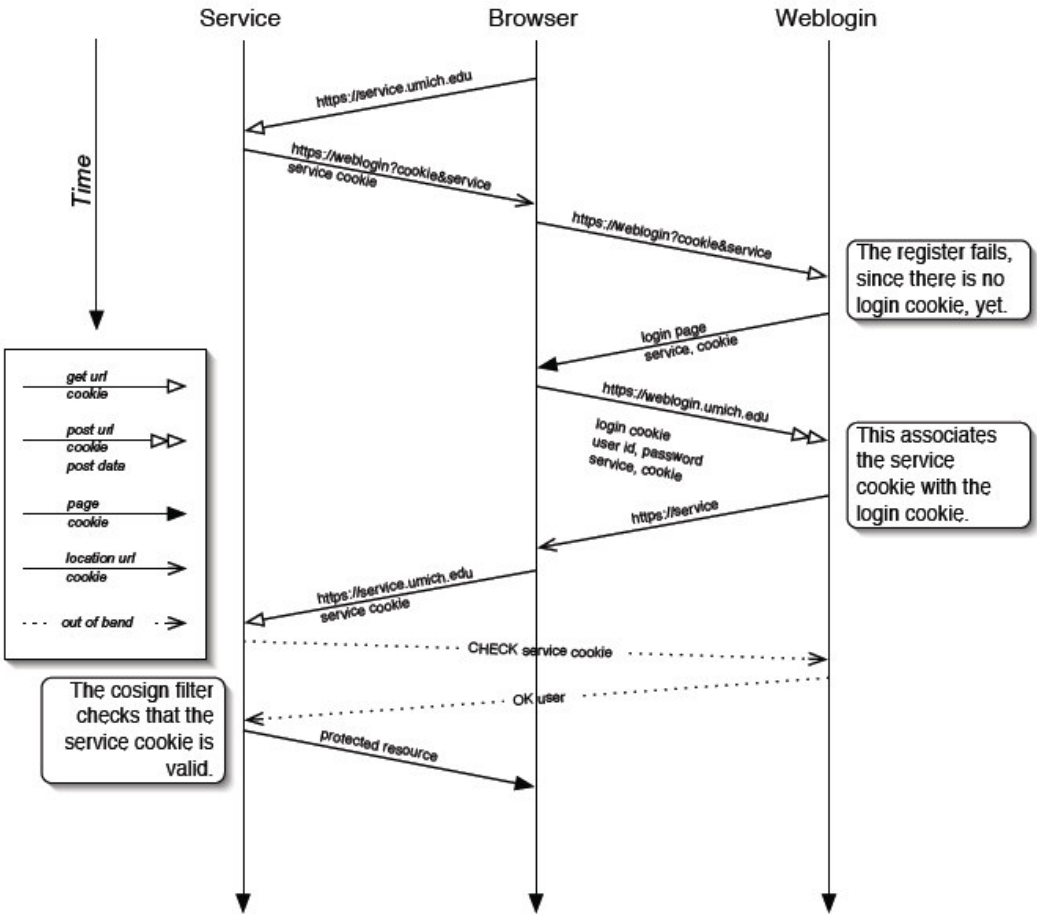


Εικόνα 25: Πρώτο «Σενάριο» Λειτουργίας του *CoSign*

Η μέθοδος αυθεντικοποίησης που χρησιμοποιεί το *CoSign* είναι το πρωτόκολλο *Kerberos*, ενώ όλη η επικοινωνία που περιγράφεται στα δύο παραπάνω «σενάρια» γίνεται με τη χρήση του «ασφαλούς» πρωτοκόλλου SSL/TLS. Ο *WebLogin Server* του *CoSign* αποτελείται κυρίως από δύο βασικές υπηρεσίες: "*CoSign CGI*" και "*CoSign Daemon*". Αυτές οι υπηρεσίες αποτελούν μαζί με το «φίλτρο» του *CoSign* τα δομικά συστατικά του [147]:

- <u>*CGI*</u>: είναι υπεύθυνο για την καταχώρηση και διαγραφή των χρηστών στον κεντρικό *CoSign* Server. Επίσης, συνδέει κάθε χρήστη με την ελεγχόμενη υπηρεσία που προσπελαύνεται στους προστατευόμενους Application Servers (πχ Web Mail, Web Directory κλπ). Η πρωτότυπη έκδοση του *CGI* χρησιμοποιεί πρωτόκολλο *Kerberos 5* για την αυθεντικοποίηση των χρηστών.

Πηγή: [147]



Εικόνα 26: Δεύτερο «Σενάριο» Λειτουργίας του *CoSign*

- *Daemon*: είναι υπεύθυνος για την παρακολούθηση της κατάστασης όλων των ενεργών «συνόδων» (sessions) του *CoSign*. Παρακολουθεί, δηλαδή, ποιοι χρήστες έχουν αυθεντικοποιηθεί, ποιοι έχουν αποχωρήσει από το σύστημα και μετρά τον ανενεργό χρόνο των χρηστών. Επίσης, καταγράφει τα *Service Cookies* που έχουν συνδεθεί με έναν μεμονωμένο χρήστη. Υπάρχει η δυνατότητα αντιγραφής της βάσης δεδομένων που διατηρεί σε πολλούς υπολογιστές ώστε ενδεχόμενη αποτυχία ενός *server* να μην σταματήσει τη λειτουργία του συστήματος. «Απαντά» σε κλήσεις τόσο του *CGI* όσο και του «φίλτρο» του *CoSign*.

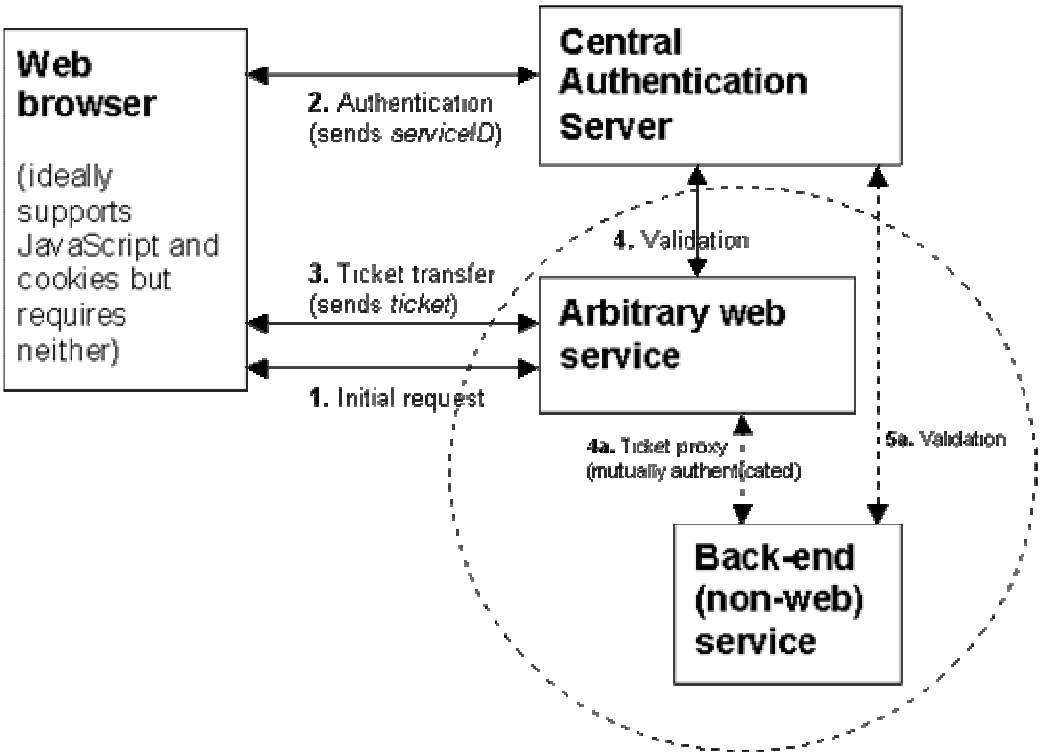
- *«Φίλτρο»*: είναι εγκατεστημένο σε κάθε Application Server του συστήματος και δεν αποτελεί μέρος του *CoSign* Server. Είναι υπεύθυνο για τον προσδιορισμό των τμημάτων του web site τα οποία προστατεύονται από το *CoSign*, έτσι ώστε όταν ένας χρήστης προσπαθήσει να προσπελάσει μία «προστατευόμενη» περιοχή να εξασφαλίσει ότι ο χρήστης είναι αυθεντικοποιημένος. Η πρωτότυπη έκδοση του φίλτρου είναι γραμμένη στη γλώσσα προγραμματισμού C για τον web server *Apache* 1.3.x ή επόμενο/*Apache* 2.0 ή επόμενο (*mod_cosign*), αλλά υπάρχει και «φίλτρο» για τον IIS των Windows.

2.4.2 "*CAS*" - Central Authentication Service (Yale University)

Το πρωτόκολλο *CAS* εφαρμόζεται σε λύσεις Web SSO, αναπτύχθηκε αρχικά από το Πανεπιστήμιο του Yale και τώρα έχει υιοθετηθεί από την ομάδα "*JA-SIG (Java Architectures)*". Είναι και αυτό βασισμένο στο μηχανισμό των Cookies. Η υλοποίησή του στο τμήμα του server έχει γίνει με τη γλώσσα προγραμματισμού Java, ενώ έχουν κυκλοφορήσει υλοποιήσεις του client τμήματος του πρωτοκόλλου σε διάφορες γλώσσες. Η εγκατάστασή του γίνεται σε Application Server ο οποίος είναι συμβατός με την πλατφόρμα "*Java Platform, Enterprise Edition – Java EE*[xiii]" (πχ BEA *Weblogic*, *Oracle* application server, *Jakarta Tomcat* κλπ) και η πλήρης λειτουργικότητά του εξαρτάται από τις υπηρεσίες που μπορεί να προσφέρει ο Application Server. Η υλοποίησή του ξεκίνησε με την έκδοση 1.0 ενώ η τρέχουσα έκδοση είναι η 2.0. Η βασική λειτουργία της αρχικής έκδοσης 1.0 είναι [57]:

- Ο server του *CAS* είναι υλοποιημένος ως ξεχωριστή, αυτόνομη Web εφαρμογή. Οι υπόλοιπες Web υπηρεσίες που θέλουν να εξυπηρετηθούν από το *CAS* τον προσπελαύνουν μέσω τριών διευθύνσεων URL: το *Login URL*, το *Validation URL* και το προαιρετικό *Logout URL*. Οι συγκεκριμένες προσβάσεις στον *CAS* server και η βασική λειτουργία του φαίνονται στην παρακάτω Εικόνα.

Πηγή: [57]



Εικόνα 27: Βασική Υλοποίηση του Πρωτοκόλλου CAS 1.0

[xiii] Είναι γνωστή και ως "Java 2, Enterprise Edition - J2EE Platform" και αποτελεί συνολική πλατφόρμα ανάπτυξης και εκτέλεσης κατανεμημένων εφαρμογών σε Java με αρχιτεκτονική πολλών επιπέδων (multi-tier). Αποτελεί πρόταση της Sun μέχρι την έκδοση J2EE 1.4 SDK – Software Development Kit [135] ενώ η τελευταία έκδοση είναι η Java EE 5 SDK [136].

- Ο χρήστης που επιθυμεί μέσω του Web Browser να χρησιμοποιήσει μία Web υπηρεσία η οποία απαιτεί *CAS* αυθεντικοποίηση κατευθύνεται προς τη login σελίδα της υπηρεσίας *CAS* (*Login URL*). Η συγκεκριμένη ανακατεύθυνση περιλαμβάνει ως παράμετρο και τη διεύθυνση URL της υπηρεσίας που κάλεσε αρχικά ο χρήστης, ώστε ο *CAS* server να προωθήσει το χρήση μετά την αυθεντικοποίηση. Ο χρήστης πρέπει να εισάγει τα προσωπικά του στοιχεία ταυτότητας (συνήθως username & password). Ο *CAS* server χρησιμοποιεί το πρωτόκολλο *Kerberos* για την αυθεντικοποίηση του χρήστη σε συνεργασία με τη εξωτερική υπηρεσία αυθεντικοποίησης η οποία χρησιμοποιείται στο συγκεκριμένο Web site. Στην περίπτωση επιτυχούς αυθεντικοποίησης ο *CAS* server δημιουργεί έναν μεγάλο, τυχαίο αριθμό ο οποίος ονομάζεται "*ticket*" και τον επιστρέφει ως παράμετρο στη σελίδα της Web υπηρεσίας που επιθυμεί να χρησιμοποιήσει ο χρήστης. Με το *ticket* ο *CAS* server συνδέει στη μνήμη του τον συγκεκριμένο χρήστη με τη συγκεκριμένη υπηρεσία και η ισχύς του είναι προσωρινή καθώς μπορεί να χρησιμοποιηθεί για την επιβεβαίωση της ταυτότητας του χρήστη μόνο για την τρέχουσα υπηρεσία (1 & 2 στην Εικόνα).

- Παράλληλα με την παραπάνω βασική διαδικασία, προαιρετικά ο *CAS* server δημιουργεί στην πλευρά του χρήστη ένα προσωρινό Cookie το οποίο ονομάζεται "*Ticket Granting Cookie – TGC*" με το οποίο επιτυγχάνεται το Single Sign-On. Το *TGC* παραμένει μόνο στη μνήμη του client Ηλ. Υπολογιστή και με αυτό ο χρήστης δεν είναι υποχρεωμένος να εισάγει τα στοιχεία του για να επιτύχει το login σε κάθε Web υπηρεσία η οποία απαιτεί το μηχανισμό *CAS,* παρά μόνο την πρώτη φορά εισόδου στην πρώτη υπηρεσία.

- Στην επόμενη φάση του πρωτοκόλλου *CAS* ο έλεγχος βρίσκεται στη συγκεκριμένη Web υπηρεσία η οποία έχει δεχθεί ως παράμετρο το *ticket* του *CAS* server για τον τρέχοντα χρήστη (3 στην Εικόνα). Προκειμένου να επιβεβαιώσει ότι πρόκειται για έγκυρο χρήστη καλεί τον *CAS* server μέσω του *Validation URL* του, ώστε να γίνει η επιβεβαίωση. Ο *CAS* server ελέγχει αν το συγκεκριμένο *ticket* υπάρχει στη μνήμη του και είναι συνδεδεμένο με τη συγκεκριμένη Web υπηρεσία. Σε περίπτωση επιτυχίας επιστρέφεται στην Web υπηρεσία το όνομα του χρήστη ο οποίος είναι συνδεδεμένος με το συγκεκριμένο *ticket* και επιτρέπεται η περαιτέρω πρόσβαση του χρήστη στην υπηρεσία (4 στην Εικόνα). Ανάλογη διαδικασία ακολουθείται και στην περίπτωση όπου η υπηρεσία δεν είναι «καθαρής» Web τεχνολογίας αλλά έχει ένα πρώτο, εισαγωγικό, Web τμήμα (Γραμμές 4a & 5a στην Εικόνα). Όλες οι μεταφορές πληροφοριών κατά τις παραπάνω φάσεις γίνονται μέσω «ασφαλών» καναλιών με τη χρήση του πρωτοκόλλου SSL/TLS.

Για παράδειγμα, ας υποθέσουμε ότι ένας χρήστης με τον κωδικό "*webUser*" προσπελαύνει μία Web υπηρεσία της οποίας η πρώτη σελίδα απαιτεί αυθεντικοποίηση και η διεύθυνσή της είναι της μορφής:

http://www.yale.edu/tp/authenticate.jsp

Ο χρήστης κατευθύνεται στη *Login URL* του *CAS* με μία κλήση της μορφής:

https://secure.its.yale.edu/cas/login?service=http://www.yale.edu/tp/authenticate.jsp

Σε αυτή τη σελίδα ο χρήστης πρέπει να εισάγει τα στοιχεία ταυτότητάς του τα οποία ελέγχονται από την εξωτερική υπηρεσία αυθεντικοποίησης με την οποία «συνεργάζεται» ο *CAS* server. Μόλις γίνει επιτυχής επιβεβαίωση και παραχθεί το *ticket*, ο έλεγχος επιστρέφεται στην Web υπηρεσία με μία κλήση της μορφής:

http://www.yale.edu/tp/authenticate.jsp?ticket=opaque-ticket-string

Η συγκεκριμένη Web σελίδα θα πρέπει να είναι προγραμματισμένη έτσι ώστε να λαμβάνει ως παράμετρο κάποιο *ticket* το οποίο στη συνέχεια θα προωθεί για επιβεβαίωση στη *Validation URL* του *CAS* server μαζί τη διεύθυνση της ίδια της υπηρεσίες. Η *Validation URL* μπορεί να έχει τη μορφή:

https://secure.its.yale.edu/cas/servlet/validate

Ο *CAS* server ελέγχει το συγκεκριμένο *ticket* και επιστρέφει στην Web υπηρεσία (στη μορφή απλού κειμένου μέσω πρωτοκόλλου HTTP) δύο γραμμές, όπου η πρώτη περιέχει "*yes*", αν έλεγχος είναι επιτυχής, ή "*no*", αν έλεγχος είναι αποτυχημένος και η δεύτερη περιλαμβάνει το όνομα του χρήστη "*webUser*", μόνο στην περίπτωση επιτυχίας. Με αυτό τον τρόπο η Web υπηρεσία αυθεντικοποιεί το χρήστη χωρίς να χρειάζεται να γνωρίζει ή διαχειρίζεται τους κωδικούς ασφαλείας (passwords) του ή γενικά τις μεθόδους αυθεντικοποίησης. Αμέσως μετά την επιβεβαίωση ο *CAS* server καταστρέφει το συγκεκριμένο *ticket* [57].

Η έκδοση 2.0 του *CAS* επιδιώκει να λύσει προβλήματα που προκύπτουν από τη χρήση Web υπηρεσιών μέσα από ευρύτερα Portals, τα οποία επίσης είναι Web εφαρμογές. Για παράδειγμα, όταν ο χρήστης αυθεντικοποιείται προκειμένου να εισέλθει σε ένα Portal το οποίο βασίζεται στο *CAS*, εισάγει τα στοιχεία του στον *CAS* server και το Portal δεν «γνωρίζει» τα passwords του χρήστη, παρά μόνο δέχεται το Cookie *TGC* για την επίτευξη του Single Sign-On. Στην περίπτωση όμως που μία από τις υπηρεσίες του Portal είναι κάποιο Web ηλεκτρονικό ταχυδρομείο του οποίου ο server είναι προγραμματισμένος να δέχεται στοιχεία ταυτότητας χρηστών από το Portal, τότε πρέπει η εφαρμογή του Portal να λειτουργήσει ως «πληρεξούσιος» (proxy) του *CAS* server στον server του Web ηλ. ταχυδρομείου, ώστε να υλοποιηθεί και το Single Sign-On του αρχικού χρήστη. Στην έκδοση 2.0, επομένως, του CAS εισάγεται η έννοια του "*Proxy Granting Ticket – PGT*" το οποίο αποκτά μία proxy Web υπηρεσία και με αυτό μπορεί να ζητά από τον *CAS* server την «εξουσιοδότηση» να αυθεντικοποιήσει η ίδια έναν χρήστη για την πρόσβαση σε μία τρίτη Web υπηρεσία. Η «εξουσιοδότηση» δίνεται στον proxy μέσω του "*Proxy Ticket – PT*". Προκειμένου να υλοποιηθεί η έκδοση 2.0 του *CAS* η καθεμιά proxy εφαρμογή πρέπει να έχει υλοποιηθεί με κατάλληλο τρόπο ώστε να παρακολουθεί η ίδια τα *tickets* που ανταλλάσσει με τον *CAS* server και που μπορούν να αφορούν πρόσβαση σε διαφορετικές τρίτες υπηρεσίες από διαφορετικούς χρήστες [57].

2.4.3 "*WebAuth*" (Stanford University)

Το πρωτόκολλο *WebAuth* αναπτύχθηκε από το Πανεπιστήμιο του Stanford και η τρέχουσα έκδοσή του v3 δημοσιεύτηκε στις αρχές του 2003. Είναι και αυτό βασισμένο στο μηχανισμό των Cookies, λειτουργεί σε συνδυασμό με τον Web server Apache και τα server τμήματα του πρωτοκόλλου έχουν υλοποιηθεί στη γλώσσα προγραμματισμού C και στη γλώσσα Perl. Σχετικά με το μηχανισμό αυθεντικοποίησης των χρηστών, υποστηρίζεται το πρωτόκολλο *Kerberos 5*. Το πρωτόκολλο προβλέπει την ύπαρξη τριών βασικών συνιστωσών [132]:

- *User – Agent (UA)*: το πρόγραμμα Web browser του χρήστη. Η μόνη απαίτηση του πρωτοκόλλου είναι ο *UA* να υποστηρίζει Cookies.

- *WebAuth-enabled Application Server (WAS)*: ένας Web server ο οποίος διαχειρίζεται Web σελίδες και υπηρεσίες οι οποίες θα αυθεντικοποιούν τους χρήστες τους μέσω του πρωτοκόλλου *WebAuth*. Σε κάθε περίπτωση όπου ένας *UA* δεν «επιδείξει» σε ένα *WAS* το απαραίτητο Cookie το οποίο αποδεικνύει την αυθεντικοποίησή του σύμφωνα με το *WebAuth*, ο *WAS* θα κατευθύνει το χρήστη στο επόμενο τμήμα, το *WebKDC*.

- *WebKDC*: ο login server και το τμήμα του *WebAuth* το οποίο προσφέρει υπηρεσίες αυθεντικοποίησης στα δύο παραπάνω συστατικά, δεχόμενο κλήσεις σε δύο διαφορετικές διευθύνσεις URL. Στην πρώτη διεύθυνση «απαντά» ο login server ο οποίος αναμένει στην κλήση του την ύπαρξη ενός έγκυρου *WebAuth* Cookie. Σε περίπτωση όπου το Cookie είναι πραγματικό και τηρεί τις προδιαγραφές του *WebAuth*, ο χρήστης είναι έγκυρος, εγκρίνεται η πρόσβασή του και υλοποιείται έτσι το Single Sign-On. Σε αντίθετη περίπτωση (μη ύπαρξη ή εγκυρότητα του Cookie) ο χρήστης καλείται να εισάγει τα στοιχεία ταυτότητάς του (συνήθως username & password) σε ειδική φόρμα του *WebKDC* τα οποία και ελέγχονται με το κατάλληλο πρωτόκολλο (προεπιλεγμένο το *Kerberos 5*). Εφόσον το αποτέλεσμα του ελέγχου είναι επιτυχές, δημιουργούνται δύο *tokens*: το πρώτο το διατηρεί ο *WebKDC* για μελλοντικό έλεγχο του ίδιου χρήστη και το δεύτερο αποστέλλεται στον *UA*. Η δεύτερη διεύθυνση του *WebKDC* «απαντά» σε XML μηνύματα απευθείας από τον *WAS* μέσω πρωτοκόλλου HTTPS και αφορούν αιτήματα πιστοποίησης κλειδιών κωδικοποίησης πληροφοριών ή αιτήματα πρόσθετων στοιχείων ταυτότητας για ένα χρήστη.

Καθοριστικό ρόλο στη λειτουργία του πρωτοκόλλου έχουν τα *WebAuth tokens* τα οποία παρέχουν έναν τυπικό μηχανισμό ανταλλαγής και αποθήκευσης πληροφοριών οι οποίες είναι κρυπτογραφημένες και ασφαλείς τόσο από ανάγνωση ή μεταβολή από τρίτους. Τα *tokens* μεταφέρονται μεταξύ των servers εναλλακτικά: είτε ως παράμετροι στη URL διεύθυνση είτε ως δεδομένα της εντολής *POST* του HTTP είτε ως Cookies και έγγραφα XML. Είναι κρυπτογραφημένα με το μηχανισμό Συμμετρικής Κρυπτογράφησης "*Advanced Encryption Standard – AES*" (FIPS PUBS 197 [92]) με τη χρήση είτε ιδιωτικού κλειδιού είτε κοινού κλειδιού διάρκειας μίας συνόδου (session). Το πρωτόκολλο αυτή τη στιγμή προβλέπει εννέα *tokens* [132]:

1. *webkdc-service*: κρυπτογραφείται με ιδιωτικό κλειδί του *WebKDC*. Χρησιμοποιείται για την επικοινωνία του *WAS* και του *WebKDC* και περιέχει το κοινό κλειδί συνόδου το οποίο χρησιμοποιούν από κοινού οι *WAS* και *WebKDC*.

2. *webkdc-proxy*: κρυπτογραφείται με ιδιωτικό κλειδί του *WebKDC*. Περιέχει πιστοποιητικά ταυτότητας ενός χρήστη, μπορεί να αποκρυπτογραφηθεί μόνο από τον *WebKDC* καθώς μόνο αυτός διαθέτει το ιδιωτικό του κλειδί και η κύρια χρήση του είναι η υλοποίηση του Single Sign-On από τον *WebKDC*.

3. *request*: κρυπτογραφείται με κλειδί συνόδου. Περιέχει αίτηση ενός *WAS* για ένα *token*, κυρίως ταυτότητας (*id token*), από τον *WebKDC*. Κρυπτογραφείται με το μηχανισμό *AES* και περιλαμβάνει την URL διεύθυνση του αποστολέα, τον τύπο του *token* που ζητείται και ένα *webkdc-service token* στο οποίο υπάρχει το κλειδί συνόδου για την επικοινωνία *WAS – WebKDC*.

4. *error*: κρυπτογραφείται με κλειδί συνόδου. Επιστρέφεται από τον *WebKDC* στην περίπτωση εμφάνισης σημαντικού λάθους κατά την επεξεργασία ενός *request token*.

5. *id*: κρυπτογραφείται με κλειδί συνόδου. Περιέχει την ταυτότητα ενός χρήστη ο οποίος προσπαθεί να προσπελάσει ένα δικτυακό πόρο. Ο *WAS* θα επιβεβαιώσει το *id token* και στη συνέχεια θα δημιουργήσει ένα *app token* για μελλοντική χρήση.

6. *proxy*: κρυπτογραφείται με κλειδί συνόδου. Χρησιμοποιείται για την επιστροφή ενός *webkdc-proxy token* σε ένα *WAS*. Περιλαμβάνει πληροφορίες για το *webkdc-proxy token*, όπως η λήξη και ο τύπος του.

7. *cred*: κρυπτογραφείται με κλειδί συνόδου. Περιέχει ένα «πιστοποιητικό» για έναν χρήστη.

8. *login*: κρυπτογραφείται με ιδιωτικό κλειδί του *WebKDC*. Περιέχει το όνομα του χρήστη και τον κωδικό του (username & password) και χρησιμοποιείται εσωτερικά από το τμήμα *Weblogin* του *WebKDC* για τη δημιουργία του αρχικού *webkdc-proxy token*.

9. *app*: κρυπτογραφείται με ιδιωτικό κλειδί του *WAS*. Χρησιμοποιείται από ένα *WAS* για την αποθήκευση δεδομένων ταυτότητας ενός χρήστης για μελλοντική χρήση, μετά την επιβεβαίωσή του με ένα *id token* ή *proxy token*.

Η λειτουργία του πρωτοκόλλου προβλέπει τέσσερα «σενάρια» [132]:

- *No Tokens (Initial Sign-On) – (Εικόνα 28)*: Ένας χρήστης επιχειρεί να προσπελάσει έναν προστατευμένο με *WebAuth* δικτυακό πόρο χωρίς να υπάρχουν Cookies αυθεντικοποίησης, δηλαδή *app token* ή *proxy token* στον *UA*. Στην αρχή ο *WAS* ζητά την αυθεντικοποίησή του από τον *WebKDC* και καταλήγει να παραλάβει ένα *webkdc-service token* και ένα κλειδί συνόδου. Αυτά τα αρχικά βήματα (βήματα 1 & 2) εφαρμόζονται επίσης σε καθένα από τα υπόλοιπα «σενάρια». Στη συνέχεια ο *UA* ζητά από τον *WAS* να προσπελάσει έναν δικτυακό πόρο (βήμα 3). Ο *WAS* δεν έχει κάποιο *app token* για το συγκεκριμένο *UA* και σχηματίζει ένα *request token* ζητώντας ένα *id token*, ενώ παράλληλα κατευθύνει το χρήστη στο τμήμα *WebLogin* του *WebKDC* για την εισαγωγή των στοιχείων ταυτότητάς του ενσωματώνοντας στη διεύθυνση URL το *request token* (βήμα 4). Μέσω της συγκεκριμένης «ανακατεύθυνσης» το *request token* αποστέλλεται στον *WebKDC* (βήμα 5). Ο *WebKDC* αποκρυπτογραφεί το *request token* και επιστρέφει στο χρήστη την κατάλληλη φόρμα καταχώρησης των προσωπικών του στοιχείων (βήμα 6). Ο χρήστης καταχωρεί τα στοιχεία αυθεντικοποίησής του και ο *UA* τα προωθεί στον *WebKDC* (βήμα 7). Ο *WebKDC* ελέγχει την ορθότητα των στοιχείων του χρήστη και εφόσον αυτός προκύψει έγκυρος δημιουργεί ένα *webkdc-proxy token* και ένα *id token* και εμφανίζει στον *UA* μία σελίδα έγκρισης του χρήστη στην οποία περιλαμβάνει μία σύνδεση προς τον *WAS* με ενσωματωμένο το *id token* (βήμα 8). Μόλις ο χρήστης ακολουθήσει τη σύνδεση της εγκριτικής σελίδας, ο *UA* θα ζητήσει ξανά την προσπέλαση του αρχικού δικτυακού πόρου, αλλά με το *id token* περιλαμβανόμενο στη διεύθυνση URL (βήμα 9). Ο *WAS* θα εντοπίσει το *id token* στη URL διεύθυνση και θα ελέγξει την «ηλικία» του και την εγκυρότητά του. Μόλις οι έλεγχοι ολοκληρωθούν ο *WAS* θα δημιουργήσει ένα *app token*, θα το μεταβιβάσει ως Cookie στον *UA* για μελλοντικές αιτήσεις του *UA* και θα προωθήσει το χρήστη στην αιτούμενη δικτυακή υπηρεσία (βήμα 10).

Πηγή: [132]

```
-------------------------------------------------------------
     UA                 WAS            WebKDC
  -------------------------------------------------------------
                        send K5 auth for webkdc-service token
  1.                    WAS ---------> WebKDC

                        return session key, webkdc-service token
  2.                    WAS <--------- WebKDC

     request resource
  3.  -----------------> WAS

     redirect to WebKDC w/request token asking for id token
  4.  <----------------- WAS

     pass along request token
  5.  ------------------------------> WebKDC

     login form sent back
  6.  <------------------------------ WebKDC

     post login form with user authentication (password)
  7.  ------------------------------> WebKDC

     confirmation page sent back, link contains id token
  8.  <------------------------------ WebKDC

     re-request resource (with returned id token in URL)
  9.  -----------------> WAS

     set the app token cookie, response from app
  10. <----------------- WAS

  -------------------------------------------------------------
```

Εικόνα 28: Πρώτο «Σενάριο» Λειτουργίας του *WebAuth*

- *App Token – (Εικόνα 29)*: Ένας χρήστης επιχειρεί να προσπελάσει έναν προστατευμένο με *WebAuth* δικτυακό πόρο και έχει ήδη στην κατοχή του ένα *app token* σε ένα Cookie. Τα βήματα 1 & 2 του προηγούμενου σεναρίου θα εφαρμοστούν και σε αυτή την περίπτωση. Στη συνέχεια ο *UA* ζητάει από τον *WAS* πρόσβαση στις προστατευόμενες υπηρεσίες περιλαμβάνοντας στην αίτησή του το *app token* (βήμα 1). Ο *WAS* αποκρυπτογραφεί το *token* με το ιδιωτικό του κλειδί, επιβεβαιώνει την ταυτότητα του χρήστη από το περιεχόμενο του *token* και προωθεί το «αίτημα» του χρήστη στη ζητούμενη προστατευόμενη υπηρεσία (βήμα 2).

Πηγή: [132]

```
-------------------------------------------------------------
     UA                 WAS            WebKDC
  -------------------------------------------------------------
    request resource
  1.  -----------------> WAS

     response
  2.  <----------------- WAS
  -------------------------------------------------------------
```

Εικόνα 29: Δεύτερο «Σενάριο» Λειτουργίας του *WebAuth*

- *No App Token, Proxy Token (Single Sign-On) – (Εικόνα 30)*: Ένας χρήστης επιχειρεί να προσπελάσει έναν προστατευμένο με *WebAuth* δικτυακό πόρο και δεν έχει *app token* για

τον συγκεκριμένο *WAS*, αλλά έχει ένα *webkdc-proxy token* (σε ένα Cookie) για τον *WebKDC*. Η συγκεκριμένη περίπτωση είναι το Single Sign-On, καθώς ο χρήστης έχει αυθεντικοποιηθεί ήδη από τον *WebAuth* server για κάποια υπηρεσία και επιθυμεί την προσπέλαση κάποιας άλλης υπηρεσίας χωρίς την επανάληψη της διαδικασίας αυθεντικοποίησης. Τα βήματα 1 & 2 του πρώτου σεναρίου θα εφαρμοστούν και σε αυτή την περίπτωση. Στη συνέχεια ο *UA* ζητάει από τον *WAS* πρόσβαση στην προστατευόμενη υπηρεσία χωρίς να περιλαμβάνει στην αίτησή του κάποιο *app token* (βήμα 1). Ο *WAS*, επομένως, δημιουργεί ένα *request token* ζητώντας ένα *id* token (βήμα 2). Ο χρήστης στη συνέχεια κατευθύνεται στο τμήμα *Weblogin* του *WebKDC* περιλαμβάνοντας στην κλήση του το *request token* του προηγούμενο βήματος και ένα Cookie με το *webkdc-proxy token* που ήδη διαθέτει (βήμα 3). Ο *WebKDC* εντοπίζει και αποκρυπτογραφεί το *webkdc-proxy token* με το ιδιωτικό του κλειδί και το χρησιμοποιεί για τη δημιουργία του νέου *id token* το οποίο και ενσωματώνει στη σύνδεση προς τον *WAS* μέσα στη σελίδα επιβεβαίωσης που επιστρέφει στο χρήστη (βήμα 4). Μόλις ο χρήστης ακολουθήσει αυτή τη σύνδεση, ο *UA* στέλνει νέα αίτηση για την προστατευόμενη υπηρεσία περιλαμβάνοντας αυτή τη φορά το νέο *id token* στη URL διεύθυνση (βήμα 5). Ο *WAS* επιβεβαιώνει το *id token*, δημιουργεί ένα νέο *app token* το οποίο επιστρέφεται στο χρήστη σε ένα Cookie, ενώ παράλληλα προωθεί τον έλεγχο στη ζητούμενη υπηρεσία (βήμα 6).

Πηγή: [132]

```
-------------------------------------------------------------
      UA                 WAS            WebKDC
-------------------------------------------------------------
      request resource
  1.  -----------------> WAS

      redirect to WebKDC w/request token asking for id token
  2.  <----------------- WAS

      pass along request token
  3.  ------------------------------> WebKDC

      confirmation page sent back, link contains id token
  4.  <------------------------------ WebKDC

      re-request resource (with returned id token in URL)
  5.  -----------------> WAS

      set the app token cookie, response from app
  6.  <----------------- WAS

  -------------------------------------------------------------
```

Εικόνα 30: Τρίτο «Σενάριο» Λειτουργίας του *WebAuth*

- <u>*No App Token, Credentials Required – (Εικόνα 31)*</u>: Ένας χρήστης επιχειρεί να προσπελάσει έναν προστατευμένο με *WebAuth* δικτυακό πόρο ο οποίος όμως απαιτεί στοιχεία «εξουσιοδότησης» ώστε να ενεργήσει ως εκπρόσωπος (proxy) του χρήστη για την απόκτηση από τον *WebKDC* περαιτέρω στοιχείων ταυτότητάς του (*credentials*). Σε αυτή την περίπτωση ο *WAS* θα ζητήσει το *webkdc-proxy token* το οποίο θα χρησιμοποιήσει στη συνέχεια για να ζητήσει περαιτέρω «πιστοποίηση» μέσω XML κλήσεων. Τα βήματα 1 & 2 του πρώτου σεναρίου θα εφαρμοστούν και σε αυτή την περίπτωση. Στη συνέχεια ο *UA* ζητάει από τον *WAS* πρόσβαση στην προστατευόμενη υπηρεσία χωρίς να περιλαμβάνει στην αίτησή του κάποιο *app token* (βήμα 1). Ο *WAS*, επομένως, δημιουργεί ένα *request token* ζητώντας ένα *proxy token* (βήμα 2). Ο χρήστης στη συνέχεια κατευθύνεται στο τμήμα *Weblogin* του *WebKDC* περιλαμβάνοντας στην κλήση του το *request token* του

προηγούμενο βήματος και ένα Cookie με το *webkdc-proxy token* που διαθέτει ήδη, καθώς το σενάριο υποθέτει ότι έχει γίνει προηγούμενη αυθεντικοποίηση (βήμα 3). Όπως στα προηγούμενα «σενάρια» ο *WebKDC* δημιουργεί τη σελίδα επιβεβαίωσης στην οποία τώρα περιλαμβάνεται το *proxy token* προς τον *WAS* (βήμα 4). Με την κλήση της σύνδεσης από το χρήστη ο *WAS* παραλαμβάνει το *proxy token* (βήμα 5). Ο *WAS* εντοπίζει τα δύο *tokens*: το *webkdc-service token* και το *webkdc-proxy token* και στέλνει XML αίτηση απευθείας στον *WebKDC* για ένα δικό του *id token* και *cred token* (βήμα 6). Ο *WebKDC* παραλαμβάνει το αίτημα του *WAS* και τα δύο *tokens* και αφού τα εξετάσει δημιουργεί τα απαιτούμενα *tokens* απάντησης (βήμα 7). Ο *WAS* παραλαμβάνει το *id token* και δημιουργεί ένα *app token* για ενδεχόμενη μελλοντική αυθεντικοποίηση και ο έλεγχος μεταφέρεται στη ζητούμενη υπηρεσία μαζί με όλα τα Cookies που πρέπει να διατηρήσει ο *UA* (βήμα 8).

Πηγή: [132]

```
-----------------------------------------------------------------
      UA                 WAS            WebKDC
-----------------------------------------------------------------
     request resource
  1.  -----------------> WAS

      redirect to WebKDC w/request token asking for proxy token
  2.  <----------------- WAS

      pass along request token
  3.  ------------------------------------> WebKDC

      confirmation page sent back, contains proxy token
  4.  <------------------------------------ WebKDC

      re-request resource (with returned proxy token in URL)
  5.  -----------------> WAS

                             send proxy token with request
  6.                     WAS -------------> WebKDC

                             returns credential token
  7.                     WAS <------------- WebKDC

      set the app token cookie, response from app
  8.  <----------------- WAS

  ---------------------------------------------------------------
```

Εικόνα 31: Τέταρτο «Σενάριο» Λειτουργίας του *WebAuth*

2.4.4 "*Pubcookie*" (University of Washington)

Το *Pubcookie* δημιουργήθηκε στο Πανεπιστήμιο της Washington το 1998. Το 2001 διατέθηκε ελεύθερα ως ένα ολοκληρωμένο πακέτο διαχείρισης εγγραφής χρηστών σε Web πόρους, ενώ παράλληλα στελέχη από τα Πανεπιστήμια Carnegie Mellon και Wisconsin σχημάτισαν την ομάδα έργου του *Pubcookie*. Η τρέχουσα έκδοση του προϊόντος είναι η 3.3.1. Βασίζεται και αυτό στον μηχανισμό των Cookies και τα τμήματα που ορίζει το μοντέλο του *Pubcookie* είναι [148]:

- *UA (User Agent)*: το πρόγραμμα Web browser του χρήστη. Πρέπει να υποστηρίζει Cookies, ώστε να δέχεται τα Cookies του *Login* και *Application Server*.

- *Login Server*: παρέχει τις υπηρεσίες κεντρικής αυθεντικοποίησης. Αλληλεπιδρά απευθείας με τους χρήστες και επιβεβαιώνει τα στοιχεία ταυτότητάς τους χρησιμοποιώντας κάποιον εξωτερικό μηχανισμό αυθεντικοποίησης. Χρησιμοποιεί Cookies για τους χρήστες, ώστε να παρέχει το μηχανισμό Single Sign-On, αλλά και για την παροχή πληροφοριών αυθεντικοποίησης προς τον *Application Server*.

- *Application Server*: εξασφαλίζει την προστασία των δικτυακών εφαρμογών με την υποχρέωση του χρήστη να αυθεντικοποιηθεί προκειμένου να τις προσπελάσει, καθώς όποιοι χρήστες δεν έχουν αυθεντικοποίηση *Pubcookie* κατευθύνονται στον *Login Server*. Επικυρώνει τις πληροφορίες αυθεντικοποίησης που επιστρέφονται από τον *Login Server* και παρέχει πληροφορίες αυθεντικοποίησης των χρηστών στις δικτυακές εφαρμογές. Πρακτικά υλοποιείται από επεκτάσεις του *Pubcookie* σε υπάρχοντες Web Servers Apache ή Microsoft IIS.

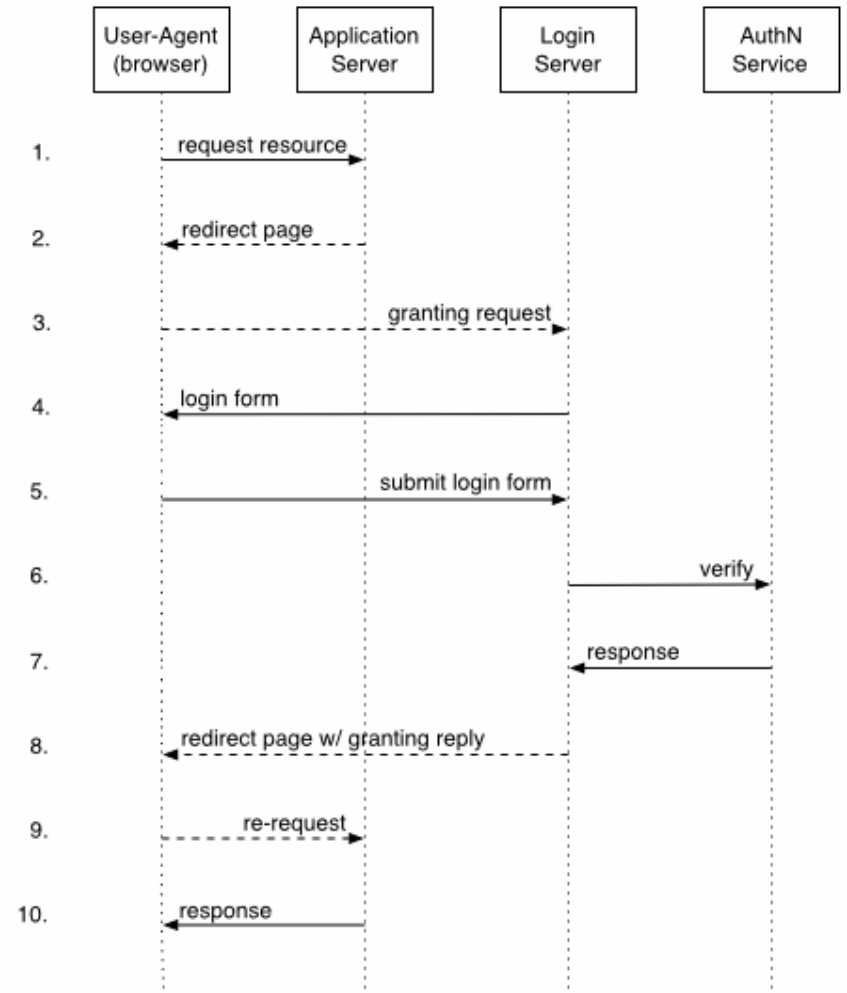
- *Authentication Service*: είναι ο εξωτερικός μηχανισμός ο οποίος ελέγχει και επιβεβαιώνει τα δεδομένα ταυτότητας των χρηστών τα οποία αποστέλλονται από τον *Login Server*.

Η εγκατάσταση των συστατικών του *Pubcookie* απαιτεί την εγκατάσταση ενός *Login Server* και τουλάχιστον ενός *Application Server* ο οποίος περιέχει τουλάχιστον μία προστατευόμενη από το *Pubcookie* δικτυακή εφαρμογή. Πριν την έναρξη λειτουργίας του *Pubcookie* ο *Login* και ο *Application Server* συμφωνούν σε ένα κοινό, συμμετρικό κλειδί το οποίο θα χρησιμοποιούν στην κρυπτογράφηση μηνυμάτων που θα ανταλλάσσουν. Επιπροσθέτως, ο *Application Server* ενημερώνεται για το δημόσιο κλειδί του *Login Server*. Τα σενάρια λειτουργίας του πρωτοκόλλου *Pubcookie* είναι [148]:

- *Initial Sign-on Process*: Είναι η φάση της αρχικής εισαγωγής του χρήστη στο προστατευόμενο από το *Pubcookie* Portal (Εικόνα 32 – βήμα 1). Ο *Application Server* ελέγχει την ύπαρξη των απαραίτητων πληροφοριών αυθεντικοποίησης στην κλήση που δέχτηκε. Από τη στιγμή που δε θα τις εντοπίσει, δημιουργεί μία «απάντηση» η οποία περιλαμβάνει μία σύνδεση προς τον *Login Server* και δύο Cookies: ένα που σχετίζεται με τη ζητούμενη υπηρεσία και ένα με το οποίο ζητείται αυθεντικοποίηση από τον *Login Server* (βήμα 2). Στο επόμενο βήμα 3 ο χρήστης κατευθύνεται προς τον *Login Server* μεταφέροντας σε αυτόν το Cookie με την αίτηση για «άδεια εισόδου» στο σύστημα, η οποία περιλαμβάνει και πρόσθετες πληροφορίες που ενδιαφέρουν τον *Login Server* (URL της υπηρεσίας, επιθυμητός βαθμός αυθεντικοποίησης κλπ). Ο *Login Server* αποκωδικοποιεί το περιεχόμενο του Cookie και εμφανίζει στο χρήστη την απαραίτητη φόρμα εισαγωγής των στοιχείων ταυτότητάς του (βήμα 4). Ο χρήστης οφείλει να εισάγει τα στοιχεία του (συνήθως username & password) τα οποία αποστέλλονται στον *Login Server* (βήμα 5). Στη συνέχεια, τα συγκεκριμένα στοιχεία προωθούνται στην εξωτερική υπηρεσία αυθεντικοποίησης προς επιβεβαίωση (βήμα 6). Αμέσως μόλις ο *Login Server* παραλάβει αυτή την επιβεβαίωση (βήμα 7), δημιουργεί μία απάντηση η οποία περιλαμβάνει δύο Cookies: το πρώτο ονομάζεται *granting cookie* και περιέχει μεταξύ άλλων το έγκυρο όνομα του χρήστη. Το συγκεκριμένο Cookie έχει ως σκοπό να χρησιμοποιείται από τον *Application Server* και προστατεύεται με κρυπτογράφησή του με το ιδιωτικό κλειδί του *Login Server* (Κρυπτογράφηση Δημοσίου Κλειδιού) και με την περαιτέρω κρυπτογράφησή του με το συμμετρικό κλειδί που μοιράζονται με τον *Application Server* (Κρυπτογράφηση Ιδιωτικού Κλειδιού).

Το δεύτερο Cookie ονομάζεται *login cookie* και σκοπός του είναι να αποστέλλεται στον *Login Server* σε ενδεχόμενες επόμενες κλήσεις του ίδιου χρήστη (βήμα 8). Ο χρήστης πρέπει να ξανακαλέσει την αρχική σελίδα της ζητούμενης υπηρεσίας, αλλά στην κλήση του περιλαμβάνεται τώρα το *granting cookie* του προηγούμενου βήματος και το πρώτο Cookie που δημιουργήθηκε στο βήμα 2 από τον *Application Server* (βήμα 9). Ο *Application Server* βρίσκει τα δύο Cookies στην κλήση του χρήστη και αποκρυπτογραφεί το *granting cookie* με το συμμετρικό κλειδί που μοιράζεται με τον *Login Server* και επιβεβαιώνει την ορθότητα της προέλευσής του αποκρυπτογραφώντας το περαιτέρω και με το δημόσιο κλειδί του *Login Server*. Στην περίπτωση όπου όλοι οι έλεγχοι είναι επιτυχείς δημιουργείται ένα Cookie συνόδου (*session cookie*) για επόμενες κλήσεις του χρήστη στη συγκεκριμένη υπηρεσία και ο *Application Server* προωθεί τον έλεγχο και το όνομα του χρήστη προς την προστατευόμενη υπηρεσία (βήμα 10).

Πηγή: [148]



Εικόνα 32: Βασικό «Σενάριο» Λειτουργίας του *Pubcookie*

- <u>*Single Sign – On*</u>: Στην περίπτωση που ο χρήστης επιθυμεί την προσπέλαση σε μία νέα δικτυακή υπηρεσία, ενώ έχει ήδη αυθεντικοποιηθεί για κάποια άλλη, τα βήματα που αναλύθηκαν παραπάνω θα είναι τα ίδια μέχρι το βήμα 3, όπου τώρα ο χρήστης θα ενσωμα-

τώσει το *login cookie* που του είχε επιστρέψει ο *Login Server* κατά την προηγούμενη αυθεντικοποίησή του. Ο *Login Server* δεν ξαναζητά τα στοιχεία του χρήστη και δημιουργεί ένα νέο *granting cookie* με τα στοιχεία που εντοπίζει μέσα στο *login cookie*. Με αυτό τον τρόπο ο χρήστης αποκτά πρόσβαση στη νέα προστατευόμενη υπηρεσία χωρίς την επανάληψη καταχώρισης των στοιχείων και αυτό μπορεί να επαναληφθεί για όσο χρόνο παραμένει έγκυρο το αρχικό του *login cookie* (πχ 8 ώρες από την αρχική είσοδό του)

- Logging Out: Στην περίπτωση όπου ο χρήστης επιθυμεί την έξοδό του από τους δικτυακούς πόρους για τους οποίους έχει αυθεντικοποιηθεί μπορεί απλώς να κλείσει τον Web browser του. Με το κλείσιμο της συνόδου (session) τα Cookies που έχει αποκτήσει καταστρέφονται και χάνουν την ισχύ τους. Σε πολλές περιπτώσεις, όμως, οι Web browsers διατηρούν ενεργά τα Cookies για κάποιο χρονικό διάστημα, οπότε το *Pubcookie* προσφέρει τη λειτουργικότητα εξόδου (log out) από το σύστημα και διαγραφής των στοιχείων αυθεντικοποίησης που διατηρούν για το συγκεκριμένο χρήστη. Η λεπτομέρεια ,όμως, στη συγκεκριμένη λειτουργικότητα είναι ότι πρέπει να γίνει log out για καθεμία υπηρεσία την οποία έχει προσπελάσει ο χρήστης ξεχωριστά.

2.4.5 Η Προδιαγραφή *WS-Federation* και τα *Active Directory Federation Services* (*ADFS*) του Microsoft Windows Server 2003

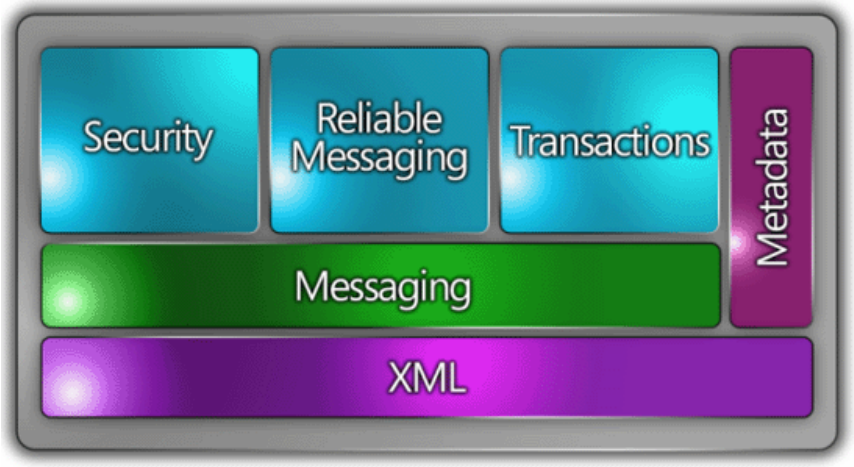
Μία ακόμα εφαρμογή Web Single Sign-On, αλλά και υλοποίηση *Federated Identity Management*, πραγματοποιείται στο Λειτουργικό Σύστημα Windows Server 2003 της Microsoft με τις υπηρεσίες *Active Directory Federation Services* (*ADFS*). Οι *ADFS* βασίζονται στην υπηρεσία καταλόγου *Active Directory* μέσα από την οποία εξασφαλίζεται ενιαία αυθεντικοποίηση (Single Sign – On) για τους χρήστες των πόρων του τοπικού δικτύου της καθεμιάς εγκατάστασης του Windows Server 2003. Τα βασικά χαρακτηριστικά των *ADFS* είναι [115]:

- Federation & Web SSO: η εφαρμογή του *Active Directory* εξασφαλίζει λειτουργικότητα SSO στα πλαίσια των *Domains* και του *Forest* ενός οργανισμού μέσω της αυθεντικοποίησης των Windows. Οι *ADFS* επεκτείνουν αυτή τη λειτουργικότητα στις εφαρμογές που προσπελαύνονται από το Internet, ώστε οι πελάτες και οι συνεργάτες ενός οργανισμού να έχουν Web SSO αντιμετώπιση όταν χρησιμοποιούν τις Web – based εφαρμογές του. Επιπροσθέτως, η εγκατάσταση των *ADFS* μπορεί να επεκταθεί σε πολλαπλούς συνεργαζόμενους οργανισμούς ώστε να εφαρμοστεί *Federated* διαχείριση των χρηστών τους.

- *Διαλειτουργικότητα με τις Web Services (WS-*)*: Οι *ADFS* εξασφαλίζουν διαλειτουργικότητα με άλλα προϊόντα ασφάλειας τα οποία υποστηρίζουν την αρχιτεκτονική προδιαγραφών Web Services: *WS-**. Η αρχιτεκτονική *WS-** αποτελεί τη συνολική πρόταση υλοποίησης Web Services με βάση διεθνώς αναγνωρισμένα πρότυπα τα οποία ικανοποιούν όσο το δυνατό περισσότερες απαιτήσεις, όπως ασφάλεια, αξιόπιστη μετάδοση δεδομένων, συνημμένα τμήματα δεδομένων κλπ (βλ παρακάτω Εικόνα). Ατομικά η καθεμιά προδιαγραφή λύνει μία συγκεκριμένη απαίτηση, ενώ σε συνεργασία εξασφαλίζουν υψηλού επιπέδου λειτουργικότητα η οποία απαιτείται σε κατανεμημένες εφαρμογές, ώστε οι προγραμματιστές να επιλέγουν μόνο τις προδιαγραφές που απαιτούνται από την καθεμιά εφαρμογή. Η συγκεκριμένη αρχιτεκτονική βασίζεται στην ιδέα ότι τα πραγματικά επιχειρηματικά μοντέλα έχουν αναπτυχθεί σε διαφορετικές γλώσσες και πλατφόρμες, άρα οι Web Services πρέπει να προσφέρουν τρόπους ανάπτυξης Web εφαρμογών οι οποίες να μπορούν να επι-

κοινωνούν αποδοτικά και να ανταλλάσσουν δεδομένα μέσα από το Internet (Διαλειτουργικότητα).

Πηγή: [127]



Εικόνα 33: Σχηματική Αναπαράσταση της Αρχιτεκτονικής *WS-

Για καθένα τμήμα της παραπάνω αναπαράστασης η αρχιτεκτονική *WS-** προτείνει διαφορετικές προδιαγραφές πρωτοκόλλων. Στο τμήμα της ανταλλαγής μηνυμάτων επικρατεί η προδιαγραφή των SOAP μηνυμάτων, επομένως τα τμήματα πάνω από αυτό επεκτείνουν τη γενική προδιαγραφή για την ικανοποίηση πιο σύνθετων - εξειδικευμένων απαιτήσεων Internet επικοινωνίας. Ειδικά για το τμήμα της Ασφάλειας (*Security*) προτείνεται η γενική προδιαγραφή *WS-Security* με την οποία προδιαγράφεται η πρόταση των εταιριών Microsoft, IBM, BEA Systems, RSA, VeriSign κ.α., μέσω του Οργανισμού *OASIS*, για την επέκταση του προτύπου SOAP για την ασφάλεια και προστασία των μηνυμάτων και την ενσωμάτωση πληροφοριών ασφάλειας στο συντακτικό των SOAP μηνυμάτων [106]. Τα συγκεκριμένα τμήματα πληροφοριών ονομάζονται γενικά *Security Tokens* και μπορεί να είναι Ψηφιακά Πιστοποιητικά του πρωτοκόλλου X.509, *Tickets* του πρωτοκόλλου *Kerberos*, *Tokens* του πρωτοκόλλου *SAML*, απλά usernames/passwords κλπ. Ένα παράδειγμα μηνύματος με ενσωματωμένο *Security Token* φαίνεται στην παρακάτω Εικόνα:

Πηγή: [106]

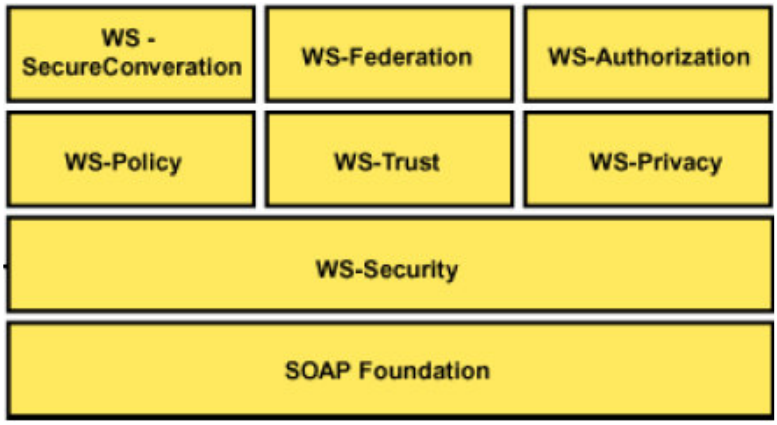
```
(001) <?xml version="1.0" encoding="utf-8"?>
(002) <S11:Envelope xmlns:S11="..." xmlns:wsse="..." xmlns:wsu="..."
            xmlns:ds="...">
(003)   <S11:Header>
(004)      <wsse:Security
             xmlns:wsse="...">
(005)         <xxx:CustomToken wsu:Id="MyID"
                                xmlns:xxx="http://fabrikam123/token">
(006)             FHUIORv...
(007)         </xxx:CustomToken>
(008)         <ds:Signature>
(009)            <ds:SignedInfo>
(010)               <ds:CanonicalizationMethod
                        Algorithm=
                          "http://www.w3.org/2001/10/xml-exc-c14n#"/>
(011)               <ds:SignatureMethod
                        Algorithm=
                        "http://www.w3.org/2000/09/xmldsig#hmac-sha1"/>
(012)               <ds:Reference URI="#MsgBody">
(013)                  <ds:DigestMethod
                          Algorithm=
                        "http://www.w3.org/2000/09/xmldsig#sha1"/>
(014)                  <ds:DigestValue>LyLsF0Pi4wPU...</ds:DigestValue>
(015)               </ds:Reference>
(016)            </ds:SignedInfo>
(017)            <ds:SignatureValue>DJbchm5gK...</ds:SignatureValue>
(018)            <ds:KeyInfo>
(019)                <wsse:SecurityTokenReference>
(020)                   <wsse:Reference URI="#MyID"/>
(021)                </wsse:SecurityTokenReference>
(022)            </ds:KeyInfo>
(023)         </ds:Signature>
(024)      </wsse:Security>
(025)   </S11:Header>
(026)   <S11:Body wsu:Id="MsgBody">
(027)     <tru:StockSymbol xmlns:tru="http://fabrikam123.com/payloads">
              QQQ
          </tru:StockSymbol>
(028)   </S11:Body>
(029) </S11:Envelope>
```

Εικόνα 34: Παράδειγμα Μηνύματος με *Security Token* Σύμφωνα με την Προδιαγραφή WS-Security

Η περιγραφή του *Security Token* περιλαμβάνεται ανάμεσα στα στοιχεία *<wsse:Security>* και *</wsse:Security>* (γραμμές 4 – 24). Το συγκεκριμένο *Security Token* είναι οριζόμενο από το χρήστη και όχι κάποιου διαδεδομένου μηχανισμού και συνοδεύται από μία ψηφιακή υπογραφή η οποία εξασφαλίζει τον έλεγχο ακεραιότητάς του κατά τη μετάδοση του μηνύματος (γραμμές 8 – 23).

Η προδιαγραφή *WS-Security* εξειδικεύεται περαιτέρω ώστε να περιλαμβάνει πιο συγκεκριμένες περιπτώσεις μεταβίβασης πληροφοριών ασφαλείας (βλ παρακάτω Εικόνα) [45]:

Πηγή: [45]



Εικόνα 35: Σχηματική Αναπαράσταση των Προδιαγραφών της Αρχιτεκτονικής *WS-

- *WS-Policy*: περιγράφει τις δυνατότητες και περιορισμούς των πολιτικών ασφαλείας σε ενδιάμεσους παραλήπτες και τελικούς αποδέκτες μηνυμάτων (πχ απαιτούμενα *Security Tokens*, υποστηριζόμενοι αλγόριθμοι κρυπτογράφησης κλπ) [7]. Η συγκεκριμένη προδιαγραφή συμπληρώνεται με επιμέρους, εξειδικευμένες προδιαγραφές:

  WS-Policy-Attachment: περιγράφει τον τρόπο επισύναψης των πολιτικών ασφαλείας σε Web Services [6].

  WS-Policy-Assertions: περιγράφει ένα σύνολο από δηλώσεις που μπορούν να γίνουν στα πλαίσια της διατύπωσης μίας γενικότερης πολιτικής ασφαλείας [5].

  WS-Security Policy: περιγράφει ένα βασικό σύνολο από δηλώσεις ασφαλούς διακίνησης των μηνυμάτων SOAP, των μηνυμάτων *WS-Trust* και των μηνυμάτων *WS-SecureConversation* [50].

- *WS-Trust*: περιγράφει το υπόβαθρο για την ανάπτυξη «έμπιστων» μοντέλων με τα οποία μπορούν δύο συναλλασσόμενες Web Services να θεωρήσουν η μία την άλλη «έμπιστη» για την ελεύθερη ανταλλαγή προστατευμένων πληροφοριών. Με το όρο «έμπιστοι συνέταιροι» εννοούνται: τρίτοι οργανισμοί, τμήματα ή υποκαταστήματα του ίδιου οργανισμού τα οποία έχουν συνάψει συμφωνίες και μεθόδους αμοιβαίας ανταλλαγής υπηρεσιών και πληροφοριών ταυτότητας χρηστών τους [49].

- *WS-Privacy*: περιγράφει το μοντέλο βάσει του οποίου οι Web Services θα δηλώνουν τις επιλογές και πρακτικές εμπιστευτικότητας οι οποίες εφαρμόζονται σε έναν οργανισμό.

- *WS-SecureConversation*: περιγράφει τον τρόπο διαχείρισης και αυθεντικοποίησης μηνυμάτων τα οποία ανταλλάσσονται μεταξύ δύο συνδιαλεγόμενων μερών, εγκαθιστώντας το περιβάλλον ασφαλείας και τα απαραίτητα κλειδιά που ενδεχομένως απαιτηθούν για την περαιτέρω συνομιλία τους [48].

- *WS-Federation*: περιγράφει μηχανισμούς για την ανταλλαγή δεδομένων ταυτότητας, ιδιοτήτων χρηστών, αυθεντικοποίησης και εξουσιοδότησης χρηστών μεταξύ «έμπιστων» οργανισμών. Η προδιαγραφή *WS-Federation* εξασφαλίζει την επικοινωνία των συγκεκριμένων δεδομένων μεταξύ των έμπιστων μερών ανεξάρτητα από τη χρήση μοντέλου διαχείρισης ταυτοτήτων των Windows [4]. Οι γενικές αρχές της προδιαγραφής εξειδικεύονται περαιτέρω σε ξεχωριστούς μηχανισμούς ανάλογα με

το είδος των εφαρμογών στα συναλλασσόμενα μέρη που αιτούνται δεδομένα και υπηρεσίες (*requestors*). Συγκεκριμένα, αν ο *requestor* του *WS-Federation* είναι ένας Web Browser που μπορεί να υποστηρίξει το πρωτόκολλο HTTP (πχ HTTP/1.1) τότε ο *requestor* ονομάζεται "*passive*" και ισχύει η εξειδικευμένη προδιαγραφή *WS-Federation: Passive Requestor Profile* [8]. Αντίθετα, όταν ο *requestor* είναι μία διακτυακή εφαρμογή η οποία μπορεί να αποστείλει μηνύματα της μορφής των Web Services, όπως αυτά που περιγράφονται στις προδιαγραφές *WS-Trust* και *WS-Security*, τότε ο *requestor* ονομάζεται "*active*" και η εξειδικευμένη προδιαγραφή *WS-Federation: Active Requestor Profile* [47]. Είναι προφανές ότι ο όρος "*profile*" στις παραπάνω προδιαγραφές αναφέρεται στο σύνολο των συγκεκριμένων παραμέτρων με τους οποίους μπορεί να εφαρμοστεί η γενική προδιαγραφή *WS-Federation* στα δύο είδη *requestors*. Ειδικά τα *profile* του *Passive Requestor* εξειδικεύεται ακόμα περισσότερο με τον ακριβή καθορισμό του είδους των μηνυμάτων που θα ανταλλάσσονται μεταξύ διαφορετικών *Realms* για την εξασφάλιση διαλειτουργικότητας, με την προδιαγραφή: *WS-Federation Passive Requestor Interoperability Profile* [44].

- *WS-Authorization*: περιγράφει τον τρόπο διαχείρισης δεδομένων και πολιτικών εξουσιοδότησης και ελέγχου πρόσβασης σε εφαρμογές και υπηρεσίες.

❖ <u>*Επέκταση του Active Directory στο Internet:*</u> Με την εφαρμογή του *Active Directory* είναι εφικτή η διαμοίραση της πρόσβασης σε πόρους οι οποίοι βρίσκονται σε διαφορετικές επιχειρηματικές οντότητες ή οργανισμούς και ανήκουν στα ίδια ή διαφορετικά *Forests*. Οι *ADFS* επεκτείνουν αυτή τη δυνατότητα του *Active Directory* ώστε να υλοποιείται η πρόσβαση σε πόρους από επιλεγμένους «έμπιστους συνεταίρους» μέσα από το Internet. Οι *ADFS* λειτουργούν σε στενή συνεργασία με το *Active Directory*: διαβάζουν τα δεδομένα των χρηστών από αυτό και αυθεντικοποιούν τους χρήστες κάνοντας χρήση των υποστηριζόμενων τεχνολογιών «ισχυρής» αυθεντικοποίησης (ψηφιακά πιστοποιητικά X.509, έξυπνες κάρτες κλπ). Οι *ADFS* μπορούν να λειτουργήσουν και με την έκδοση *Active Directory Application Mode* (*ADAM*) με την οποία χρησιμοποιούν το πρωτόκολλο *LDAP* για αυθεντικοποίηση.

2.4.5.1 Πρότυπα υλοποίησης Federated Identity Management

Οι *ADFS* εφαρμόζουν *Federated* σενάρια ταυτοτήτων ακολουθώντας την προδιαγραφή *WS-Federation* και ειδικότερα τις προδιαγραφές *WS-Federation Passive Requestor Profile* και *WS-Federation Passive Requestor Interoperability Profile* [115]. Συγκεκριμένα, το *WS-Federation Passive Requestor Profile* καθορίζει τους μηχανισμούς εφαρμογής της προδιαγραφής *WS-Federation* στις περιπτώσεις όπου η εφαρμογή που αποστέλλει τα αιτήματα μπορεί να υλοποιήσει μόνο το HTTP Πρωτόκολλο (πχ απλός Web Browser). Για την καλύτερη κατανόηση των συγκεκριμένων προτύπων πρέπει να αποσαφηνιστούν οι έννοιες που υφίστανται σε όλη την οικογένεια πάνω από το *WS-Security* [4]:

❖ *Claim*: είναι μία δήλωση πληροφορίας ταυτότητας μίας οντότητας (πχ όνομα, ταυτότητα, κλειδί κρυπτογράφησης, ομάδα συμμετοχής της οντότητας, δικαίωμα, δυνατότητα εκτέλεσης υπηρεσίας κλπ)

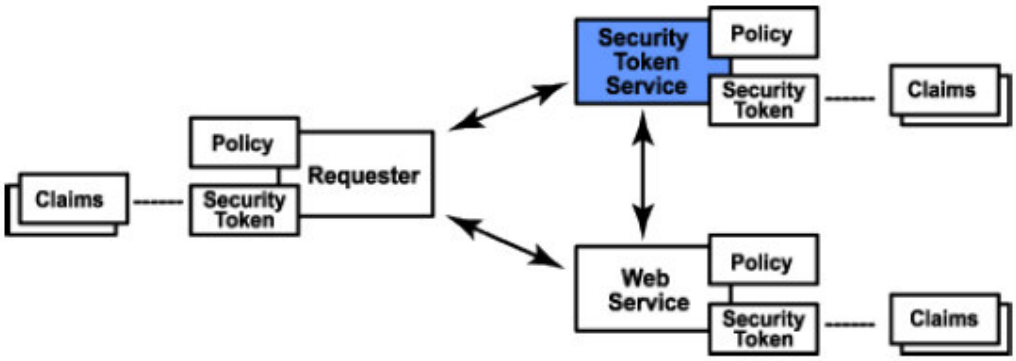
❖ *Security Token*: είναι μία ομαδοποίηση από *claims*.

- *Security Token Service - STS*: είναι μία Web Service η οποία «εκδίδει» *Security Tokens*, δηλαδή βασίζεται σε στοιχεία ταυτοτήτων τα οποία εμπιστεύεται και αποστέλλει τις «βεβαιώσεις ταυτότητας» σε όποιον την εμπιστεύεται. Επιπροσθέτως, υπάρχουν πολλών ειδών *STS* οι οποίες έχουν διαφορετικές λειτουργικότητες. Μία *STS*, για παράδειγμα, μπορεί να επιβεβαιώνει πιστοποιητικά για την είσοδο σε ένα *realm* ή μία άλλη να ελέγχει αν υφίσταται «έμπιστη σχέση» σε παρεχόμενα *Security Tokens*.

- *Identity Provider - IP*: είναι η υπηρεσία παροχής ταυτοτήτων και συνήθως αποτελεί μέρος της *STS* γι αυτό και αναφέρονται μαζί ως *STS/IP*. Μία ελάχιστη λειτουργία της είναι η παροχή υπηρεσιών αυθεντικοποίησης των τελικών χρηστών (*requestors*).

Το βασισμένο στις Web Services μοντέλο ασφαλείας ακολουθεί την εξής γενική φιλοσοφία (βλ. παρακάτω Εικόνα) [45]:

Πηγή: [45]



Εικόνα 36: Γενικό Μοντέλο Εφαρμογής των *Security Tokens*

- Μία Web Service, η οποία αποτελεί τον προσπελάσιμο πόρο μίας επικοινωνίας, μπορεί να απαιτήσει από μία «κλήση» σε αυτή να αποδείξει ένα σύνολο από *Claims* (πχ Όνομα, Κλειδί κρυπτογράφησης κλπ). Στην περίπτωση όπου ένα μήνυμα δεν έχει τα απαιτούμενα *Claims*, τότε απορρίπτεται. Το σύνολο όλων των απαραίτητων *Claims* που απαιτεί μία Web Service καλείται *Policy*.

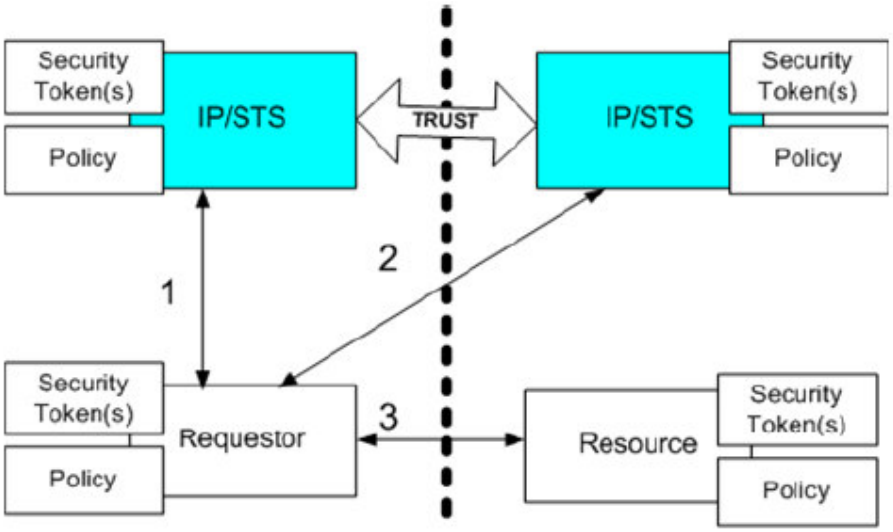
- Η οντότητα που αποστέλλει τα μηνύματα προς την Web Service (*requestor*) μπορεί να αποδείξει την κατοχή των απαιτούμενων *Claims* με την ενσωμάτωση *Security Tokens* μέσα στο μήνυμα. Με αυτό τον τρόπο ένα μήνυμα ζητάει ταυτόχρονα εξυπηρέτηση από μία Web Service και επιδεικνύει τα απαιτούμενα *Claims* σύμφωνα με την *Policy* της *Web Service*.

- Στην περίπτωση όπου ο *requestor* δεν κατέχει τα απαιτούμενα *Claims* τότε μπορεί να επικοινωνήσει ο ίδιος (ή κάποια άλλη οντότητα για λογαριασμό του) με άλλες Web Services οι οποίες επιτελούν το εξειδικευμένο έργο της παραγωγής *Security Tokens* γι αυτό και αποκαλούνται *Security Token Services - STS*. Οι *STS* με τη σειρά τους, ως αυτόνομες Web Services, απαιτούν το δικό τους σύνολο από *Claims* βασισμένο στη δικιά τους *Policy*, ώστε να εξυπηρετήσουν τον *requestor*. Το ίδιο ισχύει και για τον *requestor*, ο οποίος είναι πιθανό να αποτελεί μία Web Service με τη δικιά του *Policy* να καθορίζει το σύνολο των αποδεκτών *Claims*.

Ειδικότερα, για την επίτευξη της *Federated* διαχείρισης της αυθεντικοποίησης, συνδυάζονται οι απαιτήσεις των προδιαγραφών *WS-Security*, *WS-Trust* και *WS-Policy*. Η *WS-Security* καθορίζει το γενικότερο μοντέλο ανταλλαγής δεδομένων ασφαλείας μέσω SOAP μηνυμάτων, η *WS-Trust* καθορίζει τις διαδικασίες με τις οποίες μπορεί μία Web Service ενός συγκεκριμένου *realm* να εγκαθιδρύσει και να ελέγχει την ύπαρξη «έμπιστης» σχέσης με οντότητες ενός άλλου *realm*, ενώ η *WS-Policy* καθορίζει τις διαδικασίες με τις οποίες μπορεί ένας *requestor* να «μάθει» τις απαιτήσεις της *Policy* μίας Web Service. Συνδυάζοντας, επομένως, τις παραπάνω προδιαγραφές η *WS-Federation* καθορίζει τον τρόπο με τον οποίο ένας *requestor* ενός *realm* μπορεί να αυθεντικοποιηθεί για να προσπελάσει πόρους σε ένα άλλο *realm*, εφόσον υπάρχει «έμπιστη» σχέση μεταξύ των *realms*.

Το βασικό μοντέλο λειτουργίας της *WS-Federation* φαίνεται στην παρακάτω Εικόνα, όπου ο *requestor* παραλαμβάνει *Security Tokens* από το *STS* του δικού του *realm* (1) τα οποία χρησιμοποιεί για την αίτηση *Security Tokens* από το *STS* του *realm* στο οποίο ανήκει ο προσπελάσιμος πόρος (2) και στη συνέχεια τα επιδεικνύει στον πόρο προορισμού προκειμένου να ελεγχθεί η ταυτότητά του και να του επιτραπεί η πρόσβαση (3).

Πηγή: [4]



Εικόνα 37: Βασικό Μοντέλο της *WS-Federation*

Η προδιαγραφή *WS-Federation* επεκτείνει το παραπάνω βασικό μοντέλο και προβλέπει πολλές περιπτώσεις «έμπιστης» σχέσης: «άμεση εμπιστοσύνη», «έμμεση εμπιστοσύνη» μέσω ενδιάμεσου *realm*, «μεταβίβαση εμπιστοσύνης» από *realm* σε *realm* κλπ. Επιπροσθέτως, προδιαγράφει και την μεταβίβαση πληροφοριών πέρα από τα στοιχεία ταυτότητας για την εφαρμογή πολιτικών εξουσιοδότησης (*authorization*) στον προσπελάσιμο πόρο, ενώ καλύπτει και τις περιπτώσεις όπου ένας χρήστης πρόκειται να χρησιμοποιήσει ψευδώνυμο σε ένα *realm* συνολικά ή επιλεκτικά σε συγκεκριμένες υπηρεσίες του ίδιου *realm* και απαιτείται η σύνδεση του κάθε ψευδώνυμου με το συγκεκριμένο χρήστη [4].

Η προδιαγραφή *WS-Federation* εξειδικεύεται περισσότερο, ως προς τις λεπτομέρειες υλοποίησής της, ανάλογα με το είδος του *requestor*, σε *Active* και σε *Passive*. Οι *ADFS* υλοποιούν τις προδιαγραφές του *Passive Requestor*, δηλαδή την κατηγορία *requestor* που μπορεί να υ-

λοποιήσει μόνο το HTTP Πρωτόκολλο (πχ απλός Web Browser). Το πρόβλημα σε αυτή την περίπτωση είναι ότι το πρόγραμμα του Browser δεν μπορεί να προσαρμοστεί ώστε να ανταλλάσσει μηνύματα, όπως απαιτούν οι προδιαγραφές, γι αυτό και η ακολουθία των μηνυμάτων πρέπει να υλοποιηθεί με τα εργαλεία που προσφέρει το πρωτόκολλο HTTP 1.1, δηλαδή με τις εντολές *GET*, *POST*, τις ανακατευθύνσεις και τα Cookies, με την επιδίωξη να ακολουθούνται πάντα οι προδιαγραφές αποστολής μηνυμάτων των *WS-Trust* και *WS-Security*. Οι βασικές λειτουργίες που επιτυγχάνονται μέσω της προδιαγραφής *WS-Federation Passive Requestor* είναι [8]:

- *Sign – In*: η αρχική αυθεντικοποίηση και είσοδος του χρήστη σε μία υπηρεσία μέσα στο Internet.

- *Sign-Out*: η έξοδος του χρήστη από μία υπηρεσία με ακόλουθη διαγραφή των πληροφοριών αυθεντικοποίησης οι οποίες πιθανώς να έχουν προκύψει από την προηγούμενη λειτουργία.

- *Attributes*: η διαδικασία αίτησης, επεξεργασίας της αίτησης και αποστολής πρόσθετων πληροφοριών (ιδιοτήτων) για ένα χρήστη στις περιπτώσεις όπου αυτές απαιτούνται για τον περαιτέρω έλεγχο πρόσβασης του χρήστη σε μία υπηρεσία.

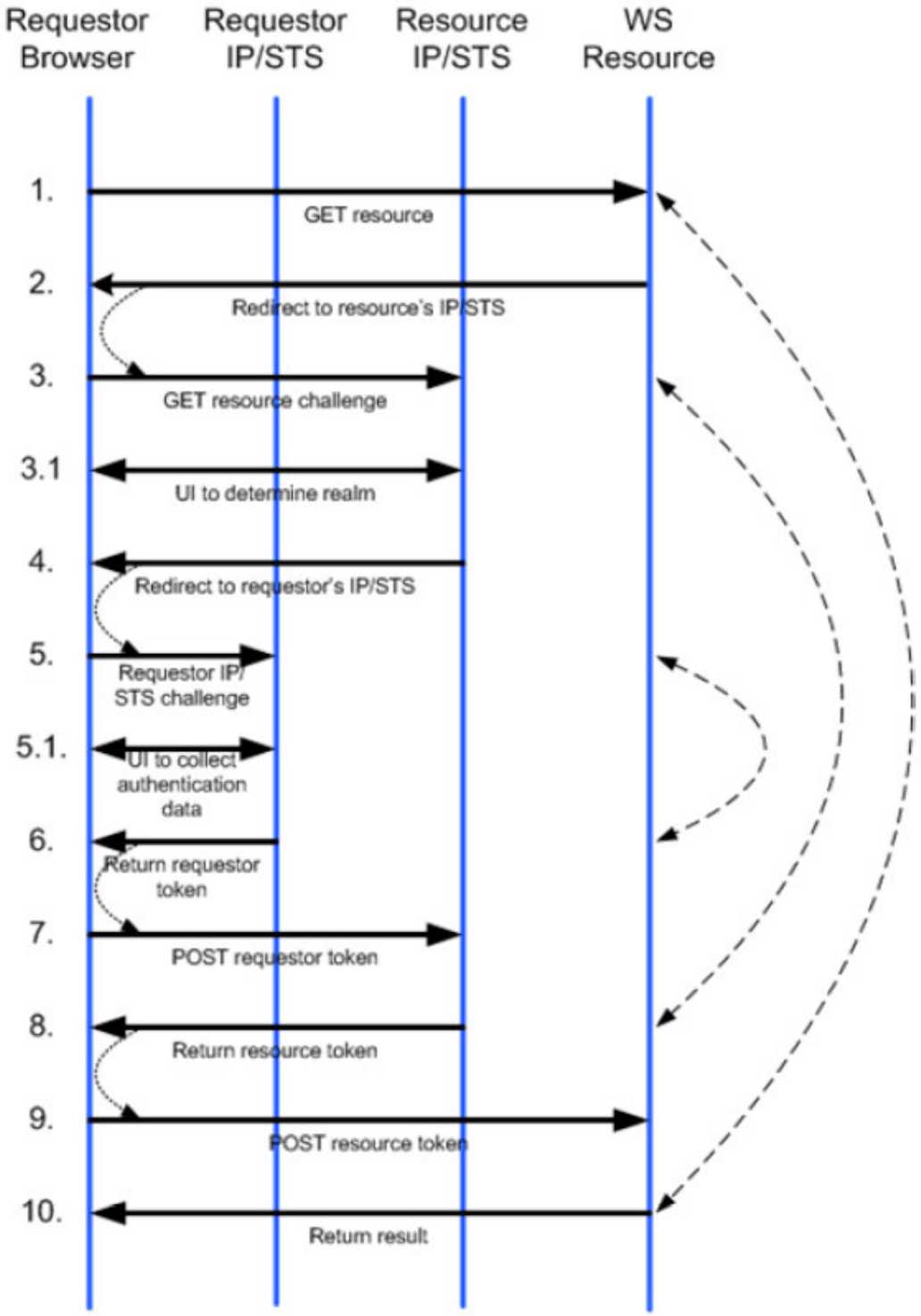
- *Pseudonyms*: η διατήρηση εναλλακτικών, προσωρινών «ονομάτων» για έναν πραγματικό χρήστη ενός *realm*, ώστε οι αναφορές σε αυτόν να γίνονται μέσω του ψευδωνύμου και όχι μέσω πραγματικών στοιχείων του χρήστη.

- *Artifacts/Cookies*: η χρήση των Cookies στο σταθμό του χρήστη για την αποθήκευση πληροφοριών ή καταστάσεων κατά τη διάρκεια της αυθεντικοποίησης, ώστε να υλοποιείται SSO χωρίς να υπάρχουν συνεχή αιτήματα για *Security Tokens*.

Ειδικότερα για τη λειτουργία του *Sign – In*, το βασικό μοντέλο της *WS-Federation* που απεικονίζεται στην παραπάνω Εικόνα εξειδικεύεται σε συγκεκριμένες εντολές του HTTP ως εξής [8]:

- Η προδιαγραφή χρησιμοποιεί τις εντολές *GET* και *POST* του πρωτοκόλλου HTTP 1.1 με τη μορφή:
  - *GET url?parameters*, όπου οι απαιτούμενες παράμετροι προσδιορίζονται στο μετά από τη *url* τμήμα.
  - *POST url?parameters*, όπου οι απαιτούμενες παράμετροι καθορίζονται μέσα στο σώμα της *POST*, ως πεδία μία HTTP φόρμας.

Πηγή: [8]



Εικόνα 38: Βασικό «Σενάριο» Λειτουργίας Εγγραφής Χρήστη με το *WS-Federation Passive Requestor*

❖ Οι παράμετροι που ορίζονται στη συγκεκριμένη προδιαγραφή είναι:

- wa = *string*, καθορίζει την ενέργεια που πρόκειται να εκτελεστεί.
  Αν πρόκειται για εγγραφή του χρήστη, η τιμή είναι: "*wsignin1.0*"
  Αν πρόκειται για έξοδο του χρήστη, η τιμή είναι: "*wsignout1.0*"
  Αν πρόκειται για μετάδοση χαρακτηριστικών, η τιμή είναι: "*wattr1.0*"
  Αν πρόκειται για μετάδοση ψευδονύμων, η τιμή είναι: "*wpseudo1.0*"
- wreply=*URL*, προαιρετική παράμετρος που ορίζει την διεύθυνση που θα κατευθυνθούν οι απαντήσεις.
- wres=*URL*, προαιρετική παράμετρος που ορίζει την διεύθυνση του προσπελάσιμου πόρου.
- wctx=*string*, προαιρετική παράμετρος που, όταν ενσωματωθεί σε μία εντολή αίτησης, πρέπει να επιστραφεί αυτούσια μαζί με το επιστρεφόμενο *token*.
- wp=*URI*, προαιρετική παράμετρος που καθορίζει την *Policy* με τον τρόπο που προδιαγράφεται στις *WS-Policy* και *WS-Trust*.
- wct=*timestring*, προαιρετική παράμετρος που περιέχει την τρέχουσα ώρα για να ελέγξει έπειτα ο παραλήπτης την «ηλικία» του μηνύματος.
- wtrealm=*string*, προαιρετική παράμετρος που καθορίζει τη διεύθυνση του αιτούντος *realm*.
- wreq=*xml*, προαιρετική παράμετρος που περιέχει ως κείμενο το xml μήνυμα μίας αίτησης *Security Token* είτε με βάση το συντακτικό του στοιχείου *<wsse:RequestSecurityToken>* της *WS-Security* είτε με βάση το συντακτικό της *WS-Trust*. Αν η συγκεκριμένη παράμετρος παραληφθεί τότε υποτίθεται ότι η υπηρεσία που πρόκειται να απαντήσει γνωρίζει τον τύπο του απαιτούμενου *Token*.
- wreqptr=*URL*, προαιρετική παράμετρος που καθορίζει τη διεύθυνση όπου μπορεί να βρεθεί η αίτηση του wreq.
- wresult=*xml*, υποχρεωτική παράμετρος που προσδιορίζει το αποτέλεσμα της έκδοσης ενός *Token*. Αυτό μπορεί να έχει είτε τη μορφή του στοιχείου *<wsse:RequestSecurityTokenResponse>* του *WS-Security* είτε τη μορφή ενός SOAP μηνύματος *<S:Envelope>* σύμφωνα με την *WS-Trust* ή ενός SOAP μηνύματος λάθους *<S:Fault>*.
- wresultptr=*url*, παράμετρος που καθορίζει τη διεύθυνση προς την οποία θα σταλεί η εντολή HTTP GET για την παραλαβή του *Token*. Το αποτέλεσμα θα είναι ένα κείμενο τύπου text/xml, η τιμή δηλαδή της wresult.
- wattr=*xml-attribute-request*, απαιτούμενη παράμετρος στις περιπτώσεις μετάδοσης *attributes*. Το ακριβές συντακτικό της παραμέτρου εξαρτάται από τις λεπτομέρειες της καθεμιάς εφαρμογής και δεν περιλαμβάνεται στην τρέχουσα προδιαγραφή.
- wpseudo=*xml-pseudonym-request*, απαιτούμενη παράμετρος στις περιπτώσεις αίτησης ψευδωνύμου και μπορεί να αποτελείται είτε από μία εντολή της μορφής *<wsse:GetPseudonym>* της *WS-Security* είτε από ένα SOAP μήνυμα *<S:Envelope>*.

❖ Για χάριν του παραδείγματος υποθέτουμε ένα σενάριο αιτήματος πρόσβασης ενός account σε έναν πόρο (*resource*) όπου ισχύουν:

- *Resource Realm* = *"Resource.com"*
- *Resource* = *"https://res.resource.com/sales"*
- *Resource's IP/STS* = *"https://sts.resource.com/sts"*
- *Account* = *"Account.com"*
- *Account's IP/STS* = *"https://sts.account.com/sts"*

❖ Σε όλα τα παρακάτω μηνύματα είναι υποχρέωση της καθεμιάς υλοποίησης να εξασφαλίσει την ασφάλεια και ακεραιότητα των περιεχομένων τους. Στο πρωτόκολλο HTTP αυτό υλοποιείται μέσω της εγκατάστασης «ασφαλούς καναλιού» με τη χρήση του πρωτοκόλλου HTTPS.

❖ <u>*Βήμα 1*</u> - Ο Browser του *requestor* επιχειρεί πρόσβαση στο ζητούμενο *resource*:

GET https://res.resource.com/sales HTTP/1.1

❖ <u>*Βήμα 2*</u> – Το ζητούμενο *resource* ανακατευθύνει τον Browser στο *IP/STS* του *realm* που αυτό ανήκει. Αυτό γίνεται συνήθως μέσω του κωδικού λάθους 302 του πρωτοκόλλου HTTP:

HTTP/1.1 302 Found ↵

*Location: https://sts.resource.com/sts?*wa=*wsignin1.0*&wreply=*https://res.resource.com/sales*&wct=*2003-03-03T19:06:21Z*

❖ <u>*Βήμα 3*</u> –Το *IP/STS* του *resource realm* μόλις λάβει την παραπάνω κλήση πρέπει να αποφασίσει το *realm* που ανήκει ο *requestor*. Αυτή η πληροφορία μπορεί να υπάρχει σε κάποιο Cookie στην πλευρά του Browser από κάποια προηγούμενη επικοινωνία, μπορεί να είναι μία σταθερή πληροφορία που κατέχει ο *IP/STS* του *resource realm* από την εγκατάσταση της «σχέσης εμπιστοσύνης» με άλλα *realms* ή διαφορετικά θα πρέπει να ερωτηθεί ο χρήστης μέσω του Browser (Βήμα 3.1).

*GET https://sts.resource.com/sts?*wa=*wsignin1.0*&wreply=*https://res.resource.com/sales*&wct=*2003-03-03T19:06:21Z HTTP/1.1*

❖ <u>*Βήμα 4*</u> – Το *resource IP/STS* ανακατευθύνει τον Browser στο *IP/STS* του *requestor*, συνήθως μέσω του κωδικού HTTP 302, προκειμένου να γίνει η αυθεντικοποίηση του *requestor*. Ανάλογα με το είδος της «συμφωνίας» που έχει εγκαθιδρυθεί μεταξύ των *IP/STS* των δύο *realms* είναι πιθανό να αποσταλούν επιπλέον πληροφορίες με την εντολή *POST*.

HTTP/1.1 302 Found ↵

*Location: https://sts.account.com/sts?*wa=*wsignin1.0*&wreply=*https://sts.resource.com/sts*&wctx=*https://res.resource.com/sales*&wct=*2003-03-03T19:06:22Z*&wtrealm=*resource.com*

- *Βήμα 5* – Το *IP/STS* του *requestor* αυθεντικοποιεί τον *requestor*, διαδικασία η οποία προαιρετικά μπορεί να απαιτήσει την προβολή στον Browser του χρήστη κατάλληλου User Interface για την υποβολή απαραίτητων στοιχείων ταυτότητας (Βήμα 5.1):

  GET
  *https://sts.account.com/sts?*wa=*wsignin1.0*&wreply=*https://sts.resource.com/sts*&wctx=*https://res.resource.com/sales*&wct=*2003-03-03T19:06:22Z*&wtrealm=*resource.com HTTP/1.1*

- *Βήμα 6* – Όταν τα στοιχεία του *requestor* έχουν αυθεντικοποιηθεί επιτυχώς, παράγεται μία απάντηση *Security Token* (*Security Token Response – RSTR*) και αποστέλλεται στο *resource IP/STS*, όπου και συνεχίζει η επεξεργασία μέσω ανακατεύθυνσης. Η συγκεκριμένη αποστολή προτείνεται να γίνεται μέσω της εντολής POST όπου το *Security Token* είναι η τιμή ενός αντικειμένου σε μία HTTP φόρμα:

```
HTTP/1.1 200 OK

...

<html xmlns="https://www.w3.org/1999/xhtml">
<head>
<title>Working...</title>
</head>
<body>
<form method="post" action="https://sts.resource.com/sts">
<p>
<input type="hidden" name="wa" value="wsignin1.0" />
<input type="hidden" name="wctx" value=https://res.resource.com/sales />
<input type="hidden" name="wresult" value="&lt; RequestSecurityTokenRe-
sponse&gt;...&lt;/RequestSecurityTokenResponse&gt;" />
<button type="submit">POST</button> <!-- included for requestors that do not
support javascript -->
</p>
</form>
<script type="text/javascript">
setTimeout('document.forms[0].submit()', 0);
</script>
</body>
</html>
```

- *Βήμα 7* – Το *resource IP/STS* αποδέχεται και επικυρώνει το *RSTR*:

```
POST https://sts.resource.com/sts HTTP/1.1 ↵
... ↵
↵
wa=wsignin1.0 ↵
wctx=https://res.resource.com/sales
wresult=<RequestSecurityTokenResponse>...</RequestSecurityTokenResponse>
```

- *Βήμα 8* - Το *resource IP/STS* εκτελεί έλεγχο σύμφωνα με την *Policy* του για *Federated* authentication/authorization. Σε περίπτωση επιτυχών ελέγχων δημιουργείται το κατάλλη-

λο *Security Token* για το συγκεκριμένο *resource* και ανακατευθύνεται ο έλεγχος στο *resource*. Προαιρετικά σε αυτή τη φάση το *resource IP/STS* μπορεί να αποστείλει στον Browser ένα Cookie με τα στοιχεία εγγραφής του χρήστη για μελλοντική πρόσβαση του χρήστη σε άλλη υπηρεσία του *resource realm* (*Federated SSO*).

```
HTTP/1.1 200 OK
...
<html xmlns="https://www.w3.org/1999/xhtml">
<head>
<title>Working...</title>
</head>
<body>
<form method="post" action="https://res.resource.com/sales">
<p>
<input type="hidden" name="wa" value="wsignin1.0" />
<input type="hidden" name="wresult"value="&
lt;RequestSecurityTokenResponse&gt;...&lt;/RequestSecurityTokenResponse&gt;"
/>
<button type="submit">POST</button> <!-- included for requestors that do not
support javascript -->
</p>
</form>
<script type="text/javascript">
setTimeout('document.forms[0].submit()', 0);
</script>
</body>
</html>
```

- *Βήμα 9* – Το *resource* δέχεται το *RSTR* από το *resource IP/STS* και εφόσον συμφωνεί με τις απαιτήσεις της *Policy* του, εξυπηρετείται ο *requestor*.

```
POST https://res.resource.com/sales HTTP/1.1 ↵
... ↵
↵
wa=wsignin1.0 ↵
wresult=<RequestSecurityTokenResponse>...</RequestSecurity TokenResponse>
```

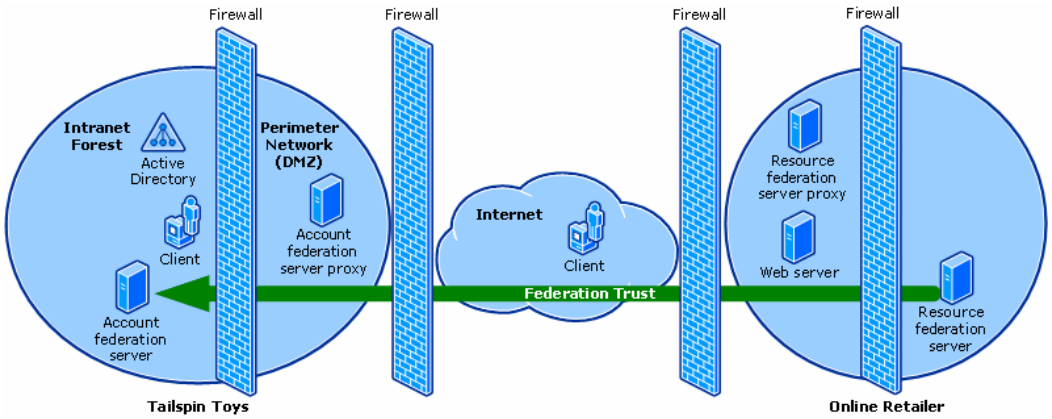
- *Βήμα 10* – Το *resource* είναι πιθανό να επιστρέψει και ένα Cookie με πληροφορίες εγγραφής του χρήστη μαζί με την απάντηση προς τον *requestor*.

2.4.5.2 Federation στις ADFS

Οι *ADFS* υλοποιώντας τις προδιαγραφές του *WS-Federation Passive Requestor Profile* σε συνδυασμό με τις δυνατότητες των server λειτουργικών συστημάτων των Windows καθιστούν δυνατή τη διαμοίραση πληροφοριών ταυτοτήτων χρηστών μεταξύ διαφορετικών, «έμπιστων» οργανισμών (*Federations*). Τα ακριβή σενάρια και τοπολογίες *Federations* που μπορούν να εξυπηρετηθούν από τις ADFS είναι [115]:

- *Federated Web SSO*: περιλαμβάνει την ανάπτυξη ασφαλούς επικοινωνίας μεταξύ δύο οργανισμών η οποία διέρχεται από τα Firewalls και τις «Προστατευόμενες Ζώνες» που διαθέτει ο καθένας για την πρόσβαση και προστασία στο Internet. Στην πράξη (βλ. παρακάτω Εικόνα), η συγκεκριμένη εγκατάσταση δίνει τη δυνατότητα σε χρήστες των οποίων οι λογαριασμοί βρίσκονται σε ένα οργανισμό (*Tailspin Toys*) να προσπελαύνουν μέσα από το Internet δικτυακές υπηρεσίες σε ένα άλλο οργανισμό (*Online Retailer*). Οι δύο οργανισμοί έχουν εγκαθιδρύσει σχέση εμπιστοσύνης (ο *Online Retailer* «εμπιστεύεται» τον *Tailspin Toys*) κατά την εγκατάσταση των *ADFS* και έχουν ρυθμίσει από κοινού τις απαραίτητες παραμέτρους. Η σχέση εμπιστοσύνης (*Federation Trust*) στις *ADFS* «κατευθύνεται» πάντα από τον οργανισμό που κατέχει τους δικτυακούς πόρους (*Resource Partner*) προς τον οργανισμό που κατέχει τους λογαριασμούς και τα δεδομένα ταυτοτήτων των χρηστών είτε στο *Active Directory* είτε σε μία εγκατάσταση του *ADAM* (*Account Partner*). Συγκεκριμένα, ο *Resource Partner* ανακατευθύνει τις αιτήσεις πρόσβασης χρηστών στον *Account Partner* και αποδέχεται τα *Claims* που του επιστρέφει με τη μορφή *Security Tokens*. Με τα συγκεκριμένα *Claims* μπορεί να εξάγει και χρησιμοποιήσει και πληροφορίες εξουσιοδότησης. Ο ρόλος του *Account Partner* είναι να εξετάζει τα «δικαιολογητικά» των χρηστών και να τους αυθεντικοποιεί δημιουργώντας τα απαραίτητα *Security Tokens*. Η «ροή», επομένως, της αυθεντικοποίησης έχει αντίθετη κατεύθυνση από αυτή της *Federation Trust*. Στη συγκεκριμένη τοπολογία παρεμβάλλονται προαιρετικά *Federation Server Proxies* (*Account* και *Resource*) στα περιμετρικά δίκτυα (***D**e**M**ilitarized **Z**ones - DMZ*) και των δύο οργανισμών, ώστε οι *Proxies* να ελέγχουν και προστατεύουν την πρόσβαση στους *Federation Servers* (*Account* και *Resource*), οι οποίοι δεν είναι άμεσα προσβάσιμοι από το Internet.

Πηγή: [115]

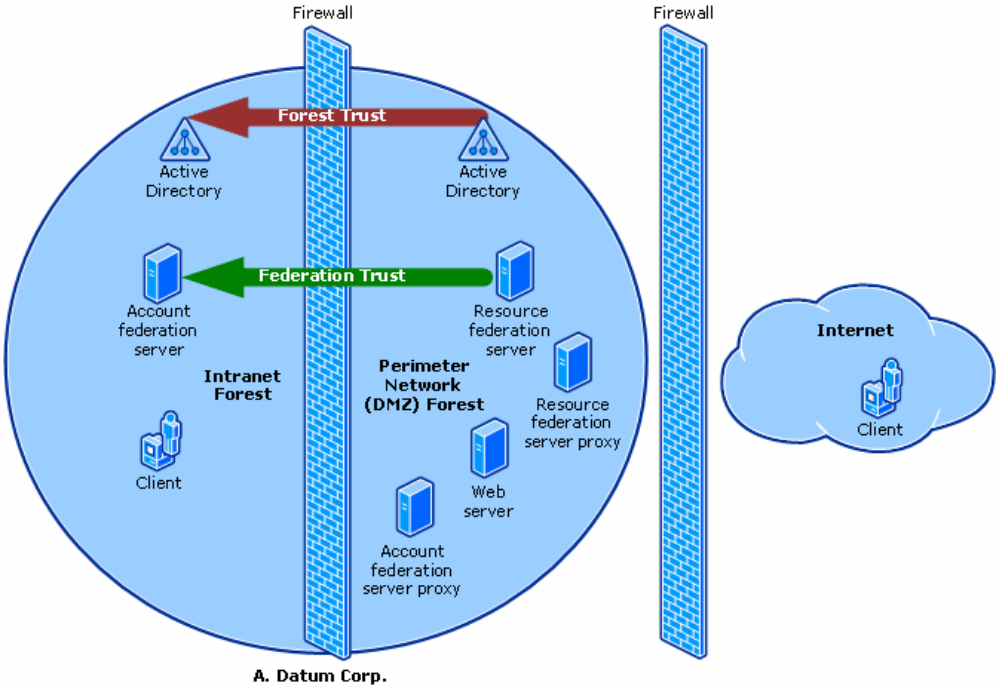


Εικόνα 39: Παράδειγμα Υλοποίησης *Federated Web SSO* στις *ADFS*

- *Federated Web SSO with Forest Trust*: περιλαμβάνει την ανάπτυξη δύο *Forests* του *Active Directory* στα πλαίσια του ίδιου οργανισμού (βλ. σχετική Εικόνα). Το ένα βρίσκεται στο δίκτυο DMZ του οργανισμού και περιέχει όλους τους εξωτερικούς χρήστες του (πχ πελάτες) των δικτυακών εφαρμογών του οργανισμού, ενώ το δεύτερο βρίσκεται στο εσωτερικό – προστατευμένο δίκτυο του οργανισμού και περιέχει όλα τα προσωπικά στοιχεία των εσωτερικών χρηστών (πχ υπαλλήλων). Στη συγκεκριμένη περίπτωση πρέπει να εγκαθιδρυθούν δύο ειδών *Trusts*, μία μεταξύ των *Active Directories*, ώστε το εξωτερικό *Forest* να «εμπιστεύεται» τα στοιχεία του εσωτερικού (*Forest Trust*) και μία μεταξύ των δύο *Federation Servers* (*Account* και *Resource*) έτσι ώστε οι εσωτερικοί χρήστες να αυθεντι-

κοποιούνται ως χρήστες των δικτυακών εφαρμογών, από όπου και αν τις προσπελαύνουν, χωρίς να διατηρούνται τα στοιχεία των λογαριασμών τους στο περιμετρικό και εν δυνάμει ευάλωτο δίκτυο του οργανισμού.

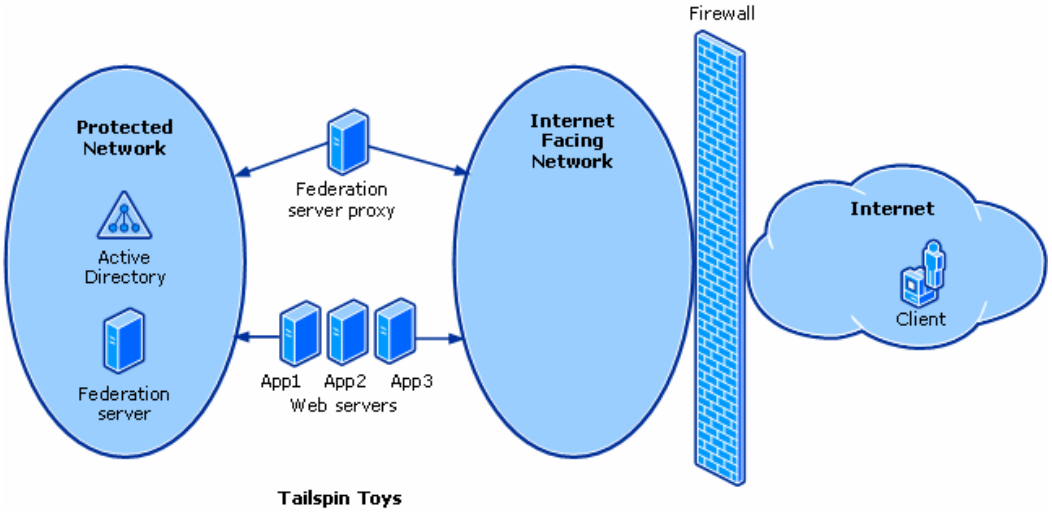
Πηγή:[115]



Εικόνα 40: Παράδειγμα Υλοποίησης *Federated Web SSO with Forest Trust* στις *ADFS*

- *Web SSO*: περιλαμβάνει την γενική ιδέα του Web SSO, δηλαδή τη μοναδική αυθετικοποίηση των εξωτερικών χρηστών των Web-based εφαρμογών ενός οργανισμού (βλ. σχετική Εικόνα). Σε αυτή την περίπτωση όλοι οι χρήστες προέρχονται από το Internet οπότε δεν υφίσταται η έννοια του *Federation Trust* μεταξύ διαφορετικών οργανισμών. Οι Web Servers των εφαρμογών του οργανισμού πρέπει να προσπελαύνουν τον server που περιέχει το *Active Directory* αλλά και να είναι προσβάσιμοι και από το Internet. Γι αυτό το λόγο είναι συνδεδεμένοι σε δύο δίκτυα μέσα στον οργανισμό, οπότε και ονομάζονται "*multihomed*": το πρώτο δίκτυο είναι το προστατευόμενο, εσωτερικό δίκτυο του *Active Directory Forest* και το δεύτερο δίκτυο είναι το περιμετρικό το οποίο προσπελαύνεται από το Internet. Το ίδιο ισχύει και για τον *Federation Server Proxy* ο οποίος προσφέρει την απαραίτητη σύνδεση μεταξύ του *Federation Server* και το Internet. Για λόγους ασφαλείας ο *Federation Server* πρέπει να είναι εγκατεστημένος σε προστατευόμενο δίκτυο το οποίο δεν είναι «ορατό» απευθείας από το Internet.

Πηγή: [115]



Εικόνα 41: Παράδειγμα Υλοποίησης Web SSO στις *ADFS*

2.4.5.3 Οι Υπηρεσίες που Αποτελούν τις ADFS

Οι *ADFS*, όπως καταδεικνύει και το όνομά τους, εξυπηρετούν τα παραπάνω σενάρια με μία σειρά από Services που τις αποτελούν [115]:

- *Federation Service*: υλοποιεί το ρόλο της υπηρεσίας *Security Token Service – STS* της προδιαγραφής *WS-Federation*, λειτουργεί ως δημιουργός και αποδέκτης των *Security Tokens* σύμφωνα με τις διαδικασίες της προδιαγραφής *WS-Federation Passive Requestor Profile* και καθιστά τον server στον οποίο εγκαθίσταται έναν *Federation Server*. Στην περίπτωση που εγκαθίσταται στον *Account Partner* εξασφαλίζει την πρόσβαση των χρηστών του *Active Directory* του οργανισμού σε Web Applications άλλων «έμπιστων» οργανισμούς ως εξής: μόλις δεχθούν από τον *Resource Partner* αίτημα αυθεντικοποίησης ενός χρήστη, συγκεντρώνουν τα στοιχεία του χρήστη και τα επικυρώνουν σε επικοινωνία με το *Active Directory* (ή την έκδοση *ADAM*). Η ανάγνωση των στοιχείων του χρήστη γίνεται με την εμφάνιση σε αυτόν μίας σελίδας Web όπου αυτός καλείται να εισάγει το username και password του, στην απλούστερη μορφή της form-based αυθεντικοποίησης, ενώ υπάρχει και η επιλογή για προβολή φόρμας για αυθεντικοποίηση κατά *Integrated Windows Authentication*. Τα στοιχεία που διατηρεί για το χρήστη το *Active Directory* αντιστοιχίζονται σε αυτά που απαιτεί η *Policy* του *Resource Partner* και όλα μαζί συνιστούν ένα *Security Token* το οποίο αποστέλλεται πίσω στον *Resource Partner*. Το επιστρεφόμενο *Security Token* «υπογράφεται» από τη *Federation Service* με το πιστοποιητικό υπογραφής των *Security Tokens* το οποίο είναι και στοιχείο ελέγχου της εγκυρότητας του *Account Partner*.

  Στην περίπτωση που η *Federation Service* εγκαθίσταται στον *Resource Partner*, εκτελεί τις αντίστροφες διαδικασίες: μόλις επιχειρείται πρόσβαση ενός χρήστη σε μία Web Application η οποία προστατεύεται από τις *ADFS*, η *Federation Service* προσδιορίζει ποιος *Account Partner* πρέπει να αυθεντικοποιήσει το χρήστη και του αποστέλλει το σχετικό αίτημα. Ο προσδιορισμός του αρμόδιου *Account Partner* γίνεται συνήθως με την εμφάνιση

στο χρήστη ανάλογης Web σελίδας όπου ο χρήστης καλείται να επιλέξει έναν *Account Partner* ανάμεσα σε αυτούς που έχουν εγκαθιδρύσει «έμπιστη» σχέση με τον *Resource Partner*. Στη συνέχεια η *Federation Service* πρέπει να παραλάβει κατάλληλο *Security Token* για τον χρήστη, το οποίο εξετάζει πρωτίστως σε σχέση με την εγκυρότητα της «υπογραφής» του «έμπιστου» οργανισμού από τον οποίο εκδόθηκε. Μέσα από το *Security Token* εξάγονται τα απαραίτητα *Claims*, τα οποία αντιστοιχίζονται σε αυτά που απαιτεί η *Policy* της Web Application. Το παραγόμενο σύνολο από *Claims* μορφοποιείται σε ένα νέο *Security Token*, το οποίο προωθείται από την *Federation Service* στη Web Application είτε «υπογεγραμμένο» από ψηφιακό πιστοποιητικό είτε κωδικοποιημένο με αμοιβαία γνωστό session key σύμφωνα με το πρωτόκολλο *Kerberos*.

Η *Federation Service* είναι σε θέση να δημιουργήσει ένα Cookie προς τον Browser του χρήστη με κατάλληλες πληροφορίες του χρήστη, ανεξάρτητα αν λειτουργεί από την πλευρά του *Account Partner* ή του *Resource Partner*. Με αυτή τη μέθοδο επιτυγχάνεται το Single Sign-On, καθώς καθίστανται γρήγορα γνωστά τα στοιχεία του χρήστη και η προηγούμενη αυθεντικοποίησή του, ώστε σε επόμενες προσπάθειες πρόσβασης του χρήστη να μην ακολουθηθεί ξανά όλη η παραπάνω διαδικασία. Τα Cookies μπορεί να είναι τριών ειδών: "*authentication cookies*", "*account partner cookies*" και "*sign-out cookies*" τα οποία αποθηκεύονται κατά τη διάρκεια της εξόδου του χρήστη από την Web Application.

- *Federation Service Proxy*: αποτελεί μία προαιρετική, διαμεσολαβητική (proxy) υπηρεσία μεταξύ του *Federation Server* και του Internet και καθιστά τον server στον οποίο εγκαθίσταται *Federation Service Proxy Server*. Επικοινωνεί με την *Federation Service* σύμφωνα με την προδιαγραφή *WS-Federation Passive Request Profile* παίρνοντας το ρόλο του client. Εγκαθίσταται στην DMZ ενός οργανισμού, για να μην υπάρχει απευθείας πρόσβαση του *Federation Server* στο Internet και κατά συνέπεια συνδέεται άμεσα και προστατεύει κάθε φορά ένα συγκεκριμένο είδος *Federation Server*, *Account* ή *Resource*. Στην περίπτωση του *Account Partner* ο *Federation Service Proxy* συγκεντρώνει από τον Browser του χρήστη τα στοιχεία ταυτότητάς του, ενώ στην περίπτωση του *Resource Partner* προωθεί τα αιτήματα και τις απαντήσεις από και προς την *Federation Service* και την Web Application.

- *ADFS Web Agent*: αποτελεί την υπηρεσία που ελέγχει τα *Security Tokens* ή τα security Cookies που δέχεται ο Web Server ώστε να επιτρέψει ή απαγορεύσει πρόσβαση στην Web Application. Απαιτεί τη σύνδεση με μία *Resource Federation Service* ώστε να προωθεί τις κλήσεις των χρηστών προς την Web Application προκειμένου να αναζητήσει τα απαιτούμενα *Security Tokens* των χρηστών. Οι Web Applications μπορεί να είναι υλοποιημένες έτσι ώστε είτε να κατανοούν τη δομή των *Security Tokens* των *ADFS*, οπότε να μπορούν να διαβάσουν από αυτά πληροφορίες εξουσιοδότησης (*Claims-aware Applications*), είτε να κατανοούν μόνο τη δομή των *Windows NT Tokens* οπότε ο *Web Agent* θα εκτελέσει τη συγκεκριμένη μετατροπή για την ανάγνωση από τις εφαρμογές πληροφοριών εξουσιοδότησης στα *Tokens* (*Windows NT token-based Applications*).

2.4.5.4 Ρόλοι των Servers στις ADFS

Προκειμένου να λειτουργήσουν οι *ADFS* μέσα σε ένα περιβάλλον λειτουργικού συστήματος Windows Server 2003 R2, σύμφωνα και με την προηγούμενη περιγραφή των συστατικών των ADFS, πρέπει να υπάρχουν μέσα στο δίκτυο servers με συγκεκριμένους ρόλους [115]:

- *Federation Server*: φιλοξενεί την υπηρεσία *Federation Service* των *ADFS* και λειτουργεί κυρίως ως ο παραλήπτης και εξυπηρετητής κλήσεων για αυθεντικοποίηση είτε από χρήστες «έμπιστων» οργανισμών (στις τοπολογίες *Federated Web SSO*) είτε από χρήστες του Internet (στην απλή τοπολογία *Web SSO*). Σύμφωνα και με τις προδιαγραφές των *Federation Services* οι ακριβείς λειτουργίες του *Federation Server* διαφέρουν ανάλογα με το αν ο οργανισμός στον οποίο εγκαθίσταται είναι ο *Account Partner* ή ο *Resource Partner* της ευρύτερης *Federation* τοπολογίας.

- *Federation Server Proxy*: φιλοξενεί την υπηρεσία *Federation Service Proxy* των *ADFS* και ενσωματώνεται στο περιμετρικό προς το Internet δίκτυο του οργανισμού (DMZ), ώστε να προωθεί τα αιτήματα προς τους *Federation Servers*, οι οποίοι δεν είναι άμεσα προσβάσιμοι από το Internet. Σύμφωνα και με τις προδιαγραφές της υπηρεσίας *Federation Service Proxy* η λειτουργία του διαφέρει ανάλογα με το αν ο οργανισμός στον οποίο εγκαθίσταται είναι ο *Account Partner* ή ο *Resource Partner* της ευρύτερης *Federation* τοπολογίας.

- *Web Server*: φιλοξενεί την υπηρεσία *Web Agent* των *ADFS* με την οποία εξασφαλίζεται η ασφαλή πρόσβαση στην Web Application που επίσης φιλοξενείται στον *Web Server*.

2.4.6. Λύσεις *Web SSO* & *Federated Identity Management* που βασίζονται στη *SAML*

Η εξέλιξη και «ωρίμανση» της γλώσσας *SAML* από τον οργανισμό OASIS, αλλά και οι εμπορικές και ακαδημαϊκές ανάγκες διαμοίρασης της πρόσβασης των δικτυακών εφαρμογών εκτός των ορίων ενός οργανισμού με αυστηρό, όμως, έλεγχο πρόσβασης οδήγησε στη διατύπωση πολλών λύσεων SSO και *Federated Identity Management* βασισμένων στη *SAML* από οργανισμούς, επιτροπές Πανεπιστημίων και εταιριών. Δύο από τις σημαντικότερες προσπάθειες είναι οι:

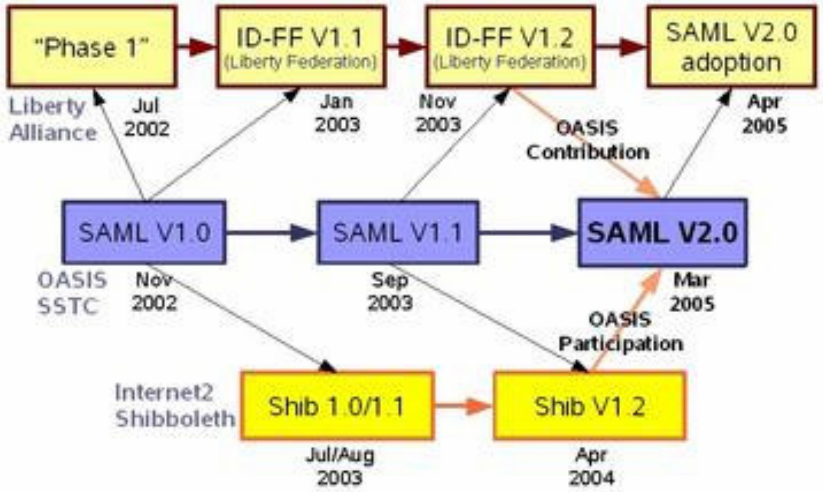
- *ID-FF* (*Identity Federation Framework*) του Οργανισμού *Liberty Alliance Project*, ο οποίος αποτελεί μία σύμπραξη μεγάλων εταιριών Information Technology (America-On-Line, Ericsson, France Telecom, IBM, Intel, Oracle, Sun κλπ), μεγάλων εμπορικών εταιριών (General Motors, Fidelity Investments κλπ) και επιστημονικών – δημοσίων φορέων [73].

- *Shibboleth* της επιτροπής M*iddleware Architecture Committee for Education – MACE* του οργανισμού *Internet2*, ο οποίος είναι μία ανοιχτή συνεργασία ερευνητικών και ακαδημαϊκών ιδρυμάτων ή άλλων μη-κερδοσκοπικών οργανισμών με κύριο σκοπό την επέκταση των δικτύων τους και την εκμετάλλευση των πόρων και συνεργασιών του κάθε Ιδρύματος από όλα τα υπόλοιπα, αλλά επίσης η ανάπτυξη και εφαρμογή νέων τεχνολογιών και με-

θόδων μέσα στο Internet. Μέλη – χορηγοί μπορεί να είναι και εμπορικές εταιρίες για τη συνεισφορά της τεχνογνωσίας τους, όπως για παράδειγμα η προδιαγραφή *Shibboleth* εξελίσσεται με την υποστήριξη της IBM [52, 54].

Οι δύο παραπάνω προδιαγραφές εξειδικεύουν τους γενικούς κανόνες της *SAML* σε συγκεκριμένες χρήσεις και πρακτικές (εμπορικές, ακαδημαϊκές, Δημοσίων Φορέων κλπ). Συγκεκριμένα, οι παραπάνω προδιαγραφές βασίζονται ή μεταβάλλουν τα *Protocols* της *SAML*, χρησιμοποιώντας *Assertions* της *SAML*, έτσι ώστε να επανα-διατυπώσουν τα *Bindings* και *Profiles* της *SAML* με βάση τα νέα πρωτόκολλα. Μία χαρακτηριστική εικόνα της παράλληλης εξέλιξης των τριών προτύπων φαίνεται παρακάτω:

Πηγή: [73]



Εικόνα 42: Εξέλιξη των Λύσεων *Federated Identity Management* σε σχέση με τη SAML

Η παράλληλη πορεία των δύο προδιαγραφών και της *SAML* οδήγησε στη συγχώνευση των προτάσεων βελτιώσεων και εξελίξεων καθεμιάς προδιαγραφής και στη διατύπωση της τρέχουσας έκδοσης *SAML* v2.0.

2.4.6.1 To Project "Liberty Alliance - Identity Federation Framework"

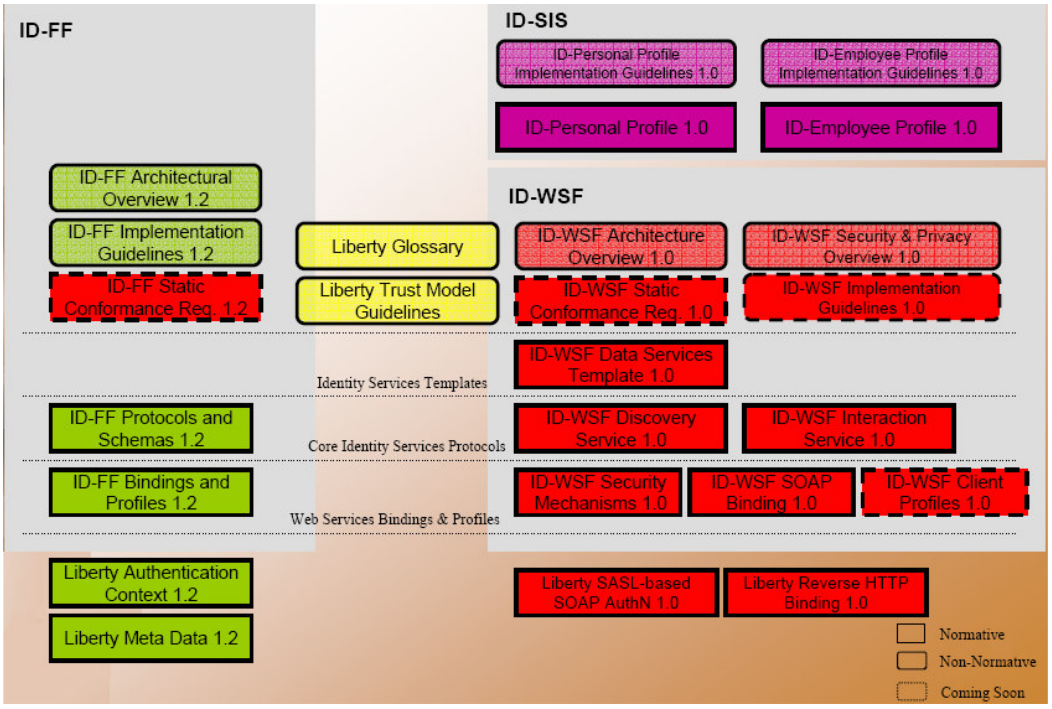
Η σύμπραξη εταιριών *Liberty Alliance Project* επικεντρώνεται στην πρόταση λύσεων σε θέματα σχετικά με τη Διαχείριση Ταυτοτήτων στο Internet μέσα από τις θεσμοθετημένες Ομάδες Ειδικών της με εξειδίκευση της καθεμιάς σε συγκεκριμένους τομείς. Η εργασία του καθένα τομέα καταλήγει στη διατύπωση προδιαγραφών οι οποίες όλες μαζί αποτελούν το γενικό πλαίσιο – πρόταση αντιμετώπισης θεμάτων Διαχείρισης Ταυτοτήτων στο Internet. Οι προδιαγραφές του *Liberty – Alliance Project* φαίνονται στην παρακάτω εικόνα και περιλαμβάνουν τις:

- *Liberty Identity Web Services Framework (ID-WSF)*: περιγράφει το πλαίσιο για Web Services βασισμένες σε πληροφορίες ταυτότητας χρηστών με τις οποίες μπορούν να ανταλλαγούν με ελεγχόμενο τρόπο πληροφορίες ταυτότητας χρηστών.

- *Liberty Identity Services Interface Specifications (ID-SIS)*: καθορίζει ένα σύνολο προδιαγραφών για την ανάπτυξη δια-λειτουργικών Web Services υψηλότερου επιπέδου που θα βασίζονται όμως στην προδιαγραφή *ID-WSF*. Τέτοιες Web Services μπορεί να είναι γενικές υπηρεσίες βασισμένες σε ένα πρόσωπο πχ ένα ημερολόγιο, μία ατζέντα, μία υπηρεσία υπενθυμίσεων κλπ.

Στα θέματα *Federated Identity Management* δόθηκε υψηλή προτεραιότητα καθώς θεωρήθηκε ότι μπορούν να οδηγήσουν σε συνεργασίες εταιριών για την προώθηση του e-Commerce, της ασφάλειας των οικονομικών συναλλαγών στο Internet και την επέκταση των Επιχειρηματικών Μοντέλων στο Internet μέσω των νέων ευκαιριών εταιρικών συμπράξεων που μπορούν να οικοδομηθούν με το *Federation* των ταυτοτήτων. Αποτέλεσμα των ερευνών της επιτροπής ήταν η προδιαγραφή *Identity Federation Framework (ID-FF)*. Η *ID-FF* ξεκίνησε με την έκδοση "*Phase 1*", έφτασε στην έκδοση *V1.2* και ενσωματώθηκε στην έκδοση *SAML V2.0* η οποία είναι αυτή που επίσημα υποστηρίζεται πια από το *Liberty Alliance Project* [73].

Πηγή: [73]



Εικόνα 43: Οι Προδιαγραφές του *Liberty – Alliance Project*

Οι βασικές έννοιες που κυριαρχούν στην προδιαγραφή *ID-FF* και προέρχονται κυρίως από την ονοματολογία του *SAML* είναι [71]:

- <u>*Principal*</u>: ειδικά για το περιβάλλον των προδιαγραφών του *Liberty Alliance*, είναι συνώνυμο του χρήστη. Γενικά, όμως είναι μία οντότητα η ταυτότητα της οποίας μπορεί να ελεγχθεί ως προς την αυθεντικότητά της ή να μεταφερθεί μεταξύ «έμπιστων» οργανισμών για τον ίδιο έλεγχο (*Federated*).

- <u>*Identity Provider - IdP*</u>: μία οντότητα συστήματος η οποία υποστηρίζει τα πρωτόκολλα του *Liberty Alliance* και διαχειρίζεται τις πληροφορίες ταυτότητας των *Principals* παρέ-

χοντας *Assertions* αυθεντικοποίησης εκ μέρους των *Principals* στις άλλες οντότητες του συστήματος (*providers*). Στην ορολογία της *SAML* είναι ο συνδυασμός του *Asserting Party* και ενός *Authentication Authority*.

- *Service Provider - SP*: από την πλευρά του *Principal* είναι γενικά ένα Web site με συγκεκριμένες, προσβάσιμες δικτυακές εφαρμογές. Στην ορολογία της *SAML* είναι το *Relying Party*.

- *Liberty Enabled Clients ή Proxies – LECP*: ένας client ο οποίος «γνωρίζει» (ή «ξέρει» πως θα «μάθει») τον *Identity Provider* που θα συνεργαστεί με τον *Service Provider* για την επικύρωση του *Principal*. Ένας "*Liberty-enabled proxy*" είναι ένας HTTP proxy ο οποίος εξομοιώνει έναν "*Liberty-enabled client*" (συνήθως είναι μία πύλη *WAP*[xiv])

Η προδιαγραφή *ID-FF* υλοποιήθηκε έτσι ώστε να ικανοποιεί τις παρακάτω ελάχιστες λειτουργικές απαιτήσεις [69]:

- *Identity Federation*: η οποία εκτός από το βασικό «μοίρασμα» ταυτοτήτων μεταξύ *realms* περιλαμβάνει την ενημέρωση μεταξύ των *Identity Providers* και *Service Providers* για τις πιθανώς πολλαπλές ταυτότητες του ίδιου χρήστη σε διαφορετικά *realms*, για τη λήξη ενός λογαριασμού σε έναν *Identity Provider*, για τη δυνατότητα *Federated* σύνδεσης ανώνυμου *Principal*.

- *Authentication*: η οποία περιλαμβάνει: υποστήριξη κάθε μεθόδου «μετακίνησης» του χρήστη μέσα στους Browsers (εισαγωγή URL στη γραμμή διευθύνσεων, σύνδεση στα «αγαπημένα» κλπ), υποστήριξη κάθε μεθόδου αυθεντικοποίησης, μεταβίβαση ενός ελάχιστου συνόλου πληροφοριών αυθεντικοποίησης («κατάσταση» αυθεντικοποίησης, μέθοδος, ψευδώνυμο), δυνατότητα ενός *Identity Provider* για έμμεση αυθεντικοποίηση ενός χρήστη μέσω δεύτερου *Identity Provider* ο οποίος και θα μεταβιβάσει την πληροφορία της ταυτότητας του χρήστη στον *Service Provider*.

- *Pseudonyms*: η οποία περιλαμβάνει την υποστήριξη ψευδώνυμων ενός χρήστη κατά τη σύνδεσή του σε άλλο *realm* από αυτό που βρίσκεται η ταυτότητά του.

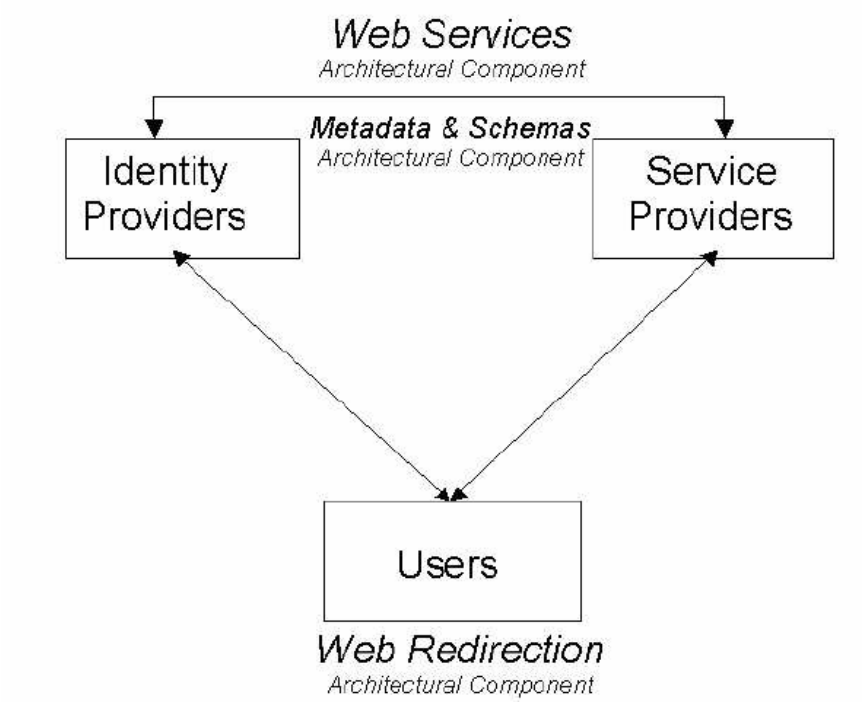
- *Anonymity*: η οποία περιλαμβάνει τη δυνατότητα ενός *Service Provider* να ζητήσει από έναν *Identity Provider* την ανάθεση ενός προσωρινού ψευδωνύμου για τη σύνδεση ενός *Principal*, ώστε να διατηρηθεί η ανωνυμία των πραγματικών στοιχείων ταυτότητας του *Principal*.

- *Global Logout*: η οποία περιλαμβάνει την ενημέρωση του *Service Provider* στην περίπτωση όπου ο χρήστης αποσυνδεθεί (*Logout*) από τον *Identity Provider*.

Τα βασικά συστατικά της αρχιτεκτονικής και φιλοσοφίας της λύσης που προτείνει το *ID-FF* είναι [69]:

[xiv] *Wireless Application Protocol – WAP*: διεθνές πρότυπο με χρήση στις ασύρματες επικοινωνίες. Βασική εφαρμογή του είναι η ενεργοποίηση πρόσβασης στο Internet μέσα από φορητές συσκευές όπως κινητά τηλέφωνα, PDA's κλπ

Πηγή: [69]



Εικόνα 44: Βασική Αρχιτεκτονική του *Liberty Alliance - Identity Federation Framework*

- *Web Redirection*: η ανακατεύθυνση στον Browser του χρήστη από μία σελίδα σε μία άλλη με ταυτόχρονο «πέρασμα» στη νέα διεύθυνση διάφορων παραμέτρων. Αποτελεί τον πιο απλό τρόπο δημιουργίας ενός καναλιού επικοινωνίας μεταξύ του *Identity Provider* και του *Service Provider*, το οποίο έχει την αφετηρία του στο σταθμό του χρήστη. Η *Web Redirection* υλοποιείται με δύο μεθόδους:

  - *HTTP-Redirect-based Redirection*: χρησιμοποιεί τη μέθοδο ανακατεύθυνσης του πρωτοκόλλου HTTP και το συντακτικό των URI's. Στο HTTP, επομένως, χρησιμοποιείται η απάντηση "*Location*" για την ανακατεύθυνση σε μία άλλη σελίδα (πχ "*Location: http://www.foobar.com/auth*") ενώ η πιθανή παράμετρος «ενσωματώνεται» στην εντολή ανακατεύθυνσης με την προσθήκη στην ίδια εντολή τμήματος που ξεκινάει με το "*?*" ("*Location:http://www.foobar.com/auth?XYZ=1234*"). Προκειμένου να δημιουργηθεί το κανάλι επικοινωνίας μεταξύ των δύο Providers, η αλληλουχία των βημάτων που προβλέπει η προδιαγραφή είναι (βλ επόμενη Εικόνα):

    Βήμα 1: Ο χρήστης καλεί τη Web σελίδα του *Service Provider*.

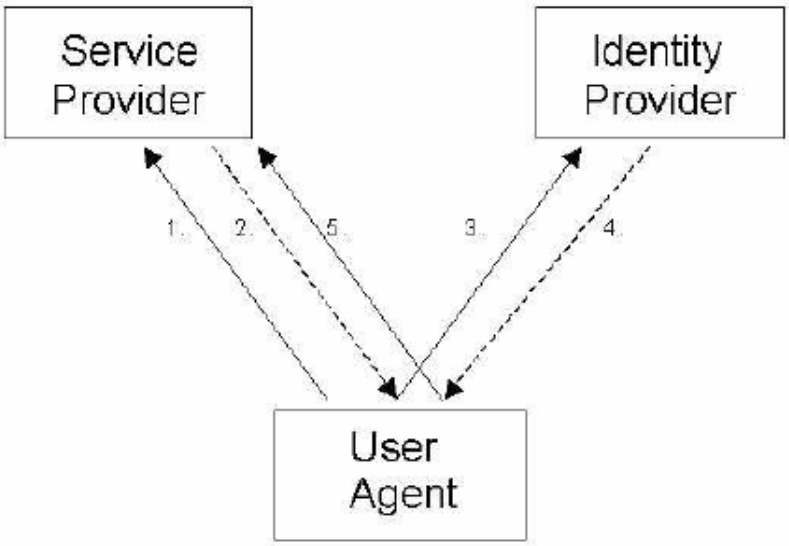
    Βήμα 2: Ο *Service Provider* απαντάει με κωδικό του HTTP 302 (redirection) και μέσω της επικεφαλίδας "*Location*" καθορίζει την URI του *Identity Provider*, ενώ εισάγεται και η δικιά του URI προκειμένου να είναι γνωστή η διεύθυνση επιστροφής.

    Βήμα 3: Ο Browser του χρήστη καλεί τη διεύθυνση του *Identity Provider* (διατηρώντας ως παράμετρο τη διεύθυνση του *Service Provider* από το Βήμα 2).

    Βήμα 4: Ο *Identity Provider* απαντάει με τον HTTP κωδικό της ανακατεύθυνσης στη διεύθυνση του *Service Provider* και τη δική του URI ως προαιρετική, εμβόλιμη παράμετρο.

Βήμα 5: Ο Browser του χρήστη καλεί τη διεύθυνση του *Service Provider* όπως την εντοπίζει στην εντολή ανακατεύθυνσης του προηγούμενου Βήματος 4.

Πηγή: [69]



Εικόνα 45: Κανάλι Επικοινωνίας μέσω Ανακατεύθυνσης στο *Liberty Alliance - Identity Federation Framework*

- *Form-POST-based Redirection*: Είναι μία άλλη μορφή εφαρμογής του Redirection μέσω του Browser του χρήστη η οποία διαφέρει ως προς την προηγούμενη στα Βήματα:

  Βήμα 2: Ο *Service Provider* απαντάει επιστρέφοντας στον Browser του χρήστη μία HTTP φόρμα με παράμετρο "*action*" τη διεύθυνση του *Identity Provider* και παράμετρο "*method*" την τιμή "*POST*". Υπάρχει η δυνατότητα δημιουργίας μέσα στη φόρμα HTTP πεδίων με ελεύθερη εισαγωγή τιμών. Είναι δυνατή, επίσης, η ενσωμάτωση στη φόρμα προγράμματος σε γλώσσα *JavaScript*[xv] για την αυτόματη ενεργοποίηση της φόρμας χωρίς την παρέμβαση του χρήστη.

  Βήμα 3: Η φόρμα εμφανίζεται στον χρήστη και είτε με την ενεργοποίηση του κατάλληλου «κουμπιού» είτε αυτόματα με την εκτέλεση του προγράμματος *JavaScript* εκτελείται η "*action*" της φόρμας και μεταφέρονται τα περιεχόμενα των πεδίων της στη διεύθυνση του *Service Provider* μέσω της εντολής "*POST*".

❖ Web Services: Οι προδιαγραφές των *Profiles* του *ID-FF* καθορίζουν την υλοποίηση κάποιων βημάτων επικοινωνίας με τα παραπάνω *Redirections* και κάποιων άλλων βημάτων μέσω μηνυμάτων που ακολουθούν την προδιαγραφή SOAP. Η επικοινωνία, επομένως, των βασικών οντοτήτων του *ID-FF* μπορεί να γίνει και μέσω SOAP μηνυμάτων που βασίζονται στην XML και ακολουθούν τη φιλοσοφία των Web Services.

[xv] *JavaScript:* η ονομασία ανήκει στην *Sun Microsystems* και είναι το όνομα της εφαρμογής από πλευρά της *Netscape Communications Corporation* του προτύπου scripting languages *ECMAScript* (πρότυπο της *Ecma International* στην προδιαγραφή *ECMA-262*). Είναι γνωστή για τη χρήση της σε Web σελίδες στον προγραμματισμό από την πλευρά του χρήστη (*client-side JavaScript*) [89].

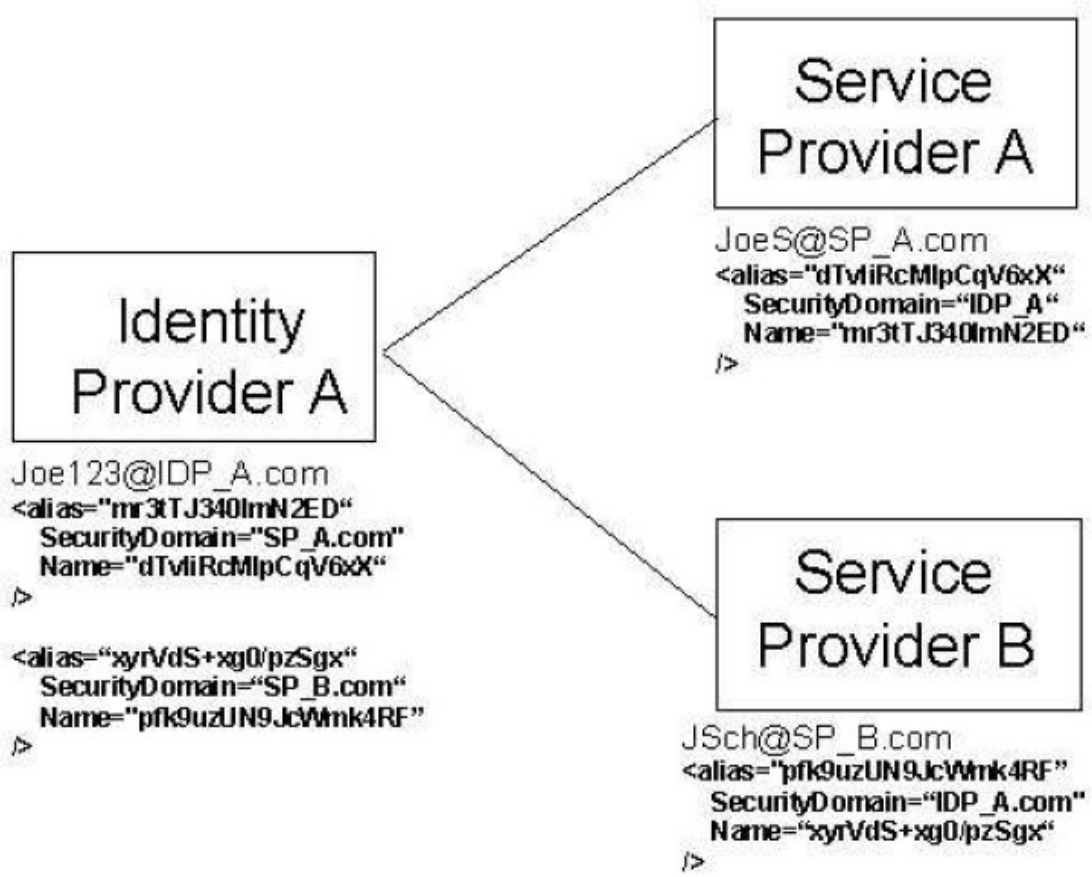
- *Metadata and Schemas*: Με το συγκεκριμένο όρο περιγράφονται όλες οι συμπληρωματικές πληροφορίες που ανταλλάσσουν μεταξύ τους οι *Identity* και *Service Providers* και απαιτούνται για τη λειτουργία της προδιαγραφής. Οι πληροφορίες αφορούν τον ακριβή τρόπο προσδιορισμού των *Principals* από τους *Providers* (ποιο πεδίο των στοιχείων του *Principal* θα χρησιμοποιείται για την αναγνώρισή του), την περιγραφή των χρησιμοποιούμενων μηχανισμών και μεθόδων αυθεντικοποίησης (*Authentication Context*), τις πληροφορίες των *Providers* που είναι απαραίτητες για την αναγνώριση και ταυτοποίησή τους (πχ Ψηφιακά Πιστοποιητικά).

Η βασική απαίτηση, την οποία πρέπει να ικανοποιεί η προδιαγραφή *ID-FF*, είναι η δυνατότητα των χρηστών για Single Sign-On συνδέσεις σε δικτυακές υπηρεσίες ανεξάρτητα από το αν έχουν καταχωρηθεί με τα ίδια στοιχεία στις συγκεκριμένες υπηρεσίες και αν οι υπηρεσίες βρίσκονται στο ίδιο *realm* (*Identity Federation*). Η *ID-FF*, επομένως, αντιμετωπίζει τις απαιτήσεις Single Sign-On και *Identity Federation* στα πλαίσια του ίδιου πρωτοκόλλου "*Single Sign-On and Federation Protocol*" [69]:

- *Υλοποίηση του Identity Federation*: σε πολλές περιπτώσεις δικτυακών υπηρεσιών οι χρήστες καταχωρούνται σε τοπικούς καταλόγους και η ταυτότητά τους συνδέεται και με συγκεκριμένα δικαιώματα που αφορούν την καθεμιά υπηρεσία. Η *Identity Federation* εξασφαλίζει ότι ο χρήστης θα μπορεί να αυθεντικοποιείται με ασφάλεια σε καθεμιά υπηρεσία με βάση την κύρια ταυτότητά του στον *Identity Provider* του *realm* που ανήκει και συνδέοντάς τη με τις τοπικές ταυτότητες που ενδεχομένως διατηρούν οι συγκεκριμένες υπηρεσίες. Κάθε φορά που ένας χρήστης συνδέεται σε έναν *Service Provider* με τον παραπάνω τρόπο δημιουργείται μία νοητή σύνδεση «εμπιστοσύνης» μεταξύ του *Identity* και του *Service Provider*. Μόλις ο χρήστης συνδεθεί σε περισσότερες από μία υπηρεσίες, τότε δημιουργείται μία ολόκληρη «αλυσίδα εμπιστοσύνης» η οποία προκειμένου να ακολουθηθεί απαιτείται το διαδοχικό «πέρασμα» από το κάθε ζευγάρι της αλυσίδας και ο έλεγχος κάθε φορά της μεταξύ τους εμπιστοσύνης. Με αυτό τον τρόπο δεν είναι απαραίτητη η ύπαρξη μίας «κυρίαρχης» ταυτότητας ενός χρήστη, η οποία θα είναι αποθηκευμένη μοναδικά σε κάποιον *Identity Provider* και θα πρέπει όλες οι άλλες ταυτότητες να αναφέρονται σε αυτή.

  Το *ID-FF* εισάγει την έννοια του "*Handle*" για την περιγραφή καθεμιάς *Identity Federation* μεταξύ *Providers*. Τα *Handles* δημιουργούνται κάθε φορά που μία ταυτότητα «μεταφέρεται» από έναν *Provider* σε έναν άλλο και περιλαμβάνει πληροφορίες για την αναγνώριση των *Providers* και του χρήστη σύμφωνα με την τοπική και την «απομακρυσμένη» ταυτότητά του. Ένα παράδειγμα *Identity Federation* ενός χρήστη από τον *Identity Provider* του σε δύο *Service Providers* και τα αντίστοιχα *Handles* που δημιουργούνται φαίνεται στην παρακάτω Εικόνα:

Πηγή: [69]

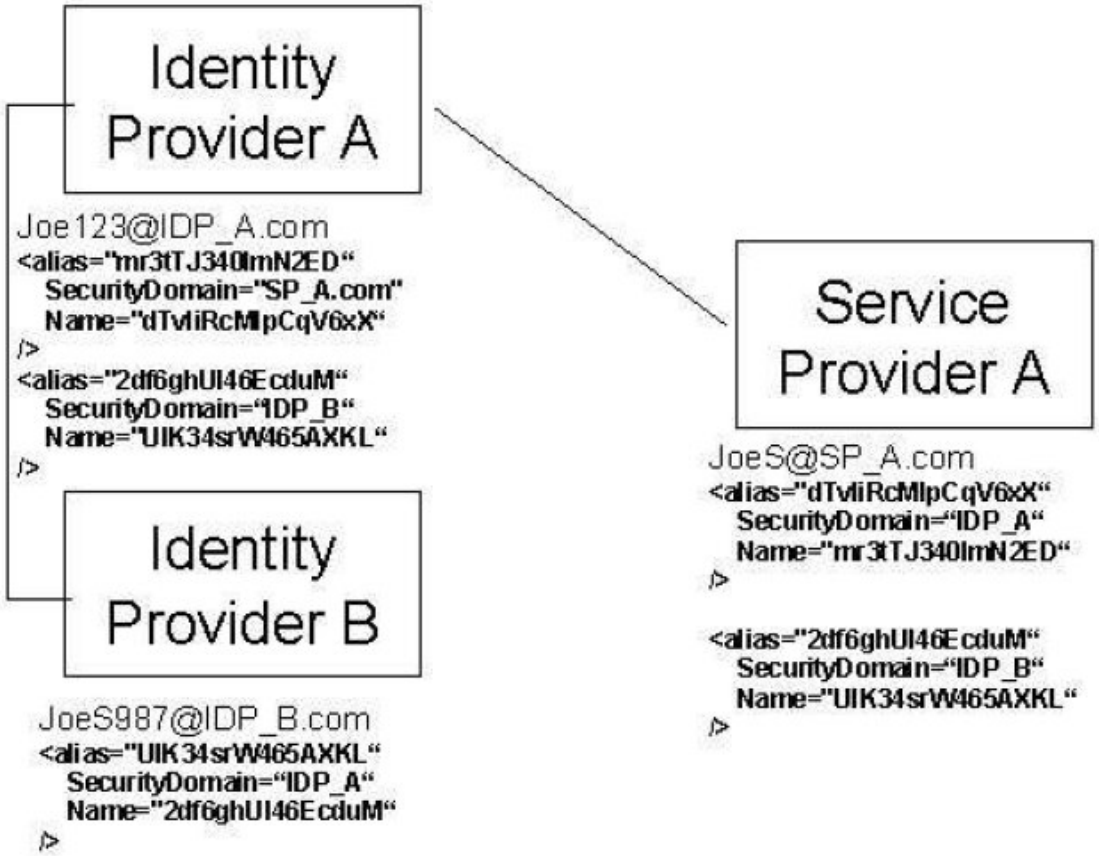


Εικόνα 46: ***Identity Federation* στο *Liberty Alliance - Identity Federation Framework* (Ενας *IdP* – Δύο *SP*)**

όπου σε κάθε οντότητα φαίνονται τα *Handles* των συνδέσεων «εμπιστοσύνης» που διατηρεί η καθεμιά από αυτές. Κάθε *Handles* περιλαμβάνει το όνομα του χρήστη στον τρέχοντα *Provider* (πεδία *Name*) και τα ονόματα που έχει αποκτήσει στους «έμπιστους» *Providers* (πεδία *alias*). Προκειμένου να ταυτοποιηθεί ένας χρήστης σε καθένα *Handle* δημιουργούνται εσωτερικά, τυχαία ονόματα (πχ *Name= "pfk9uzUN9JcWmk4RF"*) τα οποία ισχύουν για καθεμία σύνδεση «εμπιστοσύνης». Οι γραμμές στην παραπάνω Εικόνα υποδεικνύουν την αλυσίδα «εμπιστοσύνης» παρά κανάλια επικοινωνίας.

Με παρόμοιο τρόπο αντιμετωπίζεται το επίσης συχνό σενάριο όπου ο χρήστης διατηρεί ταυτότητες σε δύο *Identity Providers* και επιθυμεί τη σύνδεσή του σε μία δικτυακή υπηρεσία (πχ πρόσβαση από το δίκτυο του εργασιακού χώρου και πρόσβαση μέσω συνδρομητικού δικτύου από το σπίτι). Σε αυτή την περίπτωση απαιτείται η ύπαρξη μόνιμης «έμπιστης» σχέσης μεταξύ των δύο *Identity Providers*, ώστε να γίνονται αποδεκτά τα στοιχεία του χρήστη από τον *Identity Provider* που έχει την έμπιστη σχέση με τη δικτυακή υπηρεσία (βλ. παρακάτω Εικόνα). Ο τρόπος εγκαθίδρυσης της «έμπιστης» σχέσης μεταξύ των *Identity Providers* δεν αποτελεί αντικείμενο της παρούσας προδιαγραφής.

Πηγή: [69]



Εικόνα 47: *Identity Federation* στο "*Liberty Alliance - Identity Federation Framework*" (Δύο IdP – 1 SP)

- *Υλοποίηση του Single Sign-On*: Το Single Sign-On εξασφαλίζεται μόλις ο χρήστης συνδεθεί σε ένα *Service Provider* χωρίς να χρειαστεί να ξανα-εισάγει τα στοιχεία της τοπικής του ταυτότητας, αφού η ταυτότητά του στον *Identity Provider* που συνδέθηκε αρχικά έχει γίνει *Federated* στον *Service Provider* με την παραπάνω διαδικασία. Η υλοποίηση, επομένως, των παραπάνω βασικών σεναρίων *Federated Identity* παρέχει τη δυνατότητα στο χρήστη να αυθεντικοποιείται μόνο μία φορά αρχικά στον *Identity Provider* που τον εξυπηρετεί και μετά ο *Provider* να φροντίζει την μεταβίβαση της εγκυρότητας της ταυτότητάς του σε όλους τους άλλους *Providers* στην αλυσίδα «εμπιστοσύνης».

  Σχετικά με τα θέματα που αφορούν τη διαδικασία αυθεντικοποίησης, υποστηρίζονται πολλοί μηχανισμοί αυθεντικοποίησης όπως: απλό username και password, εφαρμογή ψηφιακών πιστοποιητικών (πχ πρωτόκολλα SSL/TLS), πρωτόκολλο *Kerberos* κλπ. Υπάρχει η δυνατότητα, επίσης, οι *Providers* να διατηρούν την τρέχουσα κατάσταση των χρηστών σε Cookies στην πλευρά του χρήστη ώστε αν χρειαστεί επόμενη επιβεβαίωση της ταυτότητάς του να μην εξετάζονται πάλι όλα τα στοιχεία του στην αλυσίδα «εμπιστοσύνης» μεταξύ των *Providers*.

- *Profiles του Πρωτοκόλλου Single Sign-On and Federation*: το πρωτόκολλο *Single Sign-On and Federation* ορίζει τα μηνύματα που ανταλλάσσονται μεταξύ *Identity* και *Service Providers*. Η αντιστοίχιση των μηνυμάτων σε συγκεκριμένα πρωτόκολλα μετάδοσης (πχ HTTP) ή μηνυμάτων (πχ SOAP) και η ακριβής ακολουθία τους ορίζονται στα *Profiles* του πρωτοκόλλου:
  - *Liberty Artifact Profile*: χρησιμοποιεί την μέθοδο της ανακατεύθυνσης του HTTP με την ενσωμάτωση μίας σχεδόν τυχαίας τιμής ως παραμέτρου της URI ανακατεύθυνσης. Η ενσωματωμένη τιμή χρησιμοποιείται μόνο μία φορά και ενεργοποιεί από την πλευρά του *Service Provider* την αποστολή από την πλευρά του *Identity Provider* ενός *Assertion* για μία συγκεκριμένη ταυτότητα. Η ενσωμάτωση στην URI μίας ψευδο-τυχαίας τιμής μίας χρήσης παρέχει προστασία απέναντι στην απειλή των *Replay Attacks* και στην εικασία της τιμής από κάποιον τρίτο (*guessing*).
  - *Liberty Browser POST Profile*: ακολουθεί την ίδια φιλοσοφία με την προηγούμενη μέθοδο με τη διαφορά ότι οι τιμές που ανταλλάσσονται μεταξύ των *Providers* είναι κρυφά πεδία HTTP φορμών και η ανακατεύθυνση μεταξύ των *Providers* γίνεται αυτόματα με τις κατάλληλες *JavaScript* εντολές. Με αυτή τη μέθοδο των πεδίων HTTP φόρμας είναι εφικτή η μετάδοση δεδομένων μεγάλου μεγέθους, έτσι ώστε ένα ολόκληρο *Assertion* να μπορεί να μεταδοθεί από τον *Identity* στον *Server Provider*.
  - *Liberty-Enabled Client and Proxy Profile*: καθορίζει τον τρόπο επικοινωνίας των *Liberty Enabled Clients* και *Proxies* με τους *Identity* και *Service Providers*. Ένας *Liberty Enabled Client* ανταλλάσσει μηνύματα με τη χρήση της μεθόδου *POST* του HTTP αντί της ανακατεύθυνσης.

2.4.6.2 To Project "Shibboleth"

Η προδιαγραφή *Shibboleth* είναι προϊόν της επιτροπής M*iddleware Architecture Committee for Education – MACE* του οργανισμού *Internet2* και της εταιρίας IBM και αφορά την ανάπτυξη ενός μηχανισμού ο οποίος να στηρίζεται σε αποδεκτά πρότυπα και να εξασφαλίζει την αυθεντικοποίηση και την εξουσιοδότηση των μελών της ακαδημαϊκής κοινότητας για την πρόσβαση πόρων σε ιδρύματα εκτός αυτού όπου ανήκουν, αλλά είναι μέλη μίας ευρύτερης ακαδημαϊκής συνεργασίας. Το *Shibboleth*, επομένως, λειτουργεί «πάνω» από τις επιμέρους λύσεις αυθεντικοποίησης και ελέγχου πρόσβασης του κάθε Ιδρύματος και ανεξάρτητα από τις τεχνολογίες που αυτές χρησιμοποιούν, επιτρέπει την ενιαία αυθεντικοποίηση των χρηστών σε όλα τα συνεργαζόμενα Ιδρύματα με τη χρήση μόνο του λογαριασμού που διατηρούν στο δικό τους Ίδρυμα. Ιδιαίτερη σημασία δίδεται στην ανταλλαγή μεταξύ των Ιδρυμάτων πρόσθετων χαρακτηριστικών του χρήστη, ώστε να είναι δυνατή η λήψη αποφάσεων ελέγχου πρόσβασης στους δικτυακούς πόρους, καθώς μέσα σε ένα Ακαδημαϊκό περιβάλλον υψηλού επιπέδου υπάρχουν αρκετές διαβαθμίσεις στις προσφερόμενες πληροφορίες και υπηρεσίες [53].

Η αρχιτεκτονική του *Shibboleth* επεκτείνει τους μηχανισμούς Single Sign-On και ανταλλαγής χαρακτηριστικών της *SAML* 1.1 με την επανα-διατύπωση συγκεκριμένων *Profiles* της *SAML*. Τα βασικά πρότυπα πάνω στα οποία βασίζεται η προδιαγραφή *Shibboleth* είναι τα: HTTP, XML, *XML Schema*, *XML Signature*, SOAP, *SAML* και ο σκοπός είναι η δημιουργία ενός

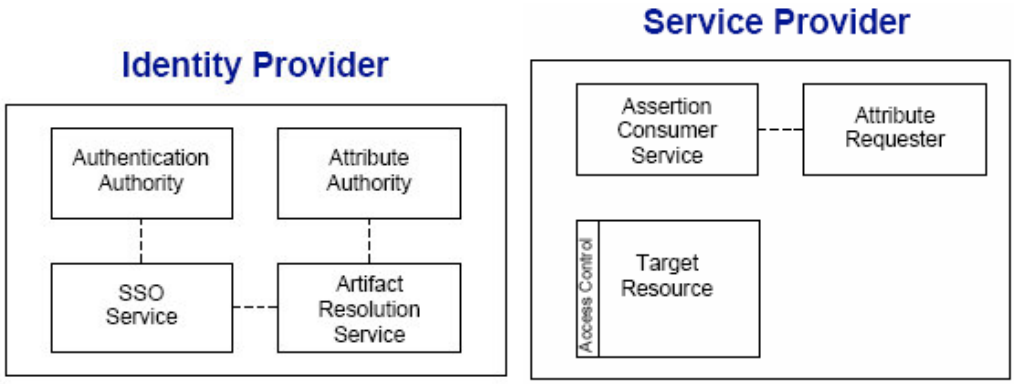
προϊόντος πλήρως «ανοιχτού κώδικα». Τα συστατικά της συγκεκριμένης αρχιτεκτονικής είναι [55]:

- *Identity Provider - IdP*: διατηρεί τα στοιχεία των χρηστών και τις ιδιότητές τους και μετά από σχετικό αίτημα μπορεί να δημιουργεί *Assertions* αυθεντικοποίησης ή ιδιοτήτων των χρηστών προς τα *Relying Parties* (τους *Service Providers*). Αποτελείται από τα υποσυστήματα:
  - *Authentication Authority*: «εκδίδει» τις δηλώσεις αυθεντικοποίησης προς τις υπόλοιπες οντότητες σε συνεργασία με την υπηρεσία – μηχανισμό αυθεντικοποίησης που έχει εγκατασταθεί στον *Provider*, αλλά δεν αποτελεί μέρος της προδιαγραφής του *Shibboleth*.
  - *Single Sign-On Service*: είναι ένας πόρος του *IdP* διαθέσιμος μέσω του HTPP έτσι ώστε να αποτελεί το πρώτο σημείο επαφής του client με τον *IdP*. Επεξεργάζεται την κλήση αυθεντικοποίησης που δέχεται μέσω του Browser από τον *Service Provider* και ξεκινάει τη διαδικασία αυθεντικοποίησης με την τελική ανακατεύθυνση του client στην υπηρεσία *Inter-site Transfer Service*.
  - *Inter-site Transfer Service*: είναι ένας πόρος του *IdP* διαθέσιμος μέσω του HTTP και συνεργάζεται με την *Authentication Authority* ώστε να αποστείλει τις κατάλληλες HTTP απαντήσεις αυθεντικοποίησης στον Browser του *Principal* ανάλογα με το *Profile* που εφαρμόζεται. Στην περίπτωση του *Browser/POST Profile* η HTTP απάντηση περιέχει μία HTML φόρμα με τα κατάλληλα πεδία που έχουν ως τιμές τους το *Assertion* μέσα σε ένα ψηφιακά υπογεγραμμένο μήνυμα *<samlp:Response>*. Στην περίπτωση του *Browser/Artifact Profile* η HTTP απάντηση περιέχει μία εντολή *Location* η οποία ανακατευθύνει τον Browser του χρήστη σε έναν *SP* με παράμετρο στην URL ένα *SAML Artifact*.
  - *Artifact Resolution Service*: όταν χρησιμοποιείται το *Profile Browser/Artifact* ο *IdP* αποστέλλει στον *Service Provider (SP)* ένα "*artifact*" (μία αναφορά σε *Assertion*) παρά ένα κανονικό *Assertion*. Στη συνέχεια, ο *SP* ζητάει το πλήρες *Assertion* από την υπηρεσία *Artifact Resolution Service* του *IdP* με βάση το *artifact* που έχει δεχθεί.
  - *Attribute Authority*: επεξεργάζεται τα αιτήματα για δηλώσεις των πρόσθετων ιδιοτήτων χρήστη και αφού τα εντοπίσει, συνθέτει τα κατάλληλα *Assertions*.
- *Service Provider – SP*: διαχειρίζεται προστατευόμενους δικτυακούς πόρους (Web Applications). Η πρόσβαση των χρηστών βασίζεται στην ύπαρξη *Assertions* αυθεντικοποίησης των χρηστών τα οποία έχουν παραχθεί από κάποιον *IdP*. Ο έλεγχος της αυθεντικοποίησης των χρηστών γίνεται με εσωτερική διαδικασία στον *SP* που προστατεύει τον δικτυακό πόρο. Τα συστατικά του *SP* είναι:
  - *Assertion Consumer Service*: αποτελεί το άλλο άκρο της συναλλαγής με την υπηρεσία SSO του *IdP* και στην αρχική έκδοση του *Shibboleth* ονομαζόταν *SHIRE*. Επεξεργάζεται το *Assertion* αυθεντικοποίησης το οποίο δέχεται από τον *IdP*, αποστέλλει προαιρετικά νέο αίτημα πρόσθετων ιδιοτήτων του χρήστη και προωθεί το χρήστη στον αρχικά αιτούμενο δικτυακό πόρο.
  - *Attribute Requester*: έχει τη δυνατότητα δημιουργίας ενός καναλιού επικοινωνίας με το υπο-σύστημα *Attribute Authority* του *IdP* για την ανταλλαγή πρόσθετων ιδιοτή-

των του χρήστη, μόλις αυτός αυθεντικοποιηθεί, χωρίς να χρησιμοποιείται το σύνηθες κανάλι μέσω του Browser του χρήστη. Στην αρχική έκδοση του *Shibboleth* ονομάζεται *SHAR*.

Οι δύο βασικοί *Providers* του *Shibboleth* με τα υπο-συστήματά τους φαίνονται στην παρακάτω Εικόνα:

Πηγή: [55]



Εικόνα 48: *Identity Provider* και *Service Provider* στην προδιαγραφή *Shibboleth*

Σημαντικά συστατικά της αρχιτεκτονικής του *Shibboleth* αποτελούν και τα εξής [55]:

- *"Where Are You From?" (WAYF) Service*: είναι μία προαιρετική υπηρεσία με την οποία ο SP μπορεί να αποφασίσει ποιος είναι ο προτεινόμενος *IdP* για τον τρέχοντα χρήστη. Η συγκεκριμένη απόφαση μπορεί να ληφθεί με ή χωρίς την παρέμβαση του χρήστη.

- *Metadata*: οι δύο *Providers* αποστέλλουν πληροφορίες που περιγράφουν τα βασικά χαρακτηριστικά τους με τη μορφή XML αρχείων τα οποία καλούνται *Metadata*. Τα συγκεκριμένα αρχεία μεταφέρονται «υπογεγραμμένα» με ψηφιακή υπογραφή ώστε να εξασφαλιστεί η ακεραιότητά τους και αφορούν πληροφορίες για υπο-συστήματα των *IdP* και *SP* οι οποίες ενσωματώνονται σε αντίστοιχα πεδία της XML:
  - *<md:IDPSSODescriptor>*, για πληροφορίες που αφορούν την υπηρεσία SSO του *IdP*.
  - *<md:SPSSODescriptor>*, για πληροφορίες που αφορούν την υπηρεσία *Assertion Consumer Service* του *SP*.
  - *<md:AuthnAuthorityDescriptor>*, για πληροφορίες που αφορούν την *Authentication Authority* του *IdP*.
  - *<md:AttributeAuthorityDescriptor>*, για πληροφορίες που αφορούν την *Attribute Authority* του *IdP*.

Τα *Profiles* που βασίζονται στη λειτουργία του Web Browser του χρήστη και προδιαγράφει το *Shibboleth* για την υλοποίηση SSO είναι τα *Browser/POST Profile* και *Browser/Artifact Profile* τα οποία επεκτείνουν τα ομώνυμα *Profiles* της *SAML* 1.1. Τα *Profiles* του *Shibboleth* προϋποθέτουν ότι ο χρήστης επιχειρεί να προσπελάσει πρώτα έναν πόρο σε έναν *SP* και από αυτό το σημείο ξεκινάει η διαδικασία SSO. Η *SAML*, όμως, διατυπώνει και την περίπτωση όπου ο χρήστης προσπελαύνει απευθείας έναν *IdP* για αυθεντικοποίηση «περνώντας» ως πα-

ραμέτρους τα στοιχεία του *SP*. Για λόγους συμβατότητας το *Shibboleth* καλύπτει και αυτό το σενάριο με το *Authentication Request Profile* [55]:

- *Authentication Request Profile*: είναι μία κλήση στην SSO υπηρεσία του *IdP* μέσω μίας URL στην οποία εκτός από τη διεύθυνση της SSO υπηρεσίας υπάρχουν ως παράμετροι:
  - *providerId*: η URI του *SP*.
  - *shire*: η θέση της υπηρεσίας *Assertion Consumer Service* του *SP*.
  - *target*: η διεύθυνση του πόρου τον οποίο επιθυμεί να προσπελάσει ο χρήστης.
  - *time*: (προαιρετική) η τρέχουσα ώρα.

  Ένα παράδειγμα μίας κλήσης *Authentication Request* είναι:

  https://idp.example.org/shibboleth/SSO?
  target=*https://sp.example.org/myresource*&
  shire=*https://sp.example.org/shibboleth/SSO*&
  providerId=*https://sp.example.org/shibboleth*&
  time=*1102260120*

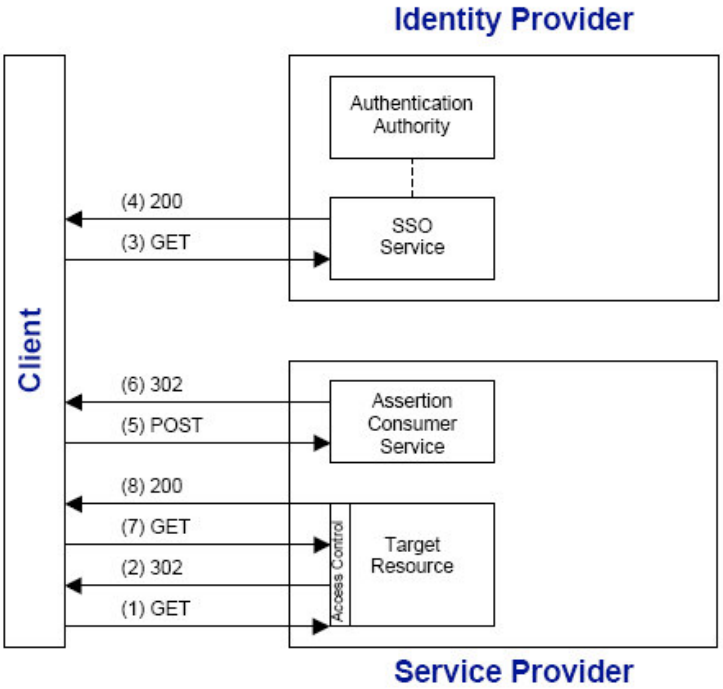
- *Browser/POST Profile*: είναι συνδυασμός των *Shibboleth Authentication Request profile* και του *SAML* 1.1 *Browser/POST profile*. Η ακολουθία των μηνυμάτων του *Profile* φαίνεται στην παρακάτω Εικόνα:
  - *Βήμα 1*: ο χρήστης επιχειρεί να προσπελάσει την προστατευόμενη υπηρεσία στον *SP*, ο οποίος εκτελεί έλεγχο ασφαλείας στον χρήστη και αν εντοπίσει τα απαραίτητα στοιχεία, επιτρέπει την πρόσβαση:

    https://sp.example.org/myresource
  - *Βήμα 2*: στην περίπτωση όπου αποτύχει ο έλεγχος ασφαλείας του χρήστη, ο *SP* ανακατευθύνει τον χρήστη στην SSO υπηρεσία του *IdP*, με τις κατάλληλες παραμέτρους στην URL.
  - *Βήμα 3*: ο Browser του χρήστη εκτελεί την ανακατεύθυνση προς την SSO υπηρεσία του *IdP,*

    https://idp.example.org/shibboleth/SSO?
    target=*https://sp.example.org/myresource*&
    shire=*https://sp.example.org/shibboleth/SSO/POST*&
    providerId=*https://sp.example.org/shibboleth*

    Η SSO υπηρεσία επεξεργάζεται το αίτημα αυθεντικοποίησης και αφού εντοπίσει την ταυτότητα του χρήστη δημιουργεί μία δήλωση αυθεντικοποίησης.

Πηγή: [55]



Εικόνα 49: *Browser/POST Profile* της προδιαγραφής *Shibboleth*

- *Βήμα 4*: η υπηρεσία SSO απαντάει με μία HTML φόρμα:

```
<form method="post"
        action="https://sp.example.org/shibboleth/SSO/POST" ...>
    <input name="TARGET" type="hidden"
            value="https://sp.example.org/myresource" />
    <input name="SAMLResponse" value="response" type="hidden" />
      ...
    <input type="submit" value="Submit" />
</form>
```

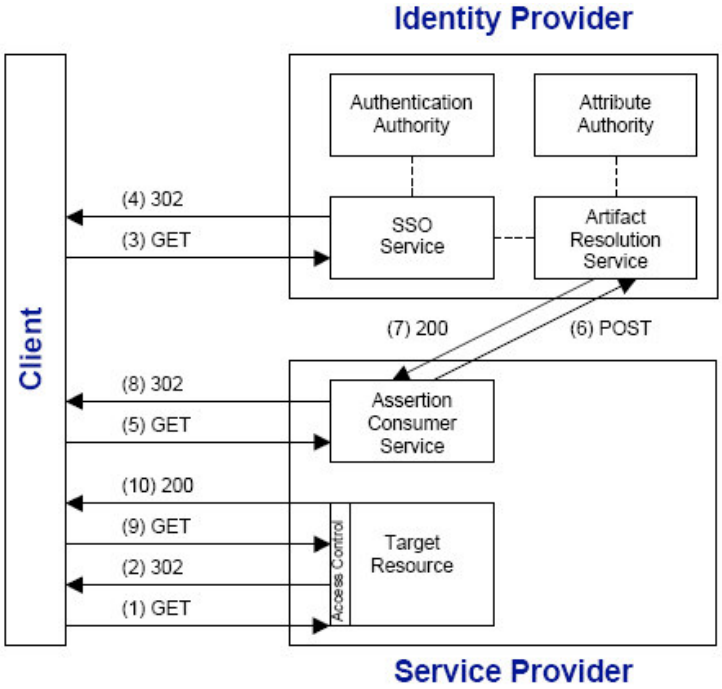
  Όπου η τιμή του πεδίου "*SAMLResponse*" είναι ένα κωδικοποιημένο *SAML Assertion*.

- *Βήμα 5*: ο χρήστης εκτελεί το κουμπί ενεργοποίησης της φόρμας στον Browser του οπότε και μεταφέρεται η κλήση *POST* στην υπηρεσία *Assertion Consumer Service* του *SP*. Η εκτέλεση της φόρμας μπορεί να υλοποιηθεί και αυτόματα με την ενσωμάτωση στην HTML εντολών *Javascript*.
- *Βήμα 6*: η υπηρεσία *Assertion Consumer Service* του *SP* ελέγχει το *Assertion* του χρήστη και εφόσον είναι έγκυρο και σωστό εκδίδει ένα τοπικό πιστοποιητικό ασφαλείας του χρήστη και ανακατευθύνει τον Browser του χρήστη στον αρχικό πόρο.
- *Βήμα 7*: ο χρήστης επιχειρεί ξανά να προσπελάσει τον ζητούμενο πόρο στον *SP* (ίδια εντολή με Βήμα 1).
- *Βήμα 8*: από τη στιγμή που ο χρήστης έχει αυθεντικοποιηθεί στο προηγούμενο βήμα ο *SP* του επιτρέπει την πρόσβαση.

Στο παραπάνω Βήμα 2 γίνεται η υπόθεση ότι ο *SP* γνωρίζει ποιος είναι ο *IdP* που υποστηρίζει τον τρέχοντα χρήστη. Στην περίπτωση όπου αυτή η παράμετρος δεν είναι γνωστή τότε ο *SP* εφαρμόζει διαδικασία προσδιορισμού του *IdP* (*Identity Provider Discovery*) η οποία υποβοηθείται από την υπηρεσία *WAYF* ("*Where are you from?*"). Συνεπώς, στο παραπάνω Βήμα 2 ο *SP* ανακατευθύνει το χρήστη στην *WAYF* υπηρεσία και ο χρήστης προσπελαύνει αυτή την υπηρεσία. Η *WAYF* υπηρεσία συνήθως εμφανίζει στο χρήστη μία σελίδα με προτεινόμενους *IdP* από τους οποίους ο χρήστης επιλέγει αυτόν στον οποίο είναι καταχωρημένος. Στη συνέχεια η *WAYF* αποστέλλει στο χρήστη ένα Cookie με τον επιλεγμένο *IdP* για μελλοντική χρήση και ανακατευθύνει τον Browser στην υπηρεσία SSO του *IdP*. Η ροή του *Profile* συνεχίζει από το παραπάνω Βήμα 3.

- *Browser/Artifact Profile*: Είναι ο συνδυασμός του *Shibboleth Authentication Request Profile* και του *SAML 1.1 Browser/Artifact Profile*. Η ακολουθία των μηνυμάτων του *Profile* φαίνεται στην παρακάτω Εικόνα:

Πηγή: [55]



Εικόνα 50: *Browser/Artifact Profile* της προδιαγραφής *Shibboleth*

Η βασική διαφορά με το *Browser/POST Profile* είναι τα Βήματα 6 & 7 της Εικόνας όπου ο *SP* αναζητεί το *Assertion* με βάση το *artifact* που έχει δεχθεί στο Βήμα 5 από τον *IdP*. Άρα το Βήμα 5 στην Εικόνα είναι μία κλήση του χρήστη προς την υπηρεσία *Assertion Consumer Service* του *SP* της μορφής:

https://sp.example.org/shibboleth/SSO/Artifact?
TARGET=*https://sp.example.org/myresource*&
SAMLart=*AAEwGDwd3Z7Fr1GPbM82Fk2CZbpNB1dxD%2Bt2Prp%2BTDtqx VA78iMf3F23*

όπου η παράμετρος *SAMLart* μεταφέρει το *artifact* του *IdP*.

Στη συνέχεια, στο Βήμα 6 η *Assertion Consumer Service* αποστέλλει απευθείας στην *Artifact Resolution Service* του *IdP* αίτηση *<samlp:Request>*, μέσω SOAP μηνύματος, για τον εντοπισμό του *Assertion*:

```
POST /shibboleth/Artifact HTTP/1.1
Host: idp.example.org
Content-Type: text/xml
Content-Length: nnn
SOAPAction: http://www.oasis-open.org/committees/security
<?xml version="1.1" encoding="ISO-8859-1"?>
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header/>
    <SOAP-ENV:Body>
        <samlp:Request
            xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
            MajorVersion="1" MinorVersion="1"
            RequestID="f81d4fae-7dec-11d0-a765-00a0c91e6bf6"
            IssueInstant="2004-12-05T09:22:04Z">
            <samlp:AssertionArtifact>
                AAEwGDwd3Z7Fr1GPbM82Fk2CZbpNB1dxD+t2Prp+TDtqxVA78iMf3F
                23
            </samlp:AssertionArtifact>
        </samlp:Request>
    </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

όπου η τιμή του πεδίου *<samlp:AssertionArtifact>* είναι το *artifact* του Βήματος 5. Στη συνέχεια η υπηρεσία *Artifact Resolution Service* του *IdP* εξετάζει το *artifact* που δέχεται και εφόσον είναι υπαρκτό δημιουργεί μία απάντηση *<samlp:Response>* με το ζητούμενο *Assertion* όπως παρακάτω:

```
HTTP/1.1 200 OK
Content-Type: text/xml
Content-Length: nnnn

<?xml version="1.1" encoding="ISO-8859-1"?>
<SOAP-ENV:Envelope
    xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
    <SOAP-ENV:Header/>
    <SOAP-ENV:Body>
        <samlp:Response
            xmlns:samlp="urn:oasis:names:tc:SAML:1.0:protocol"
            MajorVersion="1" MinorVersion="1"
            Recipient="https://sp.example.org/shibboleth/SSO/Artifact"
            ResponseID="00099cf1-a355-10f9-9e95-004005b13a2b"
            InResponseTo="f81d4fae-7dec-11d0-a765-00a0c91e6bf6"
            IssueInstant="2004-12-05T09:22:05Z">
            <samlp:Status>
```

```
            <samlp:StatusCode Value="samlp:Success"/>
        </samlp:Status>
        <!-- insert SAML assertion here (see section 3.1) -->
    </samlp:Response>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Τα υπόλοιπα βήματα του *Browser/Artifact Profile* είναι τα ίδια με αυτά του *Browser/POST Profile*. Επίσης, η προαιρετική λειτουργία της υπηρεσίας *WAYF* είναι ίδια με αυτή που περιγράφηκε στο προηγούμενο *Profile Browser/POST*.

3. ΑΞΙΟΛΟΓΗΣΗ ΜΕΘΟΔΩΝ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ

3.1 Επισκόπηση Χαρακτηριστικών των Βασικών Προδιαγραφών Αυθεντικοποίησης

Τα πρωτόκολλα και οι διαδικασίες της παραγράφου 2.3.1 σχετίζονται με την αυθεντικοποίηση, αλλά καλύπτουν διαφορετικές φάσεις και απαιτήσεις της. Συνεπώς, δεν μπορούν να θεωρηθούν ομοειδή άρα και συγκρίσιμα και η εκτίμηση της σημασίας τους μπορεί να γίνει ξεχωριστά για το καθένα, διατυπώνοντας τα γενικά συμπεράσματα που προκύπτουν μετά την αναλυτική παρουσίασή τους στο Θεωρητικό μέρος της παρούσας εργασίας.

3.1.1 *Kerberos*

Το *Kerberos* είναι πολύ διαδεδομένο πρωτόκολλο αυθεντικοποίησης και από τα πρώτα που εισήγαγε την εκτέλεση της αυθεντικοποίησης όχι από το σύστημα που δέχεται την κλήση ενός χρήστη, αλλά από ένα τρίτο σύστημα το οποίο είναι κοινώς έμπιστο από τα υπόλοιπα μέρη του δικτύου. Το *Kerberos* θεωρείται ιδανική λύση αυθεντικοποίησης σε δικτυακά περιβάλλοντα Client – Server για την πρόσβαση σε πόρους τοπικών δικτύων. Επίσης, αποτελεί ασφαλή λύση αυθεντικοποίησης σε δικτυακές εφαρμογές στα πλαίσια ενός Intranet στο οποίο όμως εφαρμόζονται αυστηρά τεχνολογίες Microsoft, ο Internet Explorer ως Web Browser και ο IIS ως Web Server. Σε αυτές τις περιπτώσεις μπορεί να εξασφαλίσει και Single Sign – On του χρήστη. Αντίθετα, δεν είναι δυνατή η εφαρμογή του στην αυθεντικοποίηση σε υπηρεσίες του Internet και συνεπώς δεν μπορεί να συμπεριληφθεί στις λύσεις Web SSO. Αυτό συμβαίνει γιατί [86]:

- Υπάρχουν εγγενείς δυσκολίες στην εγκατάσταση *Key Distribution Center* (*KDC*), όπως για παράδειγμα ένα *Active Directory*, το οποίο να είναι προσβάσιμο από τις Internet εφαρμογές, μέσω του Web Server, από απροσδιόριστο αριθμό χρηστών.

- Δεν υποστηρίζουν όλοι οι Web Servers το πρωτόκολλο *Kerberos* πάνω από το HTTP. Το συγκεκριμένο γεγονός καθιστά απαγορευτική την εφαρμογή του καθώς δεν είναι δυνατή η επιβολή συγκεκριμένων προτύπων ή εκδόσεων Web Browser μέσα στο ποικιλόμορφο περιβάλλον του Internet.

Ένα από τα σημαντικά πλεονεκτήματά του είναι η δυνατότητα επέκτασης της λειτουργίας του πρωτοκόλλου και για αυθεντικοποίηση χρηστών εκτός του realm στο οποίο αυτοί ανήκουν. Είναι εφικτή, επομένως, η inter-realm αυθεντικοποίηση με την κατάλληλη εγκατάσταση κοινών κλειδιών για την επικοινωνία των *KDC's* των δύο έμπιστων οργανισμών. Αυτό σημαίνει ότι είναι απαραίτητη η προηγούμενη ρύθμιση των παραμέτρων συνεργασίας των οργανισμών που ελέγχονται από την καθεμιά εγκατάσταση του *Kerberos* και δεν μπορεί να θεωρηθεί ως υλοποίηση πλήρους *Federated Identity Management*. Επίσης, η εγκατάσταση υποδομής PKI μεταξύ έμπιστων οργανισμών είναι αποδοτικότερη με αποτέλεσμα το συγκεκριμένο χαρακτηριστικό του *Kerberos* να μην αξιοποιείται ιδιαίτερα [105].

Στα θέματα της ασφάλειας, η έκδοση 5 του *Kerberos* θεωρείται ότι κάλυψε πολλά από τα κενά των προηγούμενων εκδόσεων και προσφέρει υψηλό βαθμό ασφαλείας. Είναι ωστόσο ευά-

λωτο σε «απειλές» πρόβλεψης passwords ("*password guessing*") κατά τη φάση απόκτησης του *TGT*, καθώς η υπηρεσία *TGS* θα δημιουργήσει και αποστείλει στο χρήστη ένα *TGT* ανεξάρτητα αν αυτός αποδείξει ότι κατέχει το απαραίτητο password με το οποίο η *TGS* κωδικοποίησε το *TGT*. Παρόλο που το *TGT* έχει περιορισμένη χρονική διάρκεια, υπάρχει χρόνος για εξαπόλυση «επίθεσης» πρόβλεψης του password στον client ώστε να αποκρυπτογραφηθεί το *TGT* [105]. Η αντιμετώπιση του συγκεκριμένου κινδύνου μπορεί να επιτευχθεί με ένα πρόσθετο βήμα αυθεντικοποίησης του client ακόμα και μέσω της κρυπτογράφησης Δημοσίου Κλειδιού. Δηλαδή, το session key που θα χρησιμοποιηθεί για την επικοινωνία του client με το *KDC* μπορεί να αποσταλεί κρυπτογραφημένο όχι όμως με ένα αμοιβαίως γνωστό, σταθερό κλειδί, αλλά με το Δημόσιο Κλειδί του χρήστη. Με αυτό τον τρόπο υπάρχει η βεβαιότητα ότι η αποκρυπτογράφηση θα μπορέσει να γίνει μόνο από το χρήστη που κατέχει το αντίστοιχο Ιδιωτικό Κλειδί. Το μόνο κενό που απομένει είναι η βεβαιότητα ότι το συγκεκριμένο ζευγάρι Δημοσίου – Ιδιωτικού κλειδιού ανήκει στον επιθυμητό χρήστη που είναι εγγεγραμμένος στον *KDC*, αλλά αυτό εξασφαλίζεται από την υφιστάμενη υποδομή PKI και την εγκυρότητα των *CA's* που «υπογράφουν» τα κλειδιά [141].

3.1.2 *Integrated Windows Authentication – IWA*

Το πρότυπο *IWA* δεν αποτελεί πρωτόκολλο αλλά μία διαδικασία αυθεντικοποίησης κατά την οποία αρχικά επιλέγεται το κατάλληλο πρωτόκολλο αυθεντικοποίησης ανάλογα με τις ρυθμίσεις και την τρέχουσα κατάσταση των συστημάτων που επικοινωνούν μεταξύ τους. Η εφαρμογή του περιορίζεται μόνο σε περιβάλλοντα του λειτουργικού συστήματος Windows της Microsoft. Αποτελεί μία από τις επιλογές αυθεντικοποίησης στον Web Server των Windows, IIS, άρα μπορεί να χρησιμοποιηθεί σε Web εφαρμογές και χαρακτηρίζεται από την ευκολία εγκατάστασης, εφόσον έχουν ρυθμιστεί σωστά τα υφιστάμενα πρωτόκολλα αυθεντικοποίησης. Κατά βάση στηρίζεται στο πρωτόκολλο *Kerberos*, άρα το *IWA* διατηρεί τις αδυναμίες επέκτασης της εφαρμογής του. Συγκεκριμένα, αποτελεί μία λύση αυθεντικοποίησης που μπορεί να εφαρμοστεί σε ηλεκτρονικές εφαρμογές εντός των ορίων του Intranet ενός Οργανισμού και μόνο σε περιβάλλοντα Windows της Microsoft. Η στενή συνεργασία με το *Active Directory* των Windows αποτελεί το βασικό παράγοντα περιορισμένης εφαρμογής του στα πλαίσια ενός Intranet. Ένας επιπλέον λόγο είναι ότι το *IWA* διατηρεί μία εγγενή αδυναμία λειτουργίας πάνω από συνδέσεις που διέρχονται από HTTP Proxies, καθώς η λειτουργία του απαιτεί επικοινωνία «*βασισμένη σε σύνδεση*» ("*connection – based*"), ενώ οι Proxies γενικά δεν διατηρούν συνδέσεις [84].

3.1.3 *Security Assertion Markup Language – SAML*

Η έννοια του "*Federation*" αποτελεί την κυρίαρχη τάση στα σύγχρονα συστήματα Διαχείρισης Ταυτοτήτων. Η ανάπτυξη, δηλαδή, συμφωνιών μεταξύ οργανισμών οι οποίες βασίζονται σε κρυπτογραφικές μεθόδους συγκρότησης «έμπιστων» σχέσεων και στον καθορισμό κοινών πολιτικών ασφαλείας ώστε να επιτευχθεί ομοιόμορφη μεταξύ τους επικοινωνία στο επίπεδο της διαχείρισης ταυτοτήτων. Τα συστήματα ανάπτυξης "*Federations*" επιδιώκουν την απομόνωση των τεχνικών λεπτομερειών της Διαχείρισης Ταυτοτήτων ενός οργανισμού από αυτές των άλλων μέσω πρότυπων μηχανισμών και κοινώς αποδεκτών μορφοποιήσεων της μεταδιδόμενης πληροφορίας ταυτοτήτων, μέσω δηλαδή ενός αποδοτικού πρωτοκόλλου. Η *SAML* –

Security Assertion Markup Language υλοποιεί ακριβώς αυτό το στόχο καθώς βασίζεται στην XML για την ανάπτυξη μίας γλώσσας περιγραφής πληροφοριών ταυτοτήτων χρηστών, πρόσθετων ιδιοτήτων των χρηστών και πληροφοριών δικαιωμάτων ή ρόλων των χρηστών. Τα δομικά συστατικά και τα τεχνικά χαρακτηριστικά της *SAML* αναπτύχθηκαν στην παρ. 2.3.1.3 και από αυτά προκύπτουν και οι βασικές χρήσεις της *SAML* σε πραγματικά «σενάρια» εφαρμογής της [101]:

- *Web Single Sign-On*: Η *SAML* μπορεί να υλοποιήσει Web SSO μέσω της μετάδοσης *Assertions* αυθεντικοποίησης από τον οργανισμό που διατηρεί τα δεδομένα ταυτότητας ενός χρήστη σε ένα οργανισμό που διαθέτει την ηλεκτρονική υπηρεσία που επιθυμεί να προσπελάσει ο χρήστης, εφόσον ελεγχθεί η ταυτότητά του και θεωρηθεί αξιόπιστο το *Assertion* του οργανισμού που εκτέλεσε την καθαυτό αυθεντικοποίηση.

- *Attribute-Based Authorization*: Το συγκεκριμένο «σενάριο» είναι παρόμοιο με το Web SSO με τη διαφορά ότι το *Assertion* της *SAML* μπορεί να μην περιέχει στοιχεία αυθεντικοποίησης ενός χρήστη αλλά στοιχεία συμμετοχής του σε κάποια ομάδα χρηστών ή πρόσθετες ιδιότητες που τον χαρακτηρίζουν, εκτός από τα βασικά δεδομένα ταυτότητάς του. Αυτές οι περιπτώσεις εμφανίζονται όταν υπάρχουν ελλιπή στοιχεία ταυτότητας των χρηστών ή δεν είναι απαραίτητη η γνώση της ταυτότητας προκειμένου να επιτραπεί η πρόσβαση του χρήστη σε μία ηλεκτρονική υπηρεσία.

- *Ασφάλεια των Web Services*: Τα *Assertions* της *SAML* μπορούν να χρησιμοποιηθούν μέσα σε μηνύματα SOAP προκειμένου να μεταδώσουν πληροφορίες πολιτικής ασφαλείας και ταυτοτήτων μεταξύ οντοτήτων που επικοινωνούν με Web Services. Ήδη αρκετές προδιαγραφές Web Services (*WS-Security* και *WS-Trust*, *Liberty Alliance's Identity Web Service Framework*) έχουν ενσωματώσει τα *SAML Assertions* ως μία από τις προτεινόμενες κατηγορίες *Security Tokens*.

Τα πλεονεκτήματα που προκύπτουν από τη χρήση της *SAML* είναι [101]:

- *Μη Εξάρτηση από Συγκεκριμένη Πλατφόρμα*: η *SAML* λειτουργεί ως ένα επίπεδο αφαίρεσης συγκεκριμένων αρχιτεκτονικών ή εμπορικών προϊόντων εξασφαλίζοντας την ανεξαρτησία της ασφάλειας από τις λεπτομέρειες των εφαρμογών που υποστηρίζει.

- *Μη Εξάρτηση από Στενές Συνδέσεις Ηλεκτρονικών Καταλόγων*: Η *SAML* δε λειτουργεί με στόχο ή προϋπόθεση ότι οι πληροφορίες των χρηστών διατηρούνται και συγχρονίζονται μεταξύ Καταλόγων των διαφορετικών οργανισμών.

- *Βελτίωση της Εμπειρίας των Χρηστών*: Με την εφαρμογή της *SAML* για την επίτευξη Web SSO και *Federated Identity Management* οι χρήστες αντιλαμβάνονται τις διαφορετικές ηλεκτρονικές υπηρεσίες διαφορετικών οργανισμών ως μία ενιαία υπηρεσία την οποία προσπελαύνουν με ενιαίο τρόπο αυθεντικοποίησης, αλλά ταυτόχρονα διατηρώντας τις ιδιαιτερότητες που πιθανώς να έχει η ταυτότητά τους σε καθεμιά υπηρεσία.

- *Μειωμένο Διαχειριστικό Κόστος*: Αυτό ισχύει για τους Παροχείς των ηλεκτρονικών υπηρεσιών (*Service Providers*) οι οποίοι μεταφέρουν το «βάρος» της αυθεντικοποίησης αλλά και της διατήρησης μεγάλων και σύνθετων καταλόγων με λογαριασμούς χρηστών στους Παροχείς Ταυτοτήτων (*Identity Providers*).

- *Μεταφορά Ευθύνης*: Η χρήση της *SAML* μεταφέρει την ευθύνη της διαχείρισης και του ελέγχου των ταυτοτήτων στον *Identity Provider* ο οποίος είναι συνήθως καταλληλότερα εξοπλισμένος γι αυτό το σκοπό, αλλά και καλύτερα ρυθμισμένος ώστε να προσεγγίζει το εφαρμοζόμενο επιχειρηματικό μοντέλο.

Η τρέχουσα έκδοση 2.0 της *SAML* ενοποιεί τα δομικά στοιχεία της διαχείρισης *Federated Identity* που υπήρχαν στη *SAML V1.1* με παρατηρήσεις και προτάσεις που προκύψαν από τα δύο σημαντικότερα projects: το "*Shibboleth*" και το "*Liberty Alliance Identity Federation Framework*", εξέλιξη η οποία ενισχύει την προσπάθεια σύγκλισης προς κοινά πρότυπα *Federated Identity Management* [101].

Περισσότερα θετικά ή αρνητικά στοιχεία της γλώσσας *SAML* προκύπτουν μέσα από τη συγκριτική αξιολόγηση των επιμέρους υλοποιήσεων ή επεκτάσεών της που παρουσιάζεται στην παράγραφο 3.2.2.

3.2 Επισκόπηση Χαρακτηριστικών των Λύσεων SSO

Από την παρουσίαση των λύσεων SSO στο Θεωρητικό μέρος προκύπτει αμέσως ο διαχωρισμός τους σε λύσεις Web SSO κατά την προσπέλαση πόρων στα πλαίσια ενός Οργανισμού και σε αυτές όπου στοχεύουν πρωτίστως στην τυποποιημένη και ασφαλή διακίνηση πληροφοριών ταυτοτήτων και ιδιοτήτων των χρηστών μεταξύ συνεργαζόμενων Οργανισμών (*Federated Identity Management*). Στη δεύτερη κατηγορία λύσεων η εξασφάλιση του Single Sing-On είναι παράπλευρη «προσφορά» τους. Η παρούσα επισκόπηση των λύσεων SSO θα ακολουθήσει τον ίδιο διαχωρισμό, ώστε να είναι ομοιόμορφη η συγκριτική παράθεση των βασικών χαρακτηριστικών τους.

3.2.1 Open - Source Λύσεις Web SSO

Από όλες τις υπάρχουσες λύσεις – πρωτόκολλα υλοποίησης Web Single Sign – On κατά την αυθεντικοποίηση χρηστών, εξετάστηκαν στις ενότητες 2.4.1 – 2.4.4 οι προτάσεις *CoSign* (University of Michigan), *CAS* (Yale University), *WebAuth* (Stanford University), *Pubcookie* (University of Washington). Η υπηρεσία Web SSO μπορεί να υλοποιηθεί με τα παραπάνω προϊόντα στα πλαίσια ενός μόνο οργανισμού, ενώ ένα από τα κριτήρια κατά την αξιολόγησή τους είναι και η δυνατότητα επέκτασης της λειτουργικότητας SSO σε συνεργασίες με άλλους οργανισμούς είτε από το ίδιο το προϊόν είτε σε συνεργασία με μία *Federated Identity Management* λύση, όπως το *Shibboleth*. Η σύγκριση των Web SSO λύσεων γίνεται κυρίως εξετάζοντας τις παραμέτρους που τις καθιστούν εύκολες και αποδοτικές σε μία επιθυμητή εγκατάσταση στα πλαίσια ενός οργανισμού.

Μία προφανής ομοιότητα των τεσσάρων λύσεων είναι η χρήση των Cookies για την υλοποίηση SSO. Γενικά, όλες οι λύσεις χρησιμοποιούν τα Cookies μόλις επιτευχθεί η αυθεντικοποίηση του χρήστη και ο κεντρικός μηχανισμός του SSO δημιουργεί ένα Cookie με πληροφορίες του χρήστη ή της σύνδεσης και το τοποθετεί στο σταθμό του χρήστη. Στην περίπτωση όπου ο

χρήστης επιθυμεί την πρόσβαση σε μία ακόμα προστατευμένη υπηρεσία, η οποία είναι είτε αυτόνομη είτε μέρος ενός portal, ο μηχανισμός SSO αναζητά το κατάλληλο Cookie στο σταθμό του χρήστη. Η μη ύπαρξη κατάλληλου Cookie ή η μη ισχύς του (λήξης ισχύος ή μη εγκυρότητα του περιεχομένου του) ενεργοποιεί την επανα-εισαγωγή των κατάλληλων «πιστοποιητικών» από τη μεριά του χρήστη ώστε να αυθεντικοποιηθεί ξανά. Στην περίπτωση όπου υπάρχει έγκυρο Cookie τότε ο κεντρικός μηχανισμός SSO επιτρέπει την πρόσβαση του χρήστη στην επιθυμητή υπηρεσία. Τα Cookies έχουν εγγενή προβλήματα ασφαλείας [150] και η μοναδική προστασία που έχει προβλεφθεί από τον ορισμό τους είναι ο περιορισμός ότι καθένα Cookie μπορεί να αναγνωσθεί μόνο από Web Applications που ανήκουν στο ίδιο *Domain* (με βάση της DNS ονομασία του) με την υπηρεσία που το δημιούργησε. Συνεπώς, ένα βασικό κριτήριο για την αξιολόγηση των SSO λύσεων είναι οι μηχανισμοί που εφαρμόζονται για την προστασία της ακεραιότητας των Cookies που χρησιμοποιούν.

Η συγκριτική παρουσίαση των λύσεων Web SSO γίνεται πάντα σε σχέση με τις προτεραιότητες και τη διαβάθμιση που θέτει η κάθε αξιολόγηση καθώς και ο υποκειμενικός σκοπός της καθεμιάς έρευνας, στην πλειοψηφία των οποίων είναι η εξέταση από ένα Πανεπιστήμιο των θετικών και αρνητικών σημείων των λύσεων ώστε να επιλεγεί μία από αυτές για το συγκεκριμένο Πανεπιστήμιο. Μία συγκριτική αντιπαράθεση των τεσσάρων προϊόντων παρουσιάζεται στην αναφορά [27] και τα συνοπτικά τους αποτελέσματα φαίνονται στον παρακάτω πίνακα.

Πηγή: [27]

	Usage	Single point of failure	Support	Docum-entation	Availability of connector modules	Shibboleth enabled
CAS	Moderate	Yes	Poor	Poor	V poor	No
Pubcookie	Widely used		Variable	Small amount	Variable	Projected
WebAuth	Not widely used	No	Responsive	V good	Poor	No
Cosign	Relatively new	No	V responsive	Small	Good	Has been demonstrated

Εικόνα 51: Γενική Σύγκριση Χαρακτηριστικών Web SSO Λύσεων

Από τον παραπάνω πίνακα προκύπτει ότι παρόλες τις πολλές ομοιότητες των μηχανισμών SSO υπάρχουν πεδία στα οποία η απόδοσή τους μπορεί να διαφέρει και να επηρεάσουν την συνολική τους αξιολόγηση:

- Την εποχή κατά την οποία διεξήχθη η συγκεκριμένη συγκριτική ανάλυση (2004) το πιο διαδεδομένο προϊόν σε εγκαταστάσεις ήταν το *Pubcookie* (ενδεικτικά: Πανεπιστήμια Washington, CMU, Wisconsin, UFL, Newcastle κ.α.) με επόμενο το *CAS* (ενδεικτικά: Πανεπιστήμια Yale, Indiana, Princeton, Bristol κ.α.). Τα προϊόντα *WebAuth* και *CoSign* χαρακτηρίζονται ως μειωμένης διάδοσης.

- Ένα από τα εξεταζόμενα χαρακτηριστικά είναι η ύπαρξη μοναδικού σημείου αποτυχίας του μηχανισμού SSO (*Single Point of Failure*), αν δηλαδή το πρωτόκολλο μπορεί να καταρρεύσει από την εμφάνιση ενός μόνο λάθους. Η αντίθετη κατάσταση είναι ένα σύστημα στο οποίο έχουν προβλεφθεί σχεδόν όλες οι πιθανότητες λάθους και έχουν επιλεγεί εναλλακτικές λειτουργίες ομαλής συνέχισης ή κλεισίματός του. Συνεπώς, οι λύσεις *WebAuth* και *Cosign* είναι περισσότερο αξιόπιστες καθώς παρέχουν περισσότερη προβλεπτικότητα και εναλλακτικούς τρόπους αντιμετώπισης προβλημάτων του πρωτοκόλλου, ενώ το *CAS* είναι λιγότερο αξιόπιστο. Το *PubCookie* βρίσκεται σε φάση εξέλιξης της ανεκτικότητάς του σε περιπτώσεις κατάρρευσης του μηχανισμού του από ένα μοναδικό σφάλμα.

- Στους τομείς της υποστήριξης (*Support*) και της τεκμηρίωσης (*Documentation*) προκειμένου να υλοποιηθούν οι συγκεκριμένες λύσεις σε τρίτους οργανισμούς, το *WebAuth* υπερτερεί των υπολοίπων, με τα *Cosign* και *Pubcookie* να ακολουθούν. Το *CAS* και σε αυτή την κατηγορία βαθμολογήθηκε αρνητικά.

- Οι δύο τελευταίες κατηγορίες αφορούν την ευκολία διασύνδεσης των μηχανισμών SSO με υπάρχοντα στον οργανισμό υπο-συστήματα αυθεντικοποίησης ή Web Servers. Ειδική έμφαση δίνεται στην τελευταία κατηγορία, στην ευκολία διασύνδεσής τους με τη λύση *Federated Identity Shibboleth*. Το *Cosign* αποδεικνύεται καλύτερο σε αυτά τα πεδία καθώς έχει ευκολότερη διασύνδεση με τα υπόλοιπα εξαρτώμενα υπο-συστήματα και υπάρχει τουλάχιστον πιλοτική σύνδεση με το *Shibboleth*. Στην αξιολόγηση ακολουθεί το *Pubcookie*, το *WebAuth* και το *CAS*.

Μία ακόμα αναλυτική σύγκριση λύσεων Web SSO παρουσιάζεται στην αναφορά [13] η οποία όμως δεν περιλαμβάνει το *Pubcookie*. Η ανάλυση θέτει συγκεκριμένες απαιτήσεις οι οποίες πρέπει να ικανοποιούνται από τις Web SSO λύσεις:

- Ασφαλή μετάδοση των «πιστοποιητικών» των χρηστών (*Secure Communication of user credentials*).

- Τα προσωρινά αποθηκευμένα «πιστοποιητικά» να μην περιέχουν προσωπικά στοιχεία (*Cached credentials do not contain user data*).

- Τα προσωρινά αποθηκευμένα «πιστοποιητικά» να μην μπορούν εύκολα να επαναπροωθηθούν στο μηχανισμό (*Cached credentials not easily re-playable*).

- Ύπαρξη επιλογής «Αποσύνδεσης» στο χρήστη (*User has a logout facility*).

- Τα προσωρινά αποθηκευμένα «πιστοποιητικά» να έχουν συγκεκριμένο χρόνο ισχύος (*Timeout on cached credentials*).

- Ύπαρξη καλής καταγραφής συμβάντων κατά τη διαδικασία της αυθεντικοποίησης (*Good logging on the authentication service*)

- Υποστήριξη του Microsoft IIS και του Apache 1.3 (*Support for Microsoft's IIS and Apache 1.3*)

Επιπροσθέτως των παραπάνω απαιτήσεων, η ανάλυση προτείνει κάποιους βασικούς παράγοντες αξιολόγησης οι οποίοι επίσης πρέπει να ληφθούν υπόψη:

- *Προσαρμοστικότητα (Resilience)*: η ικανότητα του μηχανισμού Web SSO να παρέχει υπηρεσία ακόμα και αν ένα ή περισσότερα μέρη του έχουν αποτύχει. Σχετίζεται με το κριτήριο "*Single Point of Failure*" της προηγούμενης αξιολόγησης.

- *Αποδοτικότητα (Efficiency)*: η ικανότητα εκτέλεσης του συγκεκριμένου έργου με την κατανάλωση των λιγότερων πόρων.

- *Ανθεκτικότητα (Robustness)*: η ικανότητα αντιμετώπισης λαθών με απόλυτο και ενιαία τρόπο.

- *Παραγωγικότητα (Throughput)*: Η ικανότητα εξυπηρέτησης μεγαλύτερου αριθμού συναλλαγών στο μικρότερο χρονικό διάστημα.

- *Συνολικό Κόστος Κτήσης (Total Cost of Ownership)*: είναι το κόστος εγκατάστασης, υποστήριξης και συντήρησης της λύσης και όλης της υποστηρικτικής υποδομής.

- *Κλιμάκωση (Scalability)*: η ικανότητα του μηχανισμού να χρησιμοποιήσει με τις λιγότερες επεμβάσεις περισσότερους πόρους ώστε να ικανοποιεί μεγαλύτερο αριθμό συναλλαγών.

- *Υποστήριξη (Supportability)*: η δυνατότητα εύκολης υποστήριξης της λύσης όταν εγκατασταθεί σε παραγωγικό περιβάλλον.

- *Συντήρηση (Maintainability)*: η δυνατότητα εύκολης αναβάθμισης, εγκατάστασης πρόσθετων τμημάτων λογισμικού, επιδιορθώσεων λαθών μετά την εκκίνηση της παραγωγικής λειτουργίας.

Παρατίθενται, επίσης και συγκεκριμένα επιθυμητά χαρακτηριστικά τα οποία θα ήταν καλό να διαθέτουν οι λύσεις Web SSO:

- Να δίνεται η δυνατότητα στην Web Application που βρίσκεται πίσω από τη λύση Web SSO να καταργήσει τη δυνατότητα SSO και να επιβάλλει ξανά αυθεντικοποίηση του χρήστη (*Web Application has ability to refuse SSO and force re-auth*).

- Δυνατότητα καταγραφής της IP διεύθυνσης του χρήστη κατά την αυθεντικοποίηση (*Web server allows central auth to log the originating IP address during verification*).

- Δυνατότητα ανίχνευσης και ελαχιστοποίησης επιθέσεων σε οποιεσδήποτε φάσεις του μηχανισμού (*Detection and minimisation of brute force attacks*).

- Υποστήριξη του Apache 2.0 (*Support for Apache 2.0*).

Στο καθένα από τα παραπάνω κριτήρια αποδόθηκε ένα «βάρος» σημαντικότητας ώστε να προκύψει μία μετρήσιμη βαθμολογία και κατ' επέκταση αξιολόγηση. Με βάση, επομένως, τους παραπάνω παράγοντες και τα στοιχεία των λύσεων Web SSO προέκυψαν οι «κατατάξεις» του παρακάτω πίνακα, όπου για καθένα κριτήριο αναγράφεται η σειρά κατάταξης των τριών λύσεων ανάλογα με το βαθμό ικανοποίησής του:

Πηγή: [13]

Factor	Importance	Implementation Ranking		
		CAS	WebAuth	CoSign
Ciritical Requirements	***High***			
Secure communication of credentials	High	1	1	1
Cached credentials not easily re-playable	High	1	1	1
Timeout on cached credentials	High	3	1	1
Microsoft IIS and Apache 1.3 support	High	2	3	1
Cached credentials do not contain user/session data	Medium	1	3	1
User logout facility	Medium	1	1	1
Good logging on authentication service	Medium	2	1	2
		3	**2**	**1**
Considerations	***High***			
Resilience	High	2	3	1
Robustness	High	1	1	3
Throughput	High	3	1	1
Efficiency	Medium	1	1	1
Total Cost of Ownership	Medium	1	3	1
Scalability	Medium	1	1	1
Supportability	Medium	1	2	1
Maintainability	Medium	1	1	1
		2	**3**	**1**
Desired Features	***Medium***			
Ability to refuse SSO based on security rating		Partial	Partial	No
Can centrally log originating IP on verification		No	No	No
Minisation and detection of brute forse attacks		No	No	No
Apache 2.0 Support		Yes	No	Yes
		1	**3**	**2**
Additional Features/Problems	***Low***	2	3	1
Overall Ranking		**2**	**3**	**1**

Εικόνα 52: Συγκριτική Κατάταξη – Αξιολόγηση Web SSO Λύσεων

Στην ενότητα των σημαντικών απαιτήσεων (*Critical Requirements*) το *Cosign* αναδεικνύεται καλύτερο με βέλτιστη ικανοποίηση σχεδόν κάθε κριτηρίου:

- Τα Cookies στέλνονται μέσω το πρωτοκόλλου HTTPS (*Secure Communication of user credentials*).
- Τα πιστοποιητικά του χρήστη δεν είναι εύκολο να επανα-χρησιμοποιηθούν από κάποιον τρίτο παράγοντα υπό την προϋπόθεση ότι ο *Cosign Authentication Server* βρίσκεται σε διαφορετικό υπολογιστή από την προστατευόμενη Web Application. (*Cached credentials not easily re-playable*).
- Το *Authentication Cookie* έχει δύο διαφορετικούς χρόνους ισχύος για μεγαλύτερη εξασφάλιση (*Timeout on cached credentials*).
- Υποστηρίζονται και τα δύο προϊόντα Microsoft's IIS and Apache 1.3 (*Support for Microsoft's IIS and Apache 1.3*).

- Τα Cookies περιέχουν μόνο session keys τα οποία αντιστοιχίζονται μέσα στην εφαρμογή σε στοιχεία χρηστών (*Cached credentials do not contain user data*).

- Ο χρήστης μπορεί να «αποσυνδεθεί» από την υπηρεσία με ταυτόχρονη καταστροφή των στοιχείων που έχουν προκύψει από την πρόσφατη διαδικασία SSO (*User has a logout facility*).

- Η μόνη αδυναμία του *Cosign* σε αυτή την κατηγορία κριτηρίων είναι η ελλιπής καταγραφή κατά τη διαδικασία αυθεντικοποίηση (*Logging on the authentication service*).

Στην ενότητα των χαρακτηριστικών υπό αξιολόγηση (*Considerations*) το *Cosign* αναδεικνύεται πάλι καλύτερο με ικανοποιητική κάλυψη όλων σχεδόν των χαρακτηριστικών, τα σημαντικότερα από τα οποία είναι

- Εφόσον τηρηθεί η συνιστώμενη βέλτιστη αρχιτεκτονική και χρησιμοποιηθεί το χαρακτηριστικό του *Replication* του *Cosign* server τότε το χαρακτηριστικό *Resilience* καλύπτεται με επάρκεια.

- Στο χαρακτηριστικό *Efficiency* υπάρχει καλή συμπεριφορά του *Cosign* με την παρατήρηση ότι υπάρχει περίπτωση να μειωθεί η αποδοτικότητα της λύσης σε υψηλό φόρτο, επειδή όλα τα *Authentication cookies* και τα *Service cookies* αποθηκεύονται ως αρχεία στο δίσκο του χρήστη.

- Η απόδοσή του (*Throughput*) φαίνεται πολύ καλή, ενδεικτικά στο Παν/μιο του Michigan υπάρχει εγκατάσταση *Cosign* σε τρεις dual 2.8Ghz servers με 4GB RAM οι οποίοι εξυπηρετούν περίπου 255.000 εγγραφές *ST* και 180.000 αιτήσεις αυθεντικοποίησης την ημέρα.

- Το κόστος κτήσης του είναι σχετικά μικρό, καθώς παρόλες τις τροποποιήσεις που απαιτούνται στον πηγαίο κώδικά του κατά τη φάση της εγκατάστασής του, η μετέπειτα υποστήριξή του θεωρείται απλούστερη.

- Η ικανότητα *Scalability* μπορεί να εξασφαλιστεί καθώς υπάρχει η δυνατότητα *Replication* υπο-συστημάτων του *Cosign* σε άλλα συστήματα που έχουν εγκατεστημένη την ίδια υπηρεσία, αλλά μπορεί να περιοριστεί από το φυσικό όριο που θέτουν τα Λειτουργικά Συστήματα των χρηστών στην ποσότητα Cookies που μπορούν να αποθηκευτούν ταυτόχρονα στο δίσκο τους.

- Η δυνατότητα υποστήριξης της εγκατάστασης του *Cosign* κινείται στα επίπεδα των υπολοίπων λύσεων, χωρίς ιδιαίτερη καταγραφή συμβάντων που θα μπορούσε να είναι χρήσιμη και χωρίς ιδιαίτερα διαχειριστικά εργαλεία για το αντίστοιχο προσωπικό. Για την προγραμματιστική υποστήριξη, όμως, υπάρχει μία σχετικά μικρή, αλλά αρκετά δυναμική κοινότητα υποστήριξης του πηγαίου κώδικα του *Cosign*.

Από τις δύο παραπάνω αναλύσεις είναι χαρακτηριστική η χαμηλή αξιολόγηση του *WebAuth*. Οι λόγοι γι αυτό το φαινόμενο είναι:

- Η σχεδιαστική φιλοσοφία του *WebAuth* επιβάλλει όλα τα δεδομένα κατάστασης του χρήστη να αποθηκεύονται σε κρυπτογραφημένα Cookies στο σταθμό του. Με αυτό τον τρόπο επιτυγχάνεται μείωση της πολυπλοκότητας του κεντρικού "*daemon*" και αυξημένη δυνα-

τότητα κλιμάκωσης (*scalability*) σε περιπτώσεις μεγάλου φόρτου, προκύπτουν όμως πολλά θέματα σε σχέση με την ασφάλεια του μοντέλου. Τα Cookies που αποθηκεύονται στην πλευρά του χρήστη στο *WebAuth* περιέχουν πληροφορίες του χρήστη, οι οποίες είναι μεν κρυπτογραφημένες, αλλά η ασφαλείας τους δεν μπορεί να εξασφαλιστεί περαιτέρω, δεδομένων και των «επιθέσεων» που δέχονται συνεχώς οι σταθμοί των χρηστών του Internet. Στις υπόλοιπες λύσεις τα Cookies στην πλευρά του χρήστη, τα οποία είναι επίσης ευάλωτα σε επιθέσεις, περιέχουν μόνο τυχαίους κωδικούς που αφορούν το session του χρήστη και όχι αυτούσιες πληροφορίες γι αυτόν. Επιπροσθέτως, αν επιτευχθεί η λύση της κρυπτογράφησης των Cookies τότε είναι δυνατή η πρόσβαση στα κλειδιά κρυπτογραφημένης επικοινωνίας με τον *WebKDC* ο οποίος διατηρεί όλα τα *authentication tokens* της εγκατάστασης [13].

- Δεν υπάρχει υποστήριξη του Web Server Microsoft IIS [132].

- Δεν υπάρχει υποστήριξη ενιαίας αποσύνδεσης από ένα μόνο σημείο του Web Site. Αυτό οφείλεται στο μοντέλου λειτουργίας του *WebAuth*, όπου όλες οι πληροφορίες κατάστασης των συνδέσεων των χρηστών αποθηκεύονται σε Cookies στους σταθμούς των χρηστών και όχι σε ένα κεντρικό σύστημα. Με αυτό τον τρόπο όμως δεν είναι δυνατή η ολική αποσύνδεση του χρήστη από όσα προστατευόμενα Web Sites έχει επισκεφτεί, οπότε συστήνεται είτε το κλείσιμο του Browser είτε η σταδιακή αποσύνδεση από καθένα Web Site ξεχωριστά [132].

- Το συνολικό κόστος κτήσης θεωρείται πιθανώς υψηλό καθώς, ενώ το τεκμηριωτικό υλικό είναι ομόφωνα πολύ καλό, δεν υπάρχει αρκετή υποστήριξη για την ανάπτυξη Client τμημάτων εφαρμογών που πρόκειται να προστατεύουν από το *WebAuth*. Επιπροσθέτως, η γλώσσα Perl, στην οποία έχει αναπτυχθεί, μπορεί να έχει θετική απόδοση αλλά η υποστήριξή της μπορεί να είναι πιο δαπανηρή από αυτή της Java [13, 27].

Σχετικά με τη λύση *CAS* υπάρχει μία μάλλον μέτρια αντιμετώπιση σε σχέση με απόπειρες αξιολόγησής της:

- Υπάρχει μία γενική ομοφωνία ότι είναι η ιδανικότερη λύση για περιβάλλοντα όπου λειτουργούν αποκλειστικά τεχνολογίες της Java. Το γεγονός αυτό αποτελεί ταυτόχρονα και μειονέκτημα, καθώς η ανάπτυξη του *CAS* συνδέεται τόσο πολύ με την Java όπου καθίσταται δύσκολη η υποστήριξη εφαρμογών οι οποίες δεν έχουν γραφεί σε Java και επίσης είναι σχεδόν υποχρεωτική η εγκατάσταση Application Servers τεχνολογίας Java (J2EE) οι οποίοι μπορεί να αυξήσουν το κόστος εγκατάστασης του *CAS* [13, 132].

- Τα Cookies που αποθηκεύονται στο σταθμό του χρήστη δεν διατηρούν προσωπικά στοιχεία παρά μόνο έναν κωδικό που αντιστοιχεί στη σύνδεσή του. Επιπροσθέτως, τα *Service Tickets* που λαμβάνουν οι Web Applications για την αυθεντικοποίηση του καθένα χρήστη χρησιμοποιούνται μία φορά για καθένα χρήστη και μετά «καταστρέφονται». Με αυτό τον τρόπο δεν είναι απαραίτητη η διατήρησή τους σε κάποιο Cookie, άρα αυξάνεται η ασφάλεια του μηχανισμού SSO [3].

- Ένα σημαντικό πλεονέκτημα του *CAS* είναι η υποστήριξη επέκτασης της αυθεντικοποίησης σε ένα περαιτέρω επίπεδο από το κλασικό: Χρήστης ↔Web Application στο σχήμα: Χρήστης ↔Web Application ↔Back – End Application (*Authentication Proxying*) [3].

- Ένα βασικό μειονέκτημα του *CAS* το οποίο φαίνεται να εμφανίζεται συχνά στις αξιολογήσεις των λύσεων SSO είναι η ανεπαρκής τεκμηρίωση και υποστήριξη για την αναλυτική κατανόηση και εγκατάσταση του μηχανισμού σε έναν οργανισμό [13, 27].

3.2.2 Λύσεις *Federated Identity Management*

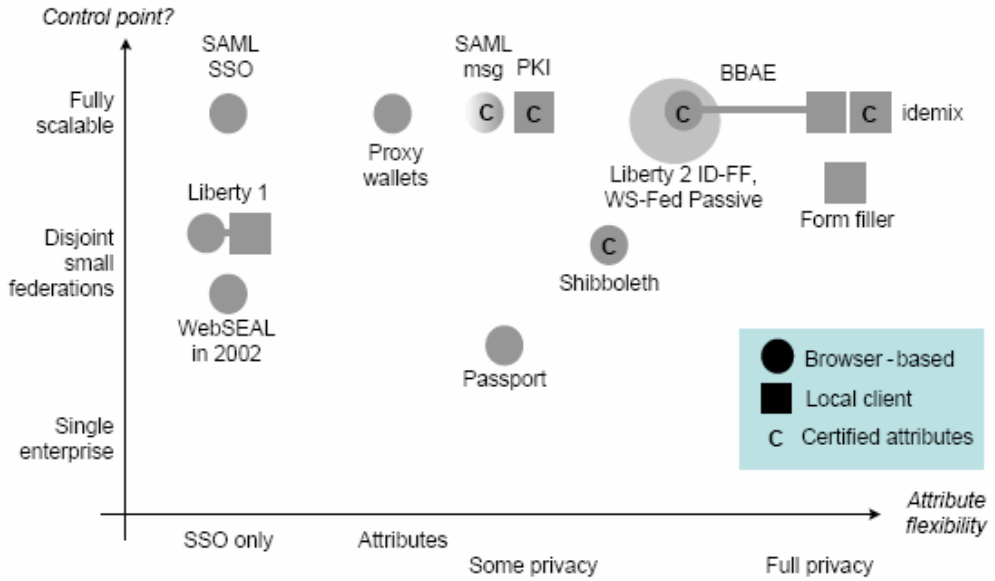
3.2.2.1 Γενικά

Τα πρωτόκολλα *Federated* διαχείρισης ταυτοτήτων (*Federated Identity Management*) τα οποία εξετάστηκαν στις ενότητες 2.4.5 & 2.4.6 (*WS-Federation*, *Liberty – Alliance ID-FF*, *Shibboleth*) αποτελούν την εξέλιξη των πρωτοκόλλων αυθεντικοποίησης και η πρόοδός τους οδηγείται από τις ανάγκες επιχειρηματικής (e-Business) και κυβερνητικής (e-Government) αξιοποίησης του Internet. Ο βασικός στόχος των επιχειρήσεων και των κρατικών φορέων που προσφέρουν υπηρεσίες στο Internet είναι η απλοποίηση των διαδικασιών εισόδου των χρηστών και διαχείριση των ταυτοτήτων τους, έτσι ώστε οι υπάλληλοι συνεργαζόμενων επιχειρήσεων μίας Εφοδιαστικής Αλυσίδας, για παράδειγμα, να έχουν απλή και ομοιόμορφη διαδικασία αυθεντικοποίησης στις υπηρεσίες διαχείρισης της Αλυσίδας, οι οποίες μπορεί να είναι εγκατεστημένες στις διαφορετικές επιχειρήσεις. Από τη μεριά των πρωτοκόλλων, η πρώτιστη απαίτηση είναι να μπορούν να λειτουργήσουν με την προϋπόθεση ότι ο χρήστης διαθέτει μόνο έναν απλό Browser για να προσπελαύνει τις διαδικτυακές υπηρεσίες και δεν μπορεί να υποτεθεί ότι υπάρχει ή θα εγκατασταθεί κάποιο client λογισμικό στο σταθμό του χρήστη για την υποστήριξη του κάθε πρωτοκόλλου. Τα πρωτόκολλα, επομένως, είναι αποκλειστικά βασισμένα στον Browser (*Browser – based*) και παράλληλα πρέπει να ολοκληρώνουν τη βασική τους λειτουργία ακόμα και αν έχει απενεργοποιηθεί από την πλευρά του χρήστη η υποστήριξη «Ενεργού Περιεχομένου» ("*Active Content*") και των Cookies. Τα συγκριμένα πρωτόκολλα, συνεπώς, πρέπει να διεξάγουν τις ενέργειές τους εκμεταλλευόμενα μόνο το HTTP πρωτόκολλο, τις ανακατευθύνσεις του (*Redirects*) και την «ασφαλή» επέκτασή του, το HTTPS.

Με βάση τις παραπάνω απαιτήσεις έχουν διατυπωθεί τρεις βασικές *Browser – based* λύσεις για *Federated Identity Management*: *Shibboleth*, *Liberty – Alliance ID – FF*, *WS-Federation Passive Requestor*, τα βασικά χαρακτηριστικά των οποίων παρουσιάστηκαν στην ενότητα 2. Από την εξέταση των βασικών λειτουργιών που παρέχουν σε σχέση με τις βασικές απαιτήσεις της έννοιας του *Identity Federation* οι συγκεκριμένες προδιαγραφές μπορούν να θεωρηθούν ισότιμες. Οι κεντρικές τους διαφορές εντοπίζονται στα κίνητρα και το υπόβαθρο της δημιουργίας τους. Συνεπώς, το *WS-Federation* είναι προϊόν της συνεργασίας ορισμένων μεγάλων εταιριών του χώρου (Microsoft, IBM, RSA κλπ) και αποτελεί μέρος μία ευρύτερης πρότασης προδιαγραφών για Web Services, της προδιαγραφής WS-*, με αποτέλεσμα η ανάπτυξη του *WS-Federation* να γίνεται κλιμακωτά, πάνω από τις γενικότερες προδιαγραφές ασφαλείας της οικογένειας WS-*. Παρόμοια φιλοσοφία παρουσιάζει και το *Liberty – Alliance Project* το οποίο μέσα από τη συνεργασία πολλών εταιριών του χώρου επιδιώκει τη διατύπωση ενός συνόλου προδιαγραφών που καλύπτουν πολλές πτυχές της διαχείρισης πληροφοριών ταυτοτήτων στο Internet. Η λύση *Liberty – Alliance ID – FF* είναι βασισμένη στη *SAML* αλλά αποτελεί μέρος ενός γενικότερου πλαισίου προτάσεων του *Liberty – Alliance Project* για την ενίσχυση της επιχειρηματικής αξιοποίησης των διαδικτυακών υπηρεσιών. Το *Shibboleth*, όμως, θεωρείται μία προσεγμένη επέκταση της *SAML* και μία υλοποίησή της στη διαμοίραση πόρων μεταξύ ακαδημαϊκών ιδρυμάτων, η οποία έχει πια φτάσει σε επίπεδο ωρίμανσης ώστε να χρησιμοποιηθεί και σε πολλές άλλες περιπτώσεις «έμπιστων» οργανισμών [30].

Ένα ευρύτερο σύνολο πρωτοκόλλων και σχετικών μηχανισμών φαίνονται στο παρακάτω διάγραμμα σε μία προσπάθεια συγκέντρωσης και σύγκρισής τους από το [114].

Πηγή: [114]



Εικόνα 53: Επισκόπηση *Browser – Based* Πρωτοκόλλων *Identity Federation* και Σχετικών Τεχνικών

Στον κάθετο άξονα αναπαρίσταται ο βαθμός εξάρτησης του πρωτοκόλλου από ένα μοναδικό σημείο ελέγχου (*Control Point*) όπου διεξάγεται ο έλεγχος ταυτότητας χρήστη. Η κλίμακα ξεκινάει από μία λύση κατάλληλη για μία μοναδική επιχείρηση (*Single Enterprise*), όπου το σημείο ελέγχου είναι μία σταθερή διεύθυνση στο εσωτερικό δίκτυο της επιχείρησης. Η ενδιάμεση κατάσταση αντιστοιχεί στην κάλυψη των αναγκών μικρών επιχειρηματικών συμπράξεων (*Federations*), όπου μπορεί να υπάρχει προ-εγκατεστημένη «εμπιστοσύνη» μεταξύ των μερών της σύμπραξης και δεν απαιτείται η επίδειξη πιστοποιητικών εμπιστοσύνης σε κάθε συναλλαγή. Το πάνω άκρο του κατακόρυφου άξονα αντιστοιχεί σε μία πλήρως προσαρμοζόμενη λύση που μπορεί να ικανοποιήσει διάφορα σενάρια σύναψης και διακοπής «έμπιστων» σχέσεων μεταξύ επιχειρήσεων, οπότε η εμπιστοσύνη πρέπει κάθε φορά να αποδεικνύεται με τα αντίστοιχα πιστοποιητικά.

Στον οριζόντιο άξονα αναπαρίσταται η ικανότητα του κάθε πρωτοκόλλου στη μετάδοση πρόσθετων ιδιοτήτων για πολλαπλούς χρήστες (*Attribute Flexibility*) ή το πρωτόκολλο απλώς εξασφαλίζει authentication και Single Sign-On. Στο συγκεκριμένο άξονα αναπαρίσταται και η έννοια της «μυστικότητας» (privacy), δηλαδή της δυνατότητας ελεγχόμενης αποστολής πληροφοριών των χρηστών βάσει συγκεκριμένων πολιτικών ασφαλείας. Υπάρχει, επομένως, διαβάθμιση μεταξύ των πρωτοκόλλων για το αν αποστέλλουν συγκεκριμένες πληροφορίες χρηστών ή μπορούν να ακολουθήσουν πολιτικές που καθορίζουν δυναμικά ποιες πληροφορίες και υπό ποιες συνθήκες μπορούν να αποσταλούν.

Τα πρωτόκολλα που συγκρίνονται στο [114] είναι τα προαναφερθέντα: *SAML*, *Shibboleth*, *Liberty-Alliance*, *WS-Federation Passive Requestor*, ενώ προστίθενται και μία πρόταση των

συγγραφέων για ένα αντίστοιχο πρωτόκολλο, το BBAE, και άλλα σχετικά εμπορικά προϊόντα ή σχετικοί μηχανισμοί. Στο διάγραμμα εμφανίζεται και το *Microsoft Passport*[xvi] το οποίο δεν έχει τεκμηριωθεί ως πρότυπο, λειτουργεί όμως ως μηχανισμός αυθεντικοποίησης και SSO για συγκεκριμένες διαδικτυακές υπηρεσίες όπου συμμετέχει η Microsoft. Το προϊόν *WebSEAL* είναι μία πρόταση της IBM [46], όπως και το *IDEMIX* το οποίο αφορά τη διαχείριση ψευδώνυμων και τις περιπτώσεις όπου δεν μπορούν να συνδυαστούν οι ταυτότητες - ψευδώνυμα χρήστη μεταξύ δύο οργανισμών [11]. Τα υπόλοιπα τετράγωνα στοιχεία του διαγράμματος αντιστοιχούν σε σχετικούς μηχανισμούς που όμως δεν είναι *Browser – Based* και εξυπηρετούν τις ανάγκες της σύγκρισης.

Από το διάγραμμα, επομένως, του [114] προκύπτει ότι γενικά από τις προαναφερθείσες λύσεις *Browser – Based* αυτές που πλησιάζουν την ικανοποίηση απαιτήσεων του πλήρους *Federated Identity Management* είναι οι *Liberty – Alliance 2 ID-FF* και *WS-Federation Passive Requestor*. Αυτό σημαίνει ότι οι συγκεκριμένες λύσεις μπορούν να υλοποιήσουν σενάρια αυξομειωμένων «αλυσίδων» εμπιστοσύνης όπου οι συμμετέχουσες επιχειρήσεις της «αλυσίδας» είναι αρκετές στο πλήθος και μπορούν να εισέρχονται και να απομακρύνονται από την «αλυσίδα» με δυναμικό τρόπο. Παράλληλα, στις υπηρεσιών των συγκεκριμένων επιχειρήσεων μπορούν να εφαρμοστούν SSO και πολιτικές ασφαλείας για την ανταλλαγή πληροφοριών των χρηστών. Ένα επίπεδο πιο κάτω και στους δύο άξονες τοποθετείται η λύση *Shibboleth*, η οποία σχεδιάστηκε για την ενοποιημένη πρόσβαση σε πόρους ακαδημαϊκών ιδρυμάτων με πιο συγκεκριμένους και περιορισμένους στην ακαδημαϊκή κοινότητα αρχικούς στόχους και κίνητρα.

Η διαφορά των *Liberty – Alliance 2 ID-FF* και του *Shibboleth* σε ότι αφορά τη διατύπωση πολιτικών διαχείρισης των προϋποθέσεων μετάδοσης των ιδιοτήτων (*attributes*) των χρηστών διατυπώνεται και στο [36]. Η δυνατότητα, δηλαδή, μετάδοσης πρόσθετων ιδιοτήτων ενός χρήστη υποστηρίζεται και από τα δύο πρότυπα με την απαραίτητη εφαρμογή συγκεκριμένων ελέγχων ώστε να ρυθμίζεται αυτή η εξαγωγή πληροφοριών χρήστη ανάλογα με το πόσο εμπιστευτικές είναι οι ζητούμενες πληροφορίες, από ποιον ζητούνται κλπ. Το *Shibboleth* υποστηρίζει το συγκεκριμένο μηχανισμό αλλά η ακριβής διατύπωση των παραπάνω ελέγχων πρόσβασης είναι ανοιχτή για κάθε υλοποίησή του και δεν προδιαγράφεται σαφώς, ενώ το *Liberty-Alliance ID-FF* καθορίζει μία πρότυπη μέθοδο ορισμού πολιτικών ελέγχου της «δημοσιοποίησης» ιδιοτήτων χρήστη με τη χρήση XML. Σε σχέση, όμως, με τη νομική παράμετρο του προβλήματος, όλα τα πρότυπα απαιτούν ως απαραίτητη προϋπόθεση τη σωστή συγκρότηση των συνεργασιών «εμπιστοσύνης» μεταξύ των οργανισμών που αποτελούν ένα *Federation* ώστε οι χρήστες να είναι ενήμεροι ότι τα δεδομένα τους ενδεχομένως να μεταδίδονται σε συνεργαζόμενους με τον δικό τους οργανισμούς. Επίσης όταν λαμβάνει χώρα μία τέτοια μετάδοση πρέπει να αναζητείται από το πρωτόκολλο η συγκατάθεση των χρηστών.

Μία ακόμα διαφορά των παραπάνω προδιαγραφών, η οποία εντοπίζεται και στο [36], είναι η δυνατότητα του *Liberty – Alliance ID – FF* να αντιστοιχεί προσωρινούς κωδικούς σε υπαρκτούς λογαριασμούς χρηστών και να αναφέρεται σε αυτούς χωρίς την αναφορά σε στοιχεία των χρηστών (*Account Federation*). Ο προσωρινός κωδικός ουσιαστικά συνδέει τους πραγματικούς λογαριασμούς του ίδιου χρήστη σε διαφορετικούς *IdP* έτσι ώστε να είναι δυνατή η πρόσβαση στους λογαριασμούς του ίδιου χρήστη χωρίς την ανταλλαγή πραγματικών πληροφοριών του. Το συγκεκριμένο χαρακτηριστικό δεν υπάρχει στο *Shibboleth* ενώ στο *WS-Federation* εξασφαλίζεται μέσω της υπηρεσίας των ψευδωνύμων (*Pseudonym Service*) [4, 8].

[xvi] Η συγκεκριμένη υπηρεσία ονομάζεται πια "*Windows Live ID*"

3.2.2.2 Ασφάλεια

Η έννοια της ασφάλειας περιλαμβάνει τον καθορισμό από την πλευρά των πρωτοκόλλων μηχανισμών αποτροπής όλων των κινδύνων που απειλούν τη διαδικασία αυθεντικοποίησης και περιγράφονται στην παράγραφο 2.1.2. Επιπροσθέτως, είναι ιδιαίτερα σημαντική η παράμετρος της ακεραιότητας των μεταδιδόμενων πληροφοριών και ειδικότερα των πληροφοριών ταυτότητας των χρηστών. Οι τρεις προδιαγραφές (*WS-Federation*, *Liberty – Alliance ID-FF*, *Shibboleth*) στα τεχνικά τους κείμενα ασχολούνται με την επίλυση θεμάτων αυθεντικοποίησης χρηστών και μεταβίβασης πληροφοριών ταυτοτήτων τους και δίνουν μόνο κατευθύνσεις για τις επιμέρους υλοποιήσεις των συγκεκριμένων προδιαγραφών για να εξασφαλίσουν την ασφάλεια ή ακεραιότητα των μεταδιδόμενων δεδομένων, ανάλογα με το περιβάλλον εφαρμογής τους. Για την επίτευξη αυτού του σκοπού αναλύουν όλες τις απειλές σε συγκεκριμένα σημεία της λειτουργίας τους και προτείνουν τρόπους αντιμετώπισής τους μέσα από τις υφιστάμενες, διαδεδομένες μεθόδους ασφαλείας: το *WS-Federation* παραπέμπει σε όλες τις μεθόδους ασφαλούς διακίνησης μηνυμάτων του *WS-Security*, τα *Liberty – Alliance ID – FF* και *Shibboleth* βασίζονται στις μεθόδους ασφαλείας της *SAML*, η οποία με τη σειρά της βασίζεται στο «ασφαλές» HTTP ή τις προδιαγραφές της «ασφαλούς» XML [8, 102]. Υπάρχει, όμως και ο αντίλογος στη συγκεκριμένη πρακτική των προδιαγραφών και ειδικότερα στο [29] θεωρείται ότι η απαρίθμηση γνωστών «επιθέσεων ασφαλείας» και η πρόταση μέτρων αντιμετώπισής τους από τα πρωτόκολλα δεν αποτελεί απόδειξη εξασφάλισης ασφαλούς λειτουργίας, γιατί δεν περιλαμβάνονται σενάρια «απειλών» εκτός των ευρέως γνωστών. Προστίθεται, επίσης, ότι όλες αυτές οι προδιαγραφές συνοδεύονται από αρνητικές μελέτες ασφάλειας και περιλαμβάνουν πολλά τρωτά σημεία.

Γενικά, οι τρεις προδιαγραφές λειτουργούν μέσω του Browser του χρήστη, άρα η κεντρική επιλογή εξασφάλισής τους είναι η εφαρμογή του πρωτοκόλλου HTTPS κατά τη μετάδοση των ευαίσθητων πληροφοριών ταυτότητας χρηστών. Στις περιπτώσεις όπου είναι επιθυμητή η ακεραιότητα των δεδομένων, τότε μπορεί να εφαρμοστεί η λύση της ψηφιακής υπογραφής στα μηνύματα με βάση την προδιαγραφή *XML Signature* [4 (ενδεικτικά)].

Ειδική περίπτωση στο θέμα της ασφάλειας αποτελούν τα Cookies. Όλα τα εξεταζόμενα πρωτόκολλα τα χρησιμοποιούν προαιρετικά για την προσωρινή αποθήκευση στο σταθμό εργασίας του χρήστη σύντομων πληροφοριών που επιταχύνουν τη ροή των πρωτοκόλλων τους. Η βασική τους χρήση και στις τρεις προδιαγραφές είναι η αποθήκευση του *Identity Provider* (*IdP*) που μπορεί να αυθεντικοποιήσει τον τρέχοντα χρήστη, στις περιπτώσεις όπου υπάρχουν πολλοί πιθανοί *Identity Providers*. Στο *WS-Federation* δεν καθορίζεται ακριβώς πως προσδιορίζεται ο επιθυμητός *IdP* αλλά υπάρχει η επιλογή δημιουργίας Cookie με κρυπτογραφημένο περιεχόμενο. Στο *Shibboleth* προβλέπεται μία αυτόνομη υπηρεσία *WAYF* η οποία αναλαμβάνει με δικές τις μεθόδους τον προσδιορισμό επιθυμητού *IdP* και είναι πάλι πιθανή η αποθήκευσή του σε ένα Cookie του χρήστη. Στο *Liberty – Alliance ID – FF* προβλέπεται η ύπαρξη ενός *DNS Domain* στο οποίο να έχουν πρόσβαση όλοι οι συμμετέχοντες οργανισμοί στην καθεμιά σύμπραξη «εμπιστοσύνης» και έναν τουλάχιστον σταθμό τους να ανήκει στο κοινό *Domain*. Συνεπώς, κάθε απόπειρα αναζήτησης του επιθυμητού *IdP* περνάει από το σταθμό του οργανισμού στο κοινό *Domain* ο οποίος μπορεί να γράφει και να διαβάζει το Cookie στο σταθμό του χρήστη με το όνομα του *IdP* που μπορεί να αυθεντικοποιήσει τον χρήστη. Αυτό συμβαίνει γιατί τα Cookies έχουν τον περιορισμό να μπορούν να διαβαστούν μόνο από το Web Site που τα δημιούργησε και αυτό ελέγχεται βάσει του *DNS Domain* του Web Site. Η

συγκεκριμένη τακτική του *Liberty – Alliance ID – FF* είναι προαιρετική και λαμβάνει κάποιες αρνητικές κριτικές [114]. Η λειτουργία των ανωτέρω μηχανισμών απαιτεί τη μείωση του επιπέδου ασφαλείας στον Browser του χρήστη, ώστε να είναι πλήρως αποδεκτά τα Cookies, γεγονός το οποίο συχνά δεν είναι αποδεκτό.

3.2.2.3 Ευκολία Υλοποίησης – Τεκμηρίωση – Εφαρμογές

Οι εξεταζόμενες λύσεις παρουσιάζουν συγκεκριμένες διαφορές και στο θέμα της διάθεσής τους προς υλοποίηση:

- Το *WS-Federation* διαθέτει τις τεχνικές της λεπτομέρειες ελεύθερες προς ενημέρωση και αναφορά, μαζί φυσικά με όλη τη σειρά WS-*. Ταυτόχρονα, όμως, γίνεται η επισήμανση ότι αυτές αποτελούν πνευματική ιδιοκτησία των εταιρών IBM Corporation, Microsoft Corporation, BEA Systems Inc., RSA Security Inc., Verisign Inc. και η περαιτέρω χρήση ή εκμετάλλευση των συγκεκριμένων προδιαγραφών υποχρεωτικά διέρχεται μέσω αυτών των εταιριών [4]. Συνεπώς, μπορούν να υπάρξουν μόνο πλήρη εμπορικά προϊόντα τα οποία υποστηρίζουν την προδιαγραφή *WS-Federation* και ο βαθμός ευκολίας εγκατάστασής τους θα εξαρτάται κατά περίπτωση από τις προσφερόμενες στο προϊόν διευκολύνσεις και υποστήριξη. Τέτοια εμπορικά προϊόντα, εκτός φυσικά από το εγγενές προϊόν της Microsoft τις *ADFS* του *Windows Server 2003*, είναι η σουίτα προϊόντων *Oracle Identity Management* και ειδικότερα το προϊόν *Oracle Identity Federation* [112] ή το προϊόν *Federated Identity Access Manager* της εταιρίας *Symlabs* [137].

- Το *Liberty – Alliance ID – FF* είναι επίσης ελεύθερο σε σχέση με τις τεχνικές του λεπτομέρειες, αλλά και σε ότι αναφορά την υλοποίησή του. Συνεπώς, τόσο εμπορικά προϊόντα όσο και λύσεις ανοιχτού κώδικα (*open - source*) έχουν ενσωματώσει και υλοποιήσει τις προδιαγραφές του *Liberty – Alliance Project*. Το ίδιο το *Project* δεν προσφέρει κάποια υλοποίηση των προδιαγραφών παρά διαθέτει μεγάλη συλλογή από υποστηρικτικό και τεκμηριωτικό υλικό και παρέχει προβολή σε όλες τις υλοποιήσεις από ιδιωτικές εταιρίες, δημόσιους φορείς, εμπορικά προϊόντα και *open - source* λύσεις. Ο οργανισμός *Liberty – Alliance Project* υποστηρίζει ότι μέχρι το τέλος του 2006 ένα δισεκατομμύριο συσκευές θα υποστηρίζουν τις προδιαγραφές του. Αυτό είναι ένα δείγμα της σχετικά έντονης διαφημιστικής προσπάθειας και υποστήριξης των προϊόντων του *Project*. Ενδεικτικά, κάποιες από τις αναφερόμενες υλοποιήσεις του *ID – FF* ανά τομέα είναι [73]:

  - <u>*eGovernment*</u>: Γαλλία (“Mon Service Public” portal), Νορβηγία (“MyPage” portal), Ηνωμένο Βασίλειο (“Gateway Authentication Service”) κλπ
  - <u>*Χρηματοπιστωτικές Υπηρεσίες*</u>: American Express κλπ
  - <u>*Τηλεπικοινωνίες*</u>: France Telecom / Orange, Nokia, Turkcell, Vodafone κλπ
  - <u>*Εμπορικά Προϊόντα*</u>: Novell, IBM, Sun, Symlabs, RSA Security κλπ. Ειδικά για τους κατασκευαστές εμπορικών προϊόντων το *Liberty – Alliance Project* παρέχει μία υπηρεσία πιστοποίησης της διαλειτουργικότητας των προϊόντων τους σε σχέση με τις προδιαγραφές του *Liberty - Alliance Project* διατυπώνοντας μία σειρά από σενάρια δοκιμών σε καθορισμένο από το *Project* περιβάλλον ελέγχου. Αυτή η υπηρεσία καλείται *Liberty Interoperable*™ και μπορεί να συνοδεύει το καθένα εμπορικό προϊόν ως ένα επιπλέον προσόν του.

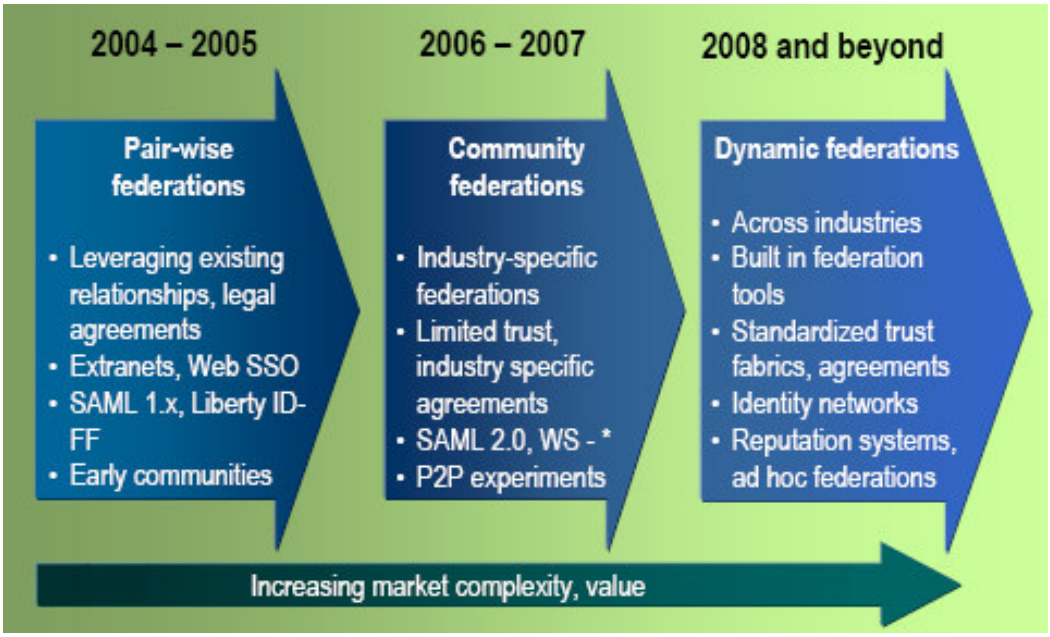
- Το *Shibboleth* είναι η μόνη ελεύθερη, καθαρά *open – source* λύση από τις τρεις και διατίθεται ελεύθερα υπό τις συνθήκες αδειών χρήσης που ισχύουν και για το λογισμικό Apache. Η υλοποίηση που παρέχεται ελεύθερα από την ομάδα ανάπτυξης τους *Shibboleth* είναι γραμμένη σε γλώσσα C++ και Java, ενώ μπορούν να υποστηριχθούν λειτουργικά συστήματα Linux, Windows και MacOS. Ένα βασικό πλεονέκτημα του *Shibboleth* είναι ότι μπορεί να λειτουργήσει τόσο με Web Server Apache όσο με τον IIS των Windows, ενώ στο τμήμα του *IdP* δημοσιοποιούνται ειδικές προεκτάσεις (extensions) για τη συνεργασία του *Shibboleth* με διαδεδομένα έργα ή προϊόντα (πχ το έργο *e-Authentication* της κυβέρνησης των ΗΠΑ ή τις *ADFS* των Windows). Η *open - source* φιλοσοφία του *Shibboleth* και η αρχική ανάπτυξή του στα πλαίσια των ακαδημαϊκών ιδρυμάτων έχει ως αποτέλεσμα την ανάπτυξη πολλών πηγών πληροφόρησης και υποστήριξης για τις τεχνικές λεπτομέρειες της λύσης αλλά και για τις φάσεις εγκατάστασής του σε μία σύμπραξη οργανισμών. Ως *open - source* προϊόν φυσικά απαιτεί αρκετές και ίσως σύνθετες εργασίες οι οποίες πρέπει να γίνουν από όσους επιθυμούν να το εγκαταστήσουν, αλλά ταυτόχρονα η «κοινότητα» που έχει σχηματιστεί γύρω από το προϊόν παρέχει αρκετό υποστηρικτικό υλικό [23]. Πέρα από τη συνεισφορά της ευρύτερης κοινότητας στην υποστήριξη του *Shibboleth*, πολλοί ακαδημαϊκοί φορείς των ΗΠΑ οργανώνουν συνέδρια και ομάδες εργασίας αποκλειστικά και μόνο για την αποσαφήνιση των διαδικασιών και δυσκολιών εγκατάστασης του *Shibboleth* και της συνεργασίας του με άλλα προϊόντα διαχείρισης ταυτοτήτων, πχ [22]. Ταυτόχρονα, υπάρχουν αρκετές αναφορές και σε επεκτάσεις που έχουν γίνει από την ίδια την κοινότητα του *Shibboleth* οι οποίες αναφέρονται στην επίσημη πηγή του προϊόντος, αλλά δεν υιοθετούνται ως μέρος του. Οι εφαρμογές του *Shibboleth* αφορούν κυρίως ακαδημαϊκά ιδρύματα σε όλο τον κόσμο, *open - source* λύσεις, κρατικούς φορείς και ιδρύματα, ψηφιακές βιβλιοθήκες κλπ. Ενδεικτικά, κάποιες από τις εγκαταστάσεις του *Shibboleth* είναι [54]:

  - <u>*ΗΠΑ - InCommon:*</u> αποτελεί τη σύμπραξη μεγάλων Πανεπιστημίων των ΗΠΑ για την ομοιόμορφη και προστατευόμενη διαμοίραση των πόρων τους [51].
  - <u>*Διεθνή Ανώτερα Ακαδημαϊκά Ιδρύματα:*</u> Ελβετία ("*SWITCH*"), Αυστραλία ("*MAMS*"), Δανία ("*DK-AAI*"), Γαλλία ("*CRU*"), Ηνωμένο Βασίλειο ("*UK Access Management Federation for Education and Research*") κλπ
  - <u>*Ψηφιακές Βιβλιοθήκες*</u>: National Science Digital Library (NSDL), Online Computer Library Center (OCLC) κλπ.

Σύμφωνα με εκτιμήσεις του συμβουλευτικού οίκου Burton Group [10] η εφαρμογή των προϊόντων – λύσεων που βασίζονται στη *SAML* έχουν ήδη αποκτήσει αξιόλογη «ορμή» και οι λειτουργικότητες των *Federated Identities* παίρνουν τη θέση τους μέσα στα ευρύτερα συστήματα Διαχείρισης Ταυτοτήτων ως σχεδόν αναπόφευκτη επιλογή. Οι λόγοι γι αυτή την ανάγκη αναλύθηκαν και στην παράγραφο 2.2 και εντοπίζονται στις διαμορφούμενες επιχειρηματικές και διοικητικές απαιτήσεις από τις σύγχρονες δικτυακές εφαρμογές και την αποδοτικότερη αξιοποίηση του Internet. Συνεπώς, η υλοποίηση λύσεων *Federated Identity Management* έχει ήδη περάσει ένα πρώτο στάδιο (2004 – 2005) με την κυριαρχία εγκατεστημένων, «έμπιστων» συνδέσεων μεταξύ ζευγαριών Οργανισμών και την εφαρμογή πρώτων εκδόσεων των σχετικών προδιαγραφών (βλ. παρακάτω Εικόνα). Στο εκτιμώμενο ως «δεύτερο κύμα» εφαρμογής των λύσεων (2006 – 2007) τα απλά «ζεύγη» συνεργασιών θα εξελιχθούν σε μικρές «κοινότητες» όπου θα είναι εφικτή η αλληλεπίδραση μεταξύ των μελών τους, με κινητήριες δυνάμεις τους σχηματιζόμενους "*Circles of Trust*" του *Liberty Alliance Project,* το *Shibboleth* και άλλα ιδιωτικά ή δημόσια έργα. Στο τρίτο προβλεπόμενο «κύμα» (2008 και μετά) υπολογίζεται ότι

θα σχηματιστούν πιο δυναμικά μεταβαλλόμενες συνεργασίες με την προϋπόθεση ότι θα έχει ξεκαθαρίσει το τοπίο των εκδόσεων των προδιαγραφών και αυτές θα είναι ενσωματωμένες είτε στα λειτουργικά συστήματα είτε σε πλατφόρμες λογισμικού γενικότερης και ευρύτερης χρήσης. Σε αυτή τη φάση θα είναι εφικτή, βιώσιμη και περισσότερο επικερδής η υλοποίηση των λύσεων *Federated Identity Management* στις καθημερινές εμπορικές ή κρατικές εφαρμογές, αλλά πιθανώς να έχουν προκύψει και νέες «απειλές» που να δοκιμάζουν τα όρια ασφαλείας των λύσεων.

Πηγή: [10]



Εικόνα 54: Προβλεπόμενη Υιοθέτηση Λύσεων *Federated Identity Management*

Οι δυνατότητες εφαρμογών των προτύπων *Identity Federation* σε επιχειρηματικά «σενάρια» εκμετάλλευσης του Internet έχει οδηγήσει σε έντονο ανταγωνισμό μεταξύ των Οργανισμών ή των εταιρικών συμπράξεων που εισηγούνται τα συγκεκριμένα πρότυπα. Πέρα, επομένως, από το καθαρά τεχνολογικό μέρος διεξάγεται αξιοπρόσεκτη επιχειρηματική αντιπαράθεση για την υπεροχή της καθεμιάς λύσης, ειδικότερα μεταξύ των *WS-Federation* προδιαγραφών και αυτών του *Liberty – Alliance Project* [59, 77].

3.3 Εφαρμογές των Λύσεων SSO στο e-Government

3.3.1 Εφαρμογές e-Government: Ιδιαίτερα Χαρακτηριστικά και Απαιτήσεις

3.3.1.1 Γενικά

Από την επισκόπηση των χαρακτηριστικών των λύσεων SSO (βλ. παράγραφο 3.2) προκύπτει το συμπέρασμα ότι ο Ακαδημαϊκός χώρος και ο χώρος της Ηλεκτρονικής Διακυβέρνησης (e-Government) παρουσιάζουν πολλές περιπτώσεις εφαρμογών των λύσεων SSO, για τις οποίες είναι δυνατή η ανάκτηση επαρκούς υλικού τεκμηρίωσης. Ειδικότερα οι εφαρμογές του e-Government παρουσιάζουν ιδιαίτερο ενδιαφέρον, γιατί η έννοια της ταυτότητας του πολίτη και η επιβεβαίωση της αυθεντικότητάς της είναι ο καθοριστικός παράγοντας έναρξης οποιασδήποτε συναλλαγής των πολιτών με το Κράτος. Καταρχήν, με τον όρο e-Government χαρακτηρίζεται η χρήση των Τεχνολογιών Πληροφορίας και Τηλεπικοινωνιών για τη βελτίωση της αποδοτικότητας, της αποτελεσματικότητας, της διαφάνειας και της υπευθυνότητας της Δημ. Διοίκησης καθώς και για τη βελτίωση της αλληλεπίδρασης Κράτους – Πολιτών – Επιχειρήσεων. Μία από τις προτεινόμενες κατηγοριοποιήσεις των χαρακτηριστικών του e-Government γίνεται με βάσει τα συναλλασσόμενα μέρη [37]:

- *Πολίτες (Citizens)*: περιλαμβάνονται οι ηλεκτρονικές υπηρεσίες *Government – to – Citizen* (*G2C*), όπως πληροφόρηση – εξυπηρέτηση των πολιτών, *Citizen – to – Government* (*C2G*), όπως η συμπλήρωση φορολογικής δήλωσης. Επίσης, μπορεί να γίνει διαχωρισμός των υπηρεσιών προς πολίτες ανά υπουργείο/τομέα: Υγεία, Παιδεία, Ασφάλεια κλπ

- *Επιχειρήσεις (Business)*: περιλαμβάνει τις υπηρεσίες *Government – to – Business* (*G2B*), όπως πληροφόρηση – εξυπηρέτηση των πολιτών, *Business – to – Government* (*B2G*) ή κατά Υπουργείο/Τομέα.

- *Άλλες Δημόσιες Υπηρεσίες ίδιου Επιπέδου*: περιλαμβάνει διαφόρων μορφών επικοινωνία μεταξύ Δημ. Υπηρεσιών (*Government – to – Government*).

- *Άλλα Επίπεδα Κρατικών Υπηρεσιών*: περιλαμβάνει επικοινωνία μεταξύ τοπικών και περιφερειακών οργανισμών αυτοδιοίκησης.

- *Ευρύτερος Δημ. Τομέας*: περιλαμβάνει επικοινωνία με άλλους φορείς εκτός όμως του ιδιωτικού – επιχειρηματικού τομέα (πχ μη-κρατικές οργανώσεις, άλλες κυβερνήσεις ή Δημ. Υπηρεσίες άλλων χωρών κλπ)

Μία περαιτέρω κατηγοριοποίηση των ηλεκτρονικών υπηρεσιών που μπορεί να προσφέρουν οι Δημόσιες Υπηρεσίες γίνεται ανάλογα με το βαθμό ολοκλήρωσης της υπηρεσίας που μπορεί να επιτευχθεί ηλεκτρονικά και διατυπώνει τέσσερα επίπεδα [165]:

- *Επίπεδο 1 - Πληροφοριακές Υπηρεσίες (Information)*: Παρέχουν μόνο πληροφοριακό υλικό για τον τρόπο διεκπεραίωσης της υπηρεσίας.

- *Επίπεδο 2 – Επικοινωνιακές Υπηρεσίες (Interaction)*: Παρέχουν πληροφοριακό υλικό για τον τρόπο διεκπεραίωσης της υπηρεσίας καθώς και επίσημο υλικό (πρότυπα αιτήσεων, βεβαιώσεων, κλπ) το οποίο οι χρήστες μπορούν να το χρησιμοποιήσουν κατά τη συναλλαγή τους με το φορέα σε φυσικό επίπεδο.

- *Επίπεδο 3 – Διαδραστικές Υπηρεσίες (Two way interaction)*: Εκτός από πληροφορίες, προσφέρουν on-line φόρμες για συμπλήρωση και ηλεκτρονική αποστολή με ταυτόχρονη

ανάπτυξη μηχανισμών αναγνώρισης, ταυτοποίησης και προστασίας των δεδομένων που αποστέλλει ο χρήστης της υπηρεσίας.

- *Επίπεδο 4 – Συναλλακτικές Υπηρεσίες (Transaction)*: Εκτός από φόρμες αποστολής στοιχείων, υποστηρίζουν λειτουργίες όπου ο χρήστης ολοκληρώνει τις συναλλαγές που περιλαμβάνει η υπηρεσία με ταυτόχρονη, πλήρη υποκατάσταση της αντίστοιχης μη-ηλεκτρονικής διαδικασίας και ανάπτυξη μηχανισμών αναγνώρισης, ταυτοποίησης και προστασίας των δεδομένων που αποστέλλει ο χρήστης της υπηρεσίας.

Στο θέμα, όμως, της αυθεντικοποίησης, η διαδικασία αποδεικνύεται ιδιαιτέρως πολύπλοκη όταν αφορά κρατικές υπηρεσίες και συγκεκριμένα όταν η εφαρμογή της λαμβάνει χώρα μέσω δικτύων δεδομένων. Η αντιμετώπιση, επομένως, της αυθεντικοποίησης σε Κρατικές ηλεκτρονικές υπηρεσίες περιλαμβάνει την πρότερη επίλυση πολλών θεμάτων διαφόρων πεδίων (νομικά, οικονομικά, κυβερνητικής πολιτικής και τεχνολογικά). Συνεπώς, κάθε σχετικό έργο ξεκινάει με τη διατύπωση ενός σύνθετου πλαισίου Διαχείρισης Ταυτοτήτων στο οποίο η αυθεντικοποίηση ορίζεται και υλοποιείται ανάλογα με τις προδιαγραφές που διέπουν τους διοικητικούς και τεχνολογικούς στόχους της υπόλοιπης υποδομής του συστήματος Διαχείρισης Ταυτοτήτων. Προκειμένου να συγκροτηθεί μία τέτοια υποδομή, τα σχετικά έργα που βρίσκονται υπό την αιγίδα κρατικών διοικήσεων καλύπτουν πολλούς ερευνητικούς τομείς και καταλήγουν σε χρήσιμα συμπεράσματα που αγγίζουν πολλές πτυχές της έννοιας της ταυτότητας και της αυθεντικοποίησης στο διαδίκτυο [37].

3.3.1.2 Αρχές Διαχείρισης Ταυτοτήτων στο e-Government

Μία μελέτη υλοποίησης ευρύτερου υπόβαθρου Κρατικής Διαχείρισης Ταυτοτήτων διατυπώνει [37] συγκεκριμένες αρχές (τόσο τεχνολογικές όσο και διοικητικές) στις οποίες ο σχεδιασμός των σχετικών συστημάτων που εφαρμόζονται σε Πληροφοριακά Συστήματα ηλεκτρονικών υπηρεσιών του Δημοσίου Τομέα οφείλει να βασίζεται:

- *Αυτονομία (Autonomy)*: Κάθε νέα υποδομή δεν πρέπει να εμποδίζει το δικαίωμα κάθε πολίτη να συναλλάσσεται ελεύθερα με τη Δημόσια Διοίκηση. Η προσωπική ελευθερία του πολίτη είναι το θεμέλιο κάθε δημοκρατικής κοινωνίας και κάθε νέο σύστημα δε θα πρέπει να την περιορίζει.

- *Εμπιστευτικότητα (Privacy)*: Κυρίως περιλαμβάνει την απέχθεια των πολιτών προς τα φαινόμενα καταπιεστικής παρακολούθησης κάθε κίνησής τους ή την απρόσωπη αντιμετώπισή τους από ένα μεγάλο σύστημα ως ένας απλός αριθμός.

- *Εσωτερική Αποδοτικότητα της Κυβέρνησης (Internal Government Efficiency)*: Ο σημαντικότερος σκοπός του e-Government είναι να καταστεί ικανή η Δημ. Διοίκηση να κάνει περισσότερα με λιγότερο κόστος (γρηγορότερες, καλύτερες και φθηνότερες υπηρεσίες). Η λειτουργία πολλών διαφορετικών συστημάτων δυσκολεύουν την εργασία πέρα από τα όρια γραφειοκρατικών σχηματισμών.

- *Ελεύθερη Κυκλοφορία της Πληροφορίας (Free Flow of Information)*: Η παρεμπόδιση της ροής των πληροφοριών μπορεί να προκαλέσει προβλήματα στην ανάπτυξη αγορών εργασίας ή κατάλληλων εμπορικών συνθηκών. Ταυτόχρονα, η διάθεση πληροφοριών ταυτο-

τήτων μπορεί να προστατέψει ή να αντιμετωπίσει απόπειρες εξαπάτησης της Δημ. Διοίκησης.

- *Κατανόηση και Διακυβέρνηση (Responsiveness and Governance)*: Η ευκολία συναλλαγής των πολιτών με το Κράτος είναι ένα δείγμα Δημοκρατίας. Η δυνατότητα πρόσβασης και επικοινωνίας των πολιτών με τα ανώτερα κλιμάκια της Δημ. Διοίκησης ενδυναμώνει τη Δημοκρατία. Επίσης, το ίδιο αποτέλεσμα έχει και η βελτίωση των διαδικασιών με ελάττωση της γραφειοκρατίας και η καλύτερη κατανόηση των διοικητικών διαδικασιών από τους πολίτες.

- *Κοινωνική (Εθνική) Ασφάλεια και Εφαρμογή του Νόμου (Social – National Security and Law Enforcement)*: Το κοινωνικό σύνολο θα πρέπει να προστατεύεται με την αναγνώριση και ταυτοποίηση των ατόμων που την απειλούν. Το «ηλεκτρονικό έγκλημα» (κλοπή δεδομένων ταυτοτήτων, spamming και οι διαφόρων ειδών ιοί) αυξάνεται δραματικά και οι πολίτες αξίζουν της προστασίας των νέων ηλεκτρονικών υποδομών, οι οποίες δε θα πρέπει να αφήνουν κενά για τέτοιους είδους απειλές.

Συμπερασματικά, οι τάσεις της αντιμετώπισης των δεδομένων ταυτοτήτων στη Δημόσιο Διοίκηση είναι [37]:

- Η ενοποίηση των δεδομένων ταυτοτήτων που διατηρούν οι διάφορες Δημόσιες Υπηρεσίες. Οι ταυτότητες πρέπει να μεταδίδονται ελεύθερα από τα σημεία της Δημ. Διοίκησης, όπου συγκεντρώνονται, στις υπόλοιπες υπηρεσίες. Ταυτόχρονα, επιδιώκεται ο περιορισμός της πολλαπλής υποβολής προσωπικών στοιχείων από πλευράς των πολιτών, εφόσον έχουν καταχωρηθεί σε κάποιο ηλεκτρονικό σύστημα Δημόσιας Διοίκησης.

- Η επιβεβαίωση της ταυτότητας των πολιτών πρέπει να εφαρμόζεται με το ασφαλέστερο δυνατό τρόπο. Πέρα από τους λόγους ασφαλείας που έχουν εγερθεί τα τελευταία χρόνια, ακόμα και οι πιο καθημερινές εργασίες των πολιτών στις Δημόσιες Υπηρεσίες απαιτούν την ορθή επιβεβαίωση του ισχυρισμού της ταυτότητας ενός πολίτη, ιδιαίτερα όταν η συναλλαγή περιλαμβάνει οικονομικά ή φορολογικά δεδομένα και ποσά.

- Το Κράτος λειτουργεί ως θεσμός επιβεβαίωσης της ταυτότητας των πολιτών και σε άλλους οργανισμούς ή φορείς του Δημόσιου βίου. Για παράδειγμα, ένα πιστοποιητικό γέννησης καθορίζει την ταυτότητα ενός πολίτη εφ' όρου ζωής και συνδέει το άτομο που το κατέχει με το όνομα που αναγράφεται σε αυτό. Συνεπώς, οι πληροφορίες ταυτοτήτων που συγκεντρώνουν και συντηρούν οι Δημόσιες Υπηρεσίες πρέπει να είναι έγκυρες και προστατευμένες ώστε να προφυλάσσεται το κύρος του Κράτους και η εύρυθμη κοινωνική ζωή.

3.3.1.3 Η Αυθεντικοποίηση σε Ηλεκτρονικές Υπηρεσίες e-Government

Για την επίτευξη των παραπάνω γενικών απαιτήσεων οι μελέτες για την εφαρμογή ενιαίας αυθεντικοποίησης στις Δημόσιες ηλεκτρονικές υπηρεσίες σε πρώτη φάση ανέλυσαν περαιτέρω την έννοια της αυθεντικοποίησης. Μία πρώτη κατηγοριοποίηση γίνεται με βάση το σκοπό της αυθεντικοποίησης [143]:

- *Identity Authentication*: επιβεβαίωση της μοναδικής ταυτότητας ενός ατόμου.

- *Attribute Authentication*: επιβεβαίωση της συμμετοχής ενός ατόμου σε μία συγκεκριμένη ομάδα.

Η *Attribute* αυθεντικοποίηση περιλαμβάνει τον έλεγχο κατοχής από την πλευρά του χρήστη μίας συγκεκριμένης ιδιότητας (*attribute*), ενώ δεν είναι απαραίτητη η σύνδεση του *attribute* με την ταυτότητά του. Σε αυτή την περίπτωση προκύπτει η έννοια των «ανώνυμων πιστοποιητικών» βάσει των οποίων ελέγχεται η ύπαρξη του συγκεκριμένου *attribute*. Στα συστήματα Διαχείρισης Ταυτότητας Δημοσίου Τομέα είναι συνηθέστερη η *Identity Authentication*.

Μία άλλη κατηγοριοποίηση αφορά τους μηχανισμούς διεξαγωγής της αυθεντικοποίησης [36]:

- *Identification (ή Knowledge based authentication)*: περιλαμβάνει τη γνώση ενός ή περισσότερων πραγματικών προσωπικών δεδομένων του χρήστη (πχ ΑΦΜ, Αστ. Ταυτότητα, ΑΜ ΙΚΑ κλπ) με βάση τα οποία γίνεται η αυθεντικοποίηση.

- *Credential Based Authentication (ή Shared Secret)*: περιλαμβάνει τη χρήση «ζευγαριών» username/password ή «πιστοποιητικών»/PIN ή αμοιβαίως γνωστών «μυστικών» (πχ μυστική ερώτηση κλπ)

- *Biometric Based Authentication*: βασίζεται σε φυσιολογικά χαρακτηριστικά του χρήστη.

- *Token Based Authentication*: περιλαμβάνει τη χρήση κάποιου hardware *Token* (Smart Card, USB Token) το οποίο περιέχει οποιοδήποτε από τα παραπάνω δεδομένα ταυτότητας.

Η παραπάνω κατηγοριοποίηση συνδέεται και με την κατάρτιση διαφορετικών επιπέδων διασφάλισης που επιθυμεί να έχει η καθεμιά ηλεκτρονική υπηρεσία από τη διαδικασία αυθεντικοποίησης που διαθέτει. Η έννοια των επιπέδων διασφάλισης (*assurance levels*) εισάγεται από τις μελέτες έργων e-Government σε ότι αφορά την αυθεντικοποίηση και περιγράφει το βαθμό βεβαιότητας της Δημ. Υπηρεσίας ότι ο χρήστης έχει παρουσιάσει ένα «πιστοποιητικό» το οποίο αναφέρεται στην ταυτότητά του. Συγκεκριμένα, η διασφάλιση της Δημ. Υπηρεσίας από τη διαδικασία αυθεντικοποίησης ορίζεται ως [143]:

- Ο βαθμός εμπιστοσύνης στη διαδικασία ελέγχου για την πιστοποίηση της ταυτότητας του χρήστη για τον οποίο «εκδόθηκε» το παρουσιαζόμενο «πιστοποιητικό» (αφορά την αρχική διαδικασία εγγραφής των χρηστών).

- Ο βαθμός εμπιστοσύνης ότι ο χρήστης που χρησιμοποιεί ένα «πιστοποιητικό» είναι ο ίδιος για τον οποίο αυτό αρχικά «εκδόθηκε».

Με βάση αυτό τον ορισμό προσδιορίζονται τέσσερα επίπεδα απαιτούμενης διασφάλισης των Δημ. Υπηρεσιών ανάλογα με το βαθμό κρισιμότητας των ηλεκτρονικών υπηρεσιών που παρέχουν σε ένα δίκτυο. Όσο πιο κρίσιμες είναι οι δικτυακές εφαρμογές, τόσο πιο μεγάλη πρέπει να είναι η διασφάλιση της Δημ. Υπηρεσίας [128, 143]:

- ***Assurance Level 1***: *Minimal Assurance* – μικρή ή καθόλου εμπιστοσύνη στην εγκυρότητα της παρουσιαζόμενης ταυτότητας.

- ***Assurance Level 2***: *Low Assurance* – μερική εμπιστοσύνη στην εγκυρότητα της παρουσιαζόμενης ταυτότητας.

- ***Assurance Level 3***: *Substantial Assurance* – υψηλή εμπιστοσύνη στην εγκυρότητα της παρουσιαζόμενης ταυτότητας.
- ***Assurance Level 4***: *High Assurance* – πολύ υψηλή εμπιστοσύνη στην εγκυρότητα της παρουσιαζόμενης ταυτότητας.

Κατά τον καθορισμό της πολιτικής αυθεντικοποίησης που θα εφαρμοστεί σε ένα διευρυμένο Πληροφ. Σύστημα διαδικτυακών εφαρμογών Δημ. Υπηρεσιών απαιτείται η αναλυτική μελέτη πιθανών απειλών κατά των διακινούμενων «πιστοποιητικών». Επιπροσθέτως, είναι απαραίτητο να καθοριστούν η πιθανότητα υλοποίησης των απειλών και οι επιπτώσεις τους. Ενδεικτικές επιπτώσεις από αποτυχία επίτευξης των στόχων της αυθεντικοποίησης μπορεί να είναι [143]:

- Διαμαρτυρίες, προσβολή της υπόληψης και του κύρους της Δημ. Υπηρεσίας.
- Οικονομική απώλεια και παθητικό στη Δημ. Υπηρεσία.
- Προσβολή των δημοσίων προγραμμάτων και συμφερόντων.
- Μη εγκεκριμένη διανομή ευαίσθητων δεδομένων.
- Διακινδύνευση της προσωπικής ασφάλειας πολιτών.
- Ποινικές ή αστικές παραβάσεις.

Ανάλογα, επομένως, με την παραπάνω μελέτη καθορίζεται και το *Επίπεδο Διασφάλισης* (*Assurance Level*) που απαιτεί καθένας Δημ. Οργανισμός από τη διαδικασία αυθεντικοποίησης των χρηστών που την προσπελαύνουν ηλεκτρονικά, το οποίο πρέπει να είναι το ελάχιστο που ικανοποιεί όλες τις ηλεκτρονικές υπηρεσίες του Οργανισμού. Μερικά παραδείγματα ηλεκτρονικών υπηρεσιών που μπορούν να αντιστοιχηθούν στα ανωτέρω *Επίπεδα Διασφάλισης* είναι [143]:

- *Assurance Level 1* – ελάχιστη ή καθόλου εμπιστοσύνη στην παρουσιαζόμενη ταυτότητα:
  - Μερικές εφαρμογές που περιλαμβάνουν υποβολή στοιχείων σε Web φόρμες, εφόσον δεν απαιτείται απόκριση από την Web εφαρμογή και δεν υπάρχει αντίστροφη ροή δεδομένων, πχ μία απλή αίτηση προς μία υπηρεσία.
  - Συμμετοχή χρηστών σε ένα δημόσιο forum που απαιτεί ελάχιστες προσωπικές πληροφορίες.
- *Assurance Level 2* – μερική εμπιστοσύνη στην παρουσιαζόμενη ταυτότητα:
  - Υπηρεσίες ενημέρωσης προσωπικών στοιχείων διεύθυνσης ή τραπεζικών λογαριασμών σε περιπτώσεις όπου ο χρήστης είναι δικαιούχος επιδοτήσεων ή δημοσίων προγραμμάτων. Η υποκλοπή των «πιστοποιητικών» αυθεντικοποίησής του και η πρόσβαση ενός τρίτου σε αυτές τις πληροφορίες προκαλούν σοβαρή ζημιά, αλλά δεν επιφέρουν κάποιες μόνιμες ή μη αναστρέψιμες καταστροφές.
  - Υπηρεσία απομακρυσμένης κατάρτισης (e-learning) πολιτών στην οποία διατηρείται και πλήρες, εξατομικευμένο προσωπικό και εκπαιδευτικό προφίλ του καθένα εκπαιδευόμενου. Η μη εγκεκριμένη πρόσβαση σε αυτά τα δεδομένα δεν προκαλεί

καταστροφικές συνέπειες, αλλά προσβάλει το κύρος της υπηρεσίας και το δικαίωμα της μυστικότητας του εκπαιδευτικού ιστορικού του καθένα συμμετέχοντα.

- *Assurance Level 3* – υψηλή εμπιστοσύνη στην παρουσιαζόμενη ταυτότητα:
  - Υπηρεσία διαχείρισης προμηθειών Δημ. Υπηρεσιών όπου οι προμηθευτές διατηρούν προσωπικούς τους λογαριασμούς. Η πρόσβαση στα στοιχεία των λογαριασμών τους πρέπει να γίνεται με «πιστοποιητικά» υψηλής ασφάλειας.
  - Υπηρεσία υποβολής ευρεσιτεχνιών από ειδικά εξουσιοδοτημένο νομικό εκπρόσωπο. Η μη εγκεκριμένη πρόσβαση στα συγκεκριμένα στοιχεία θα επιφέρει διαρροή επαγγελματικών απορρήτων και οικονομική απώλεια.
- *Assurance Level 4* – πολύ υψηλή εμπιστοσύνη στην παρουσιαζόμενη ταυτότητα:
  - Υπηρεσία πρόσβασης σε αρχεία νομικών υποθέσεων από εξουσιοδοτημένους νομικούς εκπροσώπους. Η μη εγκεκριμένη πρόσβαση, εκτός από παραβίαση των προσωπικών δεδομένων, μπορεί να διαστρεβλώσει τη διεξαγωγή νομικών διαδικασιών.
  - Υπηρεσία απομακρυσμένης πρόσβασης ειδικών στελεχών μίας Δημ. Υπηρεσίας στις εσωτερικές εφαρμογές και Βάσεις Δεδομένων της Υπηρεσίας. Η πρόσβαση επιτρέπεται μέσω δημοσίων δικτύων εκτός του εσωτερικού δικτύου της Υπηρεσίας γι αυτό και απαιτείται πολύ αυστηρός έλεγχος «πιστοποιητικών» των υπαλλήλων.

Καθένα *Επίπεδο Διασφάλισης* πρέπει να προστατεύει τη διαδικασία αυθεντικοποίησης από συγκεκριμένες «απειλές», ώστε να «εγγυηθεί» την υποσχόμενη διασφάλιση. Οι εξεταζόμενες «απειλές» είναι όσες παρουσιάστηκαν στην παρ. 2.1.2 με επιπρόσθετη την "*«Εισβολή» στη Συναλλαγή μετά την αυθεντικοποίηση*" (*Session Hijacking*) κατά την οποία η αυθεντικοποίηση ολοκληρώνεται με ασφάλεια, αλλά η υπόλοιπη συναλλαγή μένει απροστάτευτη από πιθανές υποκλοπές και επεμβάσεις τρίτων μερών. Λαμβάνοντας υπόψη και τους ανωτέρω ορισμούς των *Επιπέδων Διασφάλισης*, προκύπτει ο παρακάτω πίνακας απαρίθμησης των «απειλών» που οφείλει να «εξουδετερώνει» κάθε *Επίπεδο* [93]:

Πηγή: [93]

	Επίπεδα Διασφάλισης			
Προστασία Εναντίον	**Επίπεδο 1**	**Επίπεδο 2**	**Επίπεδο 3**	**Επίπεδο 4**
Password Guessing	√	√	√	√
Replay Attack	√	√	√	√
Υποκλοπή (*Eavesdropping*)		√	√	√
Πλαστοπροσωπία Ελεγκτή (*Verifier Impersonation*)			√	√
Man – in – the – Middle Attack			√	√
«Εισβολή» στη Συναλλαγή μετά την αυθεντικοποίηση»				√

Πίνακας 1: Αντιμετώπιση «Απειλών» Αυθεντικοποίησης από καθένα *Επίπεδο Διασφάλισης*

Η μελέτη [128] συμπληρώνει τον παραπάνω πίνακα περιλαμβάνοντας στο *Επίπεδο Διασφάλισης 3* και την προστασία από την «απειλή» "*«Εισβολή» στη Συναλλαγή*".

Η προστασία από τις παραπάνω «απειλές» μπορεί να επιτευχθεί με τη χρήση συγκεκριμένων τεχνολογιών αυθεντικοποίησης, οι οποίες περιλαμβάνουν το συνδυασμό επιλογής κατάλληλου μηχανισμού (*Token*) και πρωτοκόλλου αυθεντικοποίησης. Επομένως, για καθένα *Επίπεδο Διασφάλισης* πρέπει να προσδιοριστεί ποιοι μηχανισμοί και ποιες κατηγορίες πρωτοκόλλων ικανοποιούν τις απαιτήσεις του. Συγκεκριμένα, από την παρουσίαση των διαθέσιμων τεχνολογιών αυθεντικοποίησης στην παρ. 2.1.3 έγινε σαφές ότι η χρήση πολλών παραγόντων αυθεντικοποίησης (*multi-factor authentication*) είναι πιο ασφαλής από τη χρήση ενός μόνο παράγοντα (πχ ένα password) καθώς ο ενδεχόμενος εισβολέας θα πρέπει να αποκτήσει, εκτός από τον προσωπικό κωδικό ενός χρήστης και όποιο μηχανισμό (Smart Card, άλλα *Hard Crypto Tokens* κλπ) χρησιμοποιεί επίσης ο χρήστης ως πρόσθετους παράγοντες αυθεντικοποίησης. Συνεπώς, σύμφωνα με την κατηγοριοποίηση των διαθέσιμων *Tokens* αυθεντικοποίησης της παρ. 2.1.3 και των ανωτέρω *Επιπέδων Διασφάλισης*, η σύσταση [93] καθορίζει ότι η ασφάλεια που «υπόσχεται» καθένα *Επίπεδο Διασφάλισης* μπορεί να εξασφαλιστεί με τη χρήση συγκεκριμένων μόνο κατηγοριών *Tokens* (βλ. επόμενο Πίνακα):

Πηγή: [93]

	Επίπεδα Διασφάλισης			
Τύπος Token	**Επίπεδο 1**	**Επίπεδο 2**	**Επίπεδο 3**	**Επίπεδο 4**
Hard crypto token	√	√	√	√
Soft crypto token	√	√	√	
One-time password συσκευή	√	√	√	
Password & PINs	√	√		

Πίνακας 2: Επιτρεπόμενα *Authentication Tokens* για καθένα *Επίπεδο Διασφάλισης*

- Τα *Password Tokens* μπορούν να ικανοποιήσουν τις απαιτήσεις των *Επιπέδων Διασφάλισης 1* και *2*.

- Τα *One – Time Password Tokens*: μπορούν να ικανοποιήσουν τις απαιτήσεις των *Επιπέδων Διασφάλισης 1 – 3*. Ειδικά για το *Επίπεδο Διασφάλισης 3* πρέπει συνδυάζονται με τη χρήση password ή κάποιου βιομετρικού στοιχείου (πχ δακτυλικό αποτύπωμα), διαφορετικά θεωρούνται ότι καλύπτουν μόνο τα *Επίπεδα Διασφάλισης 1 – 2* [128].

- Τα *Soft Cryptographic Tokens* μπορούν να χρησιμοποιηθούν για τη διασφάλιση των *Επιπέδων 1 – 3*, αλλά πρέπει να συνδυάζονται με τη χρήση password ή κάποιου βιομετρικού στοιχείου για την επίτευξη του *Επιπέδου 3*.

- Τα *Hard Cryptographic Tokens*, όταν ενεργοποιούνται με τη χρήση password ή κάποιου βιομετρικού στοιχείου, μπορούν να διασφαλίσουν τα *Επίπεδα 1 – 4*.

Οι παραπάνω προδιαγραφές σε μηχανισμούς αυθεντικοποίησης πρέπει να συνοδεύονται και από αντίστοιχες απαιτήσεις εφαρμογής συγκεκριμένων κατηγοριών πρωτοκόλλων αυθεντικοποίησης με καθένα τύπο *Token* στα διαφορετικά *Επίπεδα Διασφάλισης*. Οι μελέτες [93] και [128] καταγράφουν ποιοι τύποι πρωτοκόλλων αυθεντικοποίησης ικανοποιούν τις απαιτήσεις καθενός Επιπέδου Διασφάλισης (βλ παρακάτω Πίνακα):

Πηγή: [128]

	Επίπεδα Διασφάλισης			
Τύποι Πρωτοκόλλων	**Επίπεδο 1**	**Επίπεδο 2**	**Επίπεδο 3**	**Επίπεδο 4**
Private Key PoP	√	√	√	√
Symmetric Key PoP	√	√	√	√
One-time (or strong) Password	√	√	√	
Tunnelled password PoP	√	√		
Challenge-reply password PoP	√			

Πίνακας 3: Τύποι Πρωτοκόλλων Αυθεντικοποίησης ανά *Επίπεδο Διασφάλισης*

- Πρωτόκολλα Απόδειξης Κατοχής Ιδιωτικού Κλειδιού (*Private Key PoP*): Η κρυπτογράφηση Δημοσίου Κλειδιού σε συνδυασμό με την απόδειξη κατοχής (*Proof of Possession - PoP*) του *Hard Token* το οποίο περιέχει το απαραίτητο «πιστοποιητικό» κρυπτογράφησης και ενεργοποιείται με μυστικό κλειδί ή βιομετρικό στοιχείο είναι ίσως η πιο «ισχυρή» μέθοδος αυθεντικοποίησης, επομένως ένα πρωτόκολλο που την υλοποιεί μπορεί να ικανοποιήσει τις απαιτήσεις όλων των *Επιπέδων Διασφάλισης 1 – 4*.

- Πρωτόκολλα Απόδειξης Κατοχής Συμμετρικού Κλειδιού (*Symmetric Key PoP*): Τοποθετούνται στην ίδια κατηγορία με τα πρωτόκολλα "*Private Key PoP*" με την προϋπόθεση της αυστηρής προστασίας των κοινών κλειδιών.

- Πρωτόκολλα *One-time* ή *«ισχυρών» Password*: Μπορούν να εξασφαλίσουν τη διαδικασία αυθεντικοποίησης από όλες σχεδόν τις «απειλές», καθώς, εφόσον ενεργοποιούνται με κάποιο πρόσθετο προσωπικό κωδικό του χρήστη, μπορούν να αντιστοιχηθούν στην "*two – factor*" αυθεντικοποίηση. Η προστασία, όμως, που παρέχει το πρωτόκολλο και οι αντίστοιχοι μηχανισμοί δεν έχουν ως αποτέλεσμα τη δημιουργία κάποιων κλειδιών για την περαιτέρω προστασία της συνόδου (session) του χρήστη με τη δικτυακή εφαρμογή, άρα δεν εξασφαλίζεται προστασία από την απειλή «*Session Hijacking*» και συνεπώς δεν μπορεί να ικανοποιηθεί το *Επίπεδο Διασφάλισης 4*.

- Πρωτόκολλα *Tunneled Password PoP*: Είναι τα πρωτόκολλα στα οποία τα passwords μεταδίδονται κωδικοποιημένα μέσω «ασφαλών καναλιών» με τη χρήση πρωτοκόλλων όπως το SSL/TLS. Παρά την ασφαλή μετάδοση των passwords, η οποία προστατεύει από επεμβάσεις κατά τη διάρκεια της μετάδοσής τους, τα συγκεκριμένα πρωτόκολλα δεν μπορούν να εξασφαλίσουν με σιγουριά ότι ο χρήστης αποστέλλει τους κωδικούς του στο σωστό ελεγκτή – server και όχι σε κάποια τρίτη, πλαστή υπηρεσία που αποσκοπεί στην υποκλοπή των κωδικών. Αυτό συμβαίνει γιατί η λειτουργία των «ασφαλών πρωτοκόλλων» στηρίζεται και στις ρυθμίσεις του περιβάλλοντος χρήστη και των web browsers, οι οποίοι γενικά ανήκουν στην κατηγορία των ευάλωτων προγραμμάτων.

- Πρωτόκολλα *Challenge-reply Password PoP*: Είναι τα πρωτόκολλα που κατ' ελάχιστο μπορούν να ικανοποιήσουν τις απαιτήσεις του *Επιπέδου Διασφάλισης 1*, καθώς δεν επιτρέπουν την αυτούσια μετάδοση των passwords, συνδυάζουν όμως ένα τυχαίο *Challenge* για την παραγωγή του *Reply* με βάση το οποίο γίνεται η αυθεντικοποίηση. Μπορούν, επομένως, να προστατέψουν από "*Password Guessing*" και "*Replay Attacks*", αλλά είναι ευάλωτα σε όλες τις άλλες επιθέσεις.

Ο ορισμός των *Επιπέδων Διασφάλισης* περιλαμβάνει και την παράμετρο της εμπιστοσύνης στη διαδικασία ελέγχου των φυσικών πιστοποιητικών της ταυτότητας του χρήστη κατά την αρχική εγγραφή του στο σύστημα. Αυτό αποτελεί τη φάση του *Registration* η οποία διέπεται και ορίζεται με κατάλληλο νομοθετικό πλαίσιο και καταλήγει στην απόδοση προς το χρήστη, από τη Διαχειριστική Αρχή του συστήματος, του κατάλληλου *Token* ταυτότητας, ανάλογα και με το *Επίπεδο Διαβεβαίωσης* που εφαρμόζεται στο σύστημα. Οι γενικές απαιτήσεις για τη φάση *Registration* είναι ότι τα «πιστοποιητικά» που ζητούνται από καθένα «αιτούντα» και οι μετέπειτα διαδικασίες ελέγχου τους πρέπει να είναι τέτοιες ώστε [93, 128]:

- Το άτομο με τα χαρακτηριστικά του «αιτούντα» όντως υπάρχει και αντίστροφα αυτά τα χαρακτηριστικά είναι αρκετά για τη μοναδική ταυτοποίηση ενός ατόμου.

- Ο «αιτών» για τον οποίο εκδίδεται το αντίστοιχο *Token* είναι στην πραγματικότητα αυτός στον οποίο ανήκει η περιεχόμενη ταυτότητα.

- Ο «αιτών» δεν μπορεί στο μέλλον να αρνηθεί την εγγραφή (*registration*), έτσι ώστε αν υπάρχει κάποια διένεξη για μία μελλοντική είσοδο στο σύστημα με χρήση του *Token* ενός χρήστη, ο συγκεκριμένος χρήστης δε θα μπορεί να αμφισβητήσει ότι το *Token* έχει εκδοθεί γι αυτόν.

Συμπερασματικά, η αυθεντικοποίηση των χρηστών σε δικτυακές υπηρεσίες Δημοσίων Οργανισμών αποτελεί μέρος ενός ευρύτερου πλαισίου Διαχείρισης Ταυτοτήτων και πρέπει να γίνεται με βάση την Πολιτική Αυθεντικοποίησης (*Authentication Policy*) η οποία θα καταρτιστεί για τις συγκεκριμένες υπηρεσίες. Τα συστατικά της Πολιτική Αυθεντικοποίησης είναι όσες αποφάσεις αναφέρθηκαν παραπάνω σε αυτή την παράγραφο, ενώ τα προτεινόμενα βήματα για τον καθορισμό της είναι [128, 143]:

1. Διεξαγωγή μίας ανάλυσης κινδύνων που απειλούν το e-Government σύστημα. Είναι μία υποκειμενική διαδικασία για καθένα Δημ. Οργανισμό, καθώς θα εκτιμηθούν οι κίνδυνοι, οι πιθανότητες που έχει ο καθένας, η κρισιμότητα των διαχειριζόμενων δεδομένων και πολλά πιθανά «σενάρια» αποτυχίας του συστήματος είτε από ατύχημα είτε από επεμβάσεις τρίτων.

2. Αντιστοίχηση των εντοπισμένων κινδύνων στο απαιτούμενο *Επίπεδο Διασφάλισης*. Οι κίνδυνοι που διατυπώνονται στο $1^{ο}$ βήμα είναι ανεξάρτητοι από τη διαδικασία αυθεντικοποίησης, επομένως στη συνέχεια προσδιορίζεται το μικρότερο *Επίπεδο* που καλύπτει όλους τους αναγνωρισμένους κινδύνους, σύμφωνα με τα χαρακτηριστικά των *Επιπέδων* που παρουσιάστηκαν παραπάνω.

3. Επιλογή των τεχνολογιών αυθεντικοποίησης που ικανοποιούν το επιλεγμένο Επίπεδο Διασφάλισης. Όπως έγινε ήδη σαφές, κάθε *Επίπεδο Διασφάλισης* μπορεί να υλοποιηθεί με την εφαρμογή συγκεκριμένων μόνο τεχνολογιών και μηχανισμών αυθεντικοποίησης.

4. Επιβεβαίωση της επίτευξης του επιθυμητού *Επιπέδου Διασφάλισης* μετά την παραγωγική εφαρμογή των προηγούμενων αποφάσεων. Η υλοποίηση των επιλογών κατάλληλου *Επιπέδου Διασφάλισης* και αντίστοιχων διαδικασιών αυθεντικοποίησης πρέπει να δοκιμαστεί στην πράξη καθώς είναι πιθανό να μην είχαν προβλεφθεί κάποια ενδεχόμενα ή να προκύψουν νέες αδυναμίες του συστήματος κατά τη λειτουργία του.

5. Περιοδική επανεξέταση της ενημερότητας του Πληροφ. Συστήματος. Οι διαδικασίες και οι χρησιμοποιούμενες τεχνολογίες πρέπει να επανελέγχονται σε τακτά χρονικά διαστήματα με γνώμονα την πιθανή εμφάνιση νέων τεχνολογιών ή καταγεγραμμένων απειλών και την πιθανή αλλαγή των λειτουργικών απαιτήσεων των ηλεκτρονικών υπηρεσιών που παρέχει το σύστημα. Η μελέτη του 1ου βήματος γίνεται με βάση τις τεχνολογίες αλλά και τις απαιτήσεις μίας συγκεκριμένης στιγμής, επομένως είναι απαραίτητο να ελέγχεται περιοδικά (συνήθως ετήσια) η επικαιρότητα των εφαρμοσμένων μέτρων σε σχέση με την εισαγωγή ή απενεργοποίηση υπηρεσιών στο σύστημα ή την εμφάνιση νέων εξελίξεων στα θέματα αυθεντικοποίησης.

3.3.1.4 Trust & Federated Identity σε Ηλεκτρονικές Υπηρεσίες e-Government

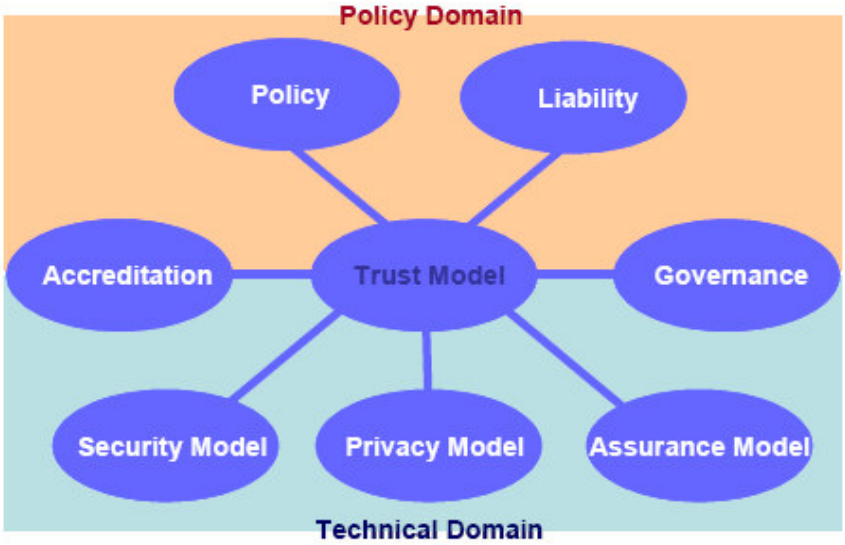
Η Πολιτική Αυθεντικοποίησης που προκύπτει με την εφαρμογή των παραπάνω συνιστώμενων βημάτων είναι μέρος του ευρύτερου πλαισίου Διαχείρισης Ταυτοτήτων του οποίου κυρίαρχος στόχος είναι η διατύπωση θεσμών και τεχνολογιών για την διαλειτουργικότητα (*interoperability*) των δεδομένων ταυτοτήτων μεταξύ των Δημ. Οργανισμών. Μία από τις βασικές απαιτήσεις των μοντέρνων συστημάτων Διαχείρισης Ταυτοτήτων στο e-Government είναι η δυνατότητα ασφαλούς μεταφοράς δεδομένων ταυτότητας ώστε να μπορεί να υλοποιηθεί αυθεντικοποίηση ενός χρήστη σε πολλές ηλεκτρονικές υπηρεσίες με τη διατήρηση των πληροφοριών ταυτότητάς του στο αρχικό σημείο εγγραφής του. Συνεπώς, η προτεινόμενη λύση είναι η εγκατάσταση νομικού και τεχνολογικού πλαισίου συνεργασίας «έμπιστων» Δημοσίων Οργανισμών και η εφαρμογή λύσεων *Federated Identity Management*. Με αυτό τον τρόπο οι χρήστες θα εγγράφονται μία φορά σε μία αρχική ηλεκτρονική υπηρεσία Δημ. Οργανισμού και θα μπορούν να προσπελαύνουν και άλλες υπηρεσίες άλλων Οργανισμών με τα ίδια *Tokens* και την ίδια διαδικασία [36]. Τα οφέλη των Δημοσίων Οργανισμών από μία τέτοια υποδομή είναι σημαντικά [74]:

- Γρηγορότερη απόκριση για κρίσιμες επικοινωνίες.
- Μείωση κόστους και υψηλή αποδοτικότητα στη λειτουργία των Υπηρεσιών.
- Ισχυρότερη ασφάλεια και καλύτερη διαχείριση «απειλών».
- Μειωμένος χρόνος ανάπτυξης των επιμέρους Πληροφ. Συστημάτων.

Απαραίτητη προϋπόθεση για τη λειτουργία των *Federated Identity Management* λύσεων είναι η σύσταση «έμπιστων» συνδέσμων μεταξύ των Δημ. Οργανισμών έτσι ώστε τα δεδομένα ταυτότητας που δέχεται ο ένας Οργανισμός από τον άλλο να θεωρούνται έγκυρα υπό ορισμένες προϋποθέσεις (*Circle of Trust*). Η επόμενη βασική προϋπόθεση είναι η τυποποίηση (*standards*) στις διεπαφές μεταξύ των Οργανισμών, ώστε να επιτυγχάνεται η «ηλεκτρονική συνομιλία» τους και η ασφαλής ανταλλαγή δεδομένων ταυτοτήτων [36, 74].

Γενικά, η επίτευξη της ηλεκτρονικής συνένωσης Δημ. Οργανισμών στον τομέα των ταυτοτήτων χρηστών είναι ένα σύνθετο ζήτημα που περιλαμβάνει ενέργειες στον τεχνολογικό και διοικητικό τομέα. Μία σχηματική αναπαράσταση του πολυδιάστατου χαρακτήρα της οικοδόμησης «εμπιστοσύνης» μεταξύ Οργανισμών φαίνεται στην παρακάτω Εικόνα:

Πηγή: [36]



Εικόνα 55: Συνιστώσες ενός Μοντέλου «Έμπιστων» Συνεργασιών μεταξύ Δημ. Οργανισμών

Οι εικονιζόμενες συνιστώσες διακρίνονται σε δύο μεγάλους χώρους, τον Τεχνολογικό και αυτόν της Πολιτικής. Καθεμία από τις απεικονιζόμενες παραμέτρους πρέπει να έχει συγκεκριμένες προδιαγραφές έτσι ώστε η συντονισμένη λειτουργία τους να εξασφαλίζει την επιθυμητή «εμπιστοσύνη» μεταξύ Οργανισμών. Όσα ζητήματα άπτονται της Πολιτικής πρέπει να καθορίζονται με το ανάλογο Νομικό Πλαίσιο, με επιχειρηματικούς κανόνες (καθορισμός ρόλων, υποχρεώσεων των μελών, ισχύς των «πιστοποιητικών», ενδεχόμενα κόστη συμμετοχής κλπ), με κανονισμούς λειτουργίας, με συμφωνίες μεταξύ χρηστών και των υπηρεσιών εγγραφής τους. Στο τεχνολογικό τμήμα, κάποιες απαιτήσεις ικανοποιούνται από την υποδομή του συστήματος (πχ *Security Model*) και κάποιες άλλες από την υλοποίηση των συναλλαγών (πχ *Assurance Model*) [36].

Στα καθαρά τεχνολογικά ζητήματα της υλοποίησης *Federated* ταυτοτήτων προτείνονται γενικά δύο αντιμετωπίσεις [36]:

- Η οικοδόμηση υποδομής PKI βασισμένης σε κοινώς συμφωνημένα πρότυπα, ώστε τα χρησιμοποιούμενα «ψηφιακά πιστοποιητικά» να είναι μεταφέρσιμα. Η συγκεκριμένη λύση απαιτεί τη συγκρότηση δικτύων από ιεραρχίες *CA's* ώστε τα πιστοποιητικά του *CA* ενός Οργανισμού να είναι επίσης έμπιστα και από τους *CA* των υπολοίπων Οργανισμών.

- Η εφαρμογή αρχιτεκτονικών *Redirection/Assertion* όπως των *Profiles* της *SAML* με τις οποίες το αίτημα για αυθεντικοποίηση ενός χρήστη σε μία ηλεκτρονική υπηρεσία ανακατευθύνεται στον Οργανισμό που διαθέτει τα στοιχεία ταυτότητάς του, ο οποίος και επιστρέφει στην υπηρεσία μία βεβαίωση για την εγκυρότητα της ταυτότητας του χρήστη.

Στις επόμενες παραγράφους παρουσιάζονται οι τρόποι που αντιμετωπίστηκαν τα συγκεκριμένα τεχνολογικά προβλήματα για την επίτευξη υποδομών *Federated Identity Management* στις Η.Π.Α. και την Ευρώπη.

3.3.2 Μελέτες Περιπτώσεων στο Διεθνή Δημόσιο Τομέα

Προκειμένου να αποσαφηνιστούν τα θέματα θεωρητικής και διοικητικής προσέγγισης της Διαχείρισης Ταυτοτήτων (και ειδικότερα της αυθεντικοποίησης) σε συστήματα δικτυακών υπηρεσιών Δημοσίων Οργανισμών θα παρουσιαστούν στοιχεία εφαρμογής τους σε πραγματικά έργα αναπτυγμένων χωρών στα θέματα e-Government. Πολλά από τα κοινά στοιχεία υποδομής, γενικών χαρακτηριστικών και απαιτήσεων των συγκεκριμένων έργων παρουσιάζονται ανωτέρω συγκεντρωμένα, επομένως στη συνέχεια αναφέρονται οι τομείς διαφοροποίησής τους και οι τρόποι ικανοποίησης των απαιτήσεων στην πράξη. Τα επιλεγμένα έργα περιλαμβάνουν πλούσιο υπόβαθρο σε τεκμηριωτικό – μελετητικό υλικό και είναι περισσότερο συναφή με το εύρος των θεμάτων της παρούσας εργασίας. Εκτός από τις παρουσιαζόμενες περιπτώσεις υπάρχουν πολλά e-Government έργα σε εξέλιξη που περιλαμβάνουν θέματα αυθεντικοποίησης και διαχείρισης ταυτοτήτων για πρόσβαση σε Δημόσιες, ηλεκτρονικές υπηρεσίες και παρουσιάζουν πολλά κοινά στοιχεία.. Χαρακτηριστικά παραδείγματα αποτελούν τα έργα της Δανίας (*Federated Identity and Access Management in the Danish Public Sector* [109] και της Νορβηγίας (*MyPage*) [98].

3.3.2.1 "E-Authentication" Initiative (U.S.A. General Services Administration)

Η πρωτοβουλία *E-Authentication* αποτελεί μία από τις 25 συγκεκριμένες πρωτοβουλίες υλοποίησης έργων e-Government που αναγνωρίστηκαν το 2001 από την υπηρεσία *Office of Management and Budget* (*OMB*) της κυβέρνησης των Η.Π.Α. υπό την αιγίδα του ίδιου του Προέδρου των Η.Π.Α. Τα 24 έργα χωρίστηκαν στις κατηγορίες [144]:

- *Government to Citizen*: On-line πληροφορίες και υπηρεσίες στους πολίτες ("*GovBenefits.gov*", "*Recreation One-Stop*", "*IRS Free File*", "*GovLoans.gov*", "*USA Services*").

- *Government to Business*: Αποδοτική εξυπηρέτηση των επιχειρήσεων από την Ομοσπονδιακή Κυβέρνηση ("*E-Rulemaking*", "*Expanding Electronic Tax Products For Businesses*", "*Federal Asset Sales*", "*International Trade Process Streamlining*", "*Business Gateway*", "*Consolidated Health Informatics*").

- *Government to Government*: Οικοδόμηση συνεργασιών μεταξύ διαφορετικών επιπέδων της Κυβέρνησης ("*Geospatial One-Stop*", "*Disaster Management*", "*SAFECOM*", "*E-Vital*", "*Grants.gov*").

- *Internal Efficiency & Effectiveness*: Εφαρμογή των βέλτιστων πρακτικών του χώρου της Πληροφορικής στην Κυβέρνηση ("*E-Training*", "*Recruitment One-Stop*", "*Enterprise HR Integration*", "*E-Clearance*", "*E-Payroll*", "*E-Gov Travel*", "*Integrated Acquisition Environment*", "*E-Records Management*").

Το *E-Authentication* αντιμετωπίστηκε ως μία ξεχωριστή κατηγορία έργου, καθώς οι κύριοι στόχοι του ήταν [144]:

- Η συγκρότηση έμπιστης, ασφαλούς και βασισμένης σε αναγνωρισμένα πρότυπα αρχιτεκτονικής αυθεντικοποίησης για την υποστήριξη όλων των e-Government εφαρμογών της Ομοσπονδιακής Κυβέρνησης. Η καθεμία εφαρμογή δε θα πρέπει να ασχολείται με θέματα

διαχείρισης των χρηστών της, γιατί η υπηρεσία *E-Authentication* θα αναλάβει την οικοδόμηση ομοιόμορφων λύσεων και διαδικασιών για την απόδοση και στη συνέχεια επιβεβαίωση των ηλεκτρονικών ταυτοτήτων χρηστών. Με αυτό τον τρόπο θα εξοικονομηθεί χρόνος ανάπτυξης των υπολοίπων έργων, αλλά και θα αξιοποιηθούν καλύτερα πόροι που χρησιμοποιούνταν από τα επιμέρους έργα για την υλοποίηση τέτοιων συστημάτων.

- Η προσφορά προς τους πολίτες και τις επιχειρήσεις ομοιόμορφων και μοναδικών μεθόδων αυθεντικοποίησής τους σε όλες τις ηλεκτρονικές, Κρατικές υπηρεσίες χωρίς να απαιτείται η διατήρηση πολλαπλών μεθόδων και πληροφοριών για την απόδειξη της ταυτότητάς τους στις διαφορετικές υπηρεσίες.

Το έργο *E-Authentication* αποτελεί μέρος ενός ευρύτερου πλαισίου e-Government πολιτικών και τεχνολογιών που καθόρισαν το απαραίτητο υπόβαθρο τεχνικών και διοικητικών λεπτομερειών του έργου. Επομένως, το *E-Authentication* περιλαμβάνει ένα σύνολο προδιαγραφών που καλύπτουν τις περιοχές [138]:

- *Πολιτική*: Περιλαμβάνει τον καθορισμό των θεμελιωδών αρχών λειτουργίας του έργου και των βασικών προτύπων στα οποία θα στηριχθεί το Τεχνολογικό υπόβαθρο της υλοποίησής του.

- *Τεχνολογία*: Αφορά τον καθορισμό των προτύπων που θα εφαρμοστούν, την ακριβή αρχιτεκτονική των υπο-συστημάτων και τις συστάσεις υλοποίησης της περιγραφόμενης αρχιτεκτονικής.

- *Διαχείριση «Πιστοποιητικών»*: Περιλαμβάνει τον καθορισμό των απαιτούμενων προδιαγραφών των ψηφιακών «πιστοποιητικών» που θα χρησιμοποιηθούν στο σύστημα.

- *Ενσωμάτωση των Δικτυακών Εφαρμογών*: Περιλαμβάνει τη διατύπωση των πρακτικών οδηγιών ενσωμάτωσης του *E-Authentication* στις πραγματικές εφαρμογές των Κρατικών Οργανισμών και τις απαραίτητες προϋποθέσεις που πρέπει αυτές να τηρούν ώστε να είναι η ενσωμάτωση επιτυχής.

- *Γραφείο Διοίκησης Προγράμματος*: Είναι η αρμόδια Υπηρεσία διαχείρισης του έργου η οποία οργανώνει όλες τις παραπάνω προδιαγραφές και συντονίζει τις φάσεις του.

Η βασική έννοια που διέπει την ανάπτυξη του *E-Authentication* είναι η «έμπιστη» σχέση (*Trust*) μεταξύ οντοτήτων που συμμετέχουν στο έργο έτσι ώστε να γίνεται μεταξύ τους ασφαλής, κατανεμημένη αυθεντικοποίηση των «πιστοποιητικών» που διαθέτουν, αφού δεν υφίσταται η έννοια μίας κεντρικής αρχής διατήρησης «πιστοποιητικών» και ελέγχου της αυθεντικότητάς τους για το σύνολο των Κρατικών Υπηρεσιών. Ο σκοπό του έργου είναι η διασπορά και των διαδικασιών έκδοσης και ελέγχου των ψηφιακών «πιστοποιητικών» ακόμα και σε οργανισμούς του Ιδιωτικού Τομέα, εφόσον όμως αυτοί τηρούν το αυστηρό νομικό και τεχνολογικό πλαίσιο που διατυπώνεται ως υπόβαθρο του έργου. Τα βήματα που ακολουθήθηκαν για τη διαμόρφωση αυτού του υπόβαθρου είναι [138]:

1. *Καθορισμός των κινδύνων του E-Authentication και των Επιπέδων Διασφάλισης για όλη τη Δημ. Διοίκηση*. Υλοποιήθηκε μέσω της σύστασης Ομοσπονδιακής Πολιτικής "*M-04-04/16-12-2003*" της Υπηρεσίας *Office of Management and Budget* της Γραμματείας του Προέδρου των Η.Π.Α. προς όλες τις Ομοσπονδιακές υπηρεσίες [143].

2. *Καθορισμός Πρότυπης Μεθοδολογίας για την εκτίμηση των κινδύνων του E-Authentication*. Περιλαμβάνει την ανάλυση από την πλευρά καθεμιά Δημ. Υπηρεσίας όλων των εφαρμογών που προβάλουν στο Internet, το είδος των δεδομένων που διακινούνται (τόσο σε όγκο όσο και σε σημαντικότητα), πόσοι χρήστες προσπελαύνουν τις εφαρμογές κλπ, ώστε να αναγνωριστούν οι πιθανοί κίνδυνοι της αυθεντικοποίησης και να προσδιοριστεί το απαιτούμενο *Επίπεδο Διασφάλισης*. Η Διοίκηση του *E-Authentication* σε συνεργασία με το Παν/μιο Carnegie Mellon ανέπτυξε ένα εργαλείο υλοποίησης της μεθοδολογίας αναγνώρισης των «κινδύνων» με βάση χαρακτηριστικά των εξεταζόμενων δικτυακών εφαρμογών το οποίο ονόμασε "*Electronic Risk and Requirements Assessment* (*e-RA*)" και το οποίο διατίθεται ελεύθερα στις Υπηρεσίες που επιθυμούν να εκτιμήσουν τις «απειλές» των δικών τους εφαρμογών σύμφωνα με τις προδιαγραφές του σταδίου 1 [139].

3. *Καθορισμός των τεχνολογιών αυθεντικοποίησης και ηλεκτρονικών «πιστοποιητικών» για τα Επίπεδα Διασφάλισης*. Υλοποιήθηκε μέσω της Τεχνικής Οδηγίας "*Special Pub 800-63*" του οργανισμού *National Institute of Standards and Technology – NIST* [93].

4. *Καθορισμός μεθοδολογίας για την εξέταση των Παρόχων ψηφιακών «Πιστοποιητικών» (Credential Providers) με βάση τα θεσμοθετημένα κριτήρια Διασφάλισης*. Αποτελεί το γενικότερο πλαίσιο ελέγχων και αξιολόγησης των οργανισμών που αιτούνται να αναλάβουν το ρόλο του «*Παρόχου Υπηρεσιών Πιστοποιητικών*» (*Credential Service Provider – CSP*) για την αυθεντικοποίηση στα πλαίσια του έργου *E-Authentication*. Συνεπώς, έχει αναπτυχθεί ένα ευρύτερο «*Πλαίσιο Αξιολόγησης Πιστοποιητικών*» (*Credential Assessment Framework – CAF*) το οποίο περιλαμβάνει κατηγοριοποιήσεις των κριτηρίων αξιολόγησης ανά είδος «πιστοποιητικού» που πιθανώς παρέχει ο εξεταζόμενος Πάροχος (password, PKI κα) οι οποίες ονομάζονται *Credential Assessment Profiles – CAPS* καθώς και περιγραφές δομημένων διαδικασιών τέλεσης των αξιολογήσεων των *CSPs*. Οι CSPs αξιολογούνται τόσο οι ίδιοι ως οργανισμοί όσο και οι διαδικασίες σχετικά με τα «πιστοποιητικά» που διαχειρίζονται. Το συγκεκριμένο στάδιο είναι ιδιαίτερα κρίσιμο καθώς εντάσσει έναν *CSP* στο δίκτυο «εμπιστοσύνης» του *E-Authentication* και όλοι οι υπόλοιποι οργανισμού θα εμπιστεύονται τα «πιστοποιητικά» και τις διαδικασίες του [140].

5. *Καθορισμός της λίστας των «έμπιστων» Οργανισμών CSP για χρήση τους από όλο το Δημόσιο και Ιδιωτικό Τομέα.* Στις 31/12/2006 η συγκεκριμένη λίστα περιείχε έξι Οργανισμούς *CSP*, μεταξύ των οποίων και ιδιωτικοί Οργανισμοί.

6. *Καθορισμός κοινών επιχειρηματικών κανόνων για τη χρήση των «πιστοποιητικών» που προέρχονται από «έμπιστους» τρίτους*. Ενδεικτικό παράδειγμα καταγραφής λειτουργικών και επιχειρηματικών κανόνων είναι το προσωρινό Νομικό Πλαίσιο που περιγράφεται στο [31].

Μία σχηματική αναπαράσταση των δομικών συστατικών του συνολικού πλαισίου του έργου *E-Authentication* φαίνεται ως πυραμίδα στην Εικόνα 56, όπου ειδικά οι τεχνικές προδιαγραφές που αφορούν το συγκεκριμένο έργο καταλαμβάνουν ποσοστό λιγότερο από το μισό. Αντίθετα, είναι διευρυμένος ο ρόλος των θεμάτων διατύπωσης και οργάνωσης των θεμελιωδών προδιαγραφών τεχνολογιών αυθεντικοποίησης, των «πιστοποιητικών», της εκτίμησης των κινδύνων, του νομικού και θεσμικού πλαισίου υλοποίησης των «έμπιστων» σχέσεων μεταξύ των Δημ. Οργανισμών.

Η τεχνολογική προσέγγιση του έργου ακολούθησε τους υψηλούς στόχους που τέθηκαν από το *Στρατηγικό Επιχειρηματικό Σχέδιο* (*Strategic Business Plan*) και τις θεμελιώδεις προδιαγραφές και είχε ως σκοπό την ικανοποίηση των απαιτήσεων [32]:

- *Ισχύς (Leverage)*: Το «πιστοποιητικό» από οποιαδήποτε εγκεκριμένη υπηρεσία έκδοσης ηλεκτρονικών «πιστοποιητικών» (*Credential Service – CS*) θα μπορεί να χρησιμοποιηθεί για την πρόσβαση του χρήστη σε κάθε δικτυακή εφαρμογή με ίδιο ή μικρότερο απαιτούμενο *Επίπεδο Διασφάλισης*. Κάθε νέα εφαρμογή Δημ. Υπηρεσίας (*Agency Application – AA*) πρέπει να αποδέχεται τα υπάρχοντα «πιστοποιητικά» των χρηστών, αντί να απαιτεί την «έκδοση» καινούριων.

- *Single Sign-on*: Μόλις ο χρήστης αυθεντικοποιηθεί από μία εφαρμογή θα μπορεί να μετακινείται σε μία άλλη με ίδιο ή μικρότερο απαιτούμενο *Επίπεδο Διασφάλισης* χωρίς να επαναλάβει τη διαδικασία αυθεντικοποίησης.

- *Εμπιστευτικότητα (Privacy)*: Δε θα υπάρχει κεντρική καταγραφή των ενεργειών εισόδου – εξόδου των χρηστών και δε θα υπάρχει κεντρικό σύστημα αυθεντικοποίησης. Τα «πιστοποιητικά» των χρηστών θα μπορούν να «μεταφέρονται» μεταξύ διαφορετικών οργανισμών (*Federated Identity*).

- *Διοίκηση (Governance)*: Το πλαίσιο της αρχιτεκτονικής πρέπει να εξασφαλίζει σαφή έλεγχο στις εφαρμογές και τις *CS* που θα συμμετέχουν στο δίκτυο του έργου *E-Authentication*.

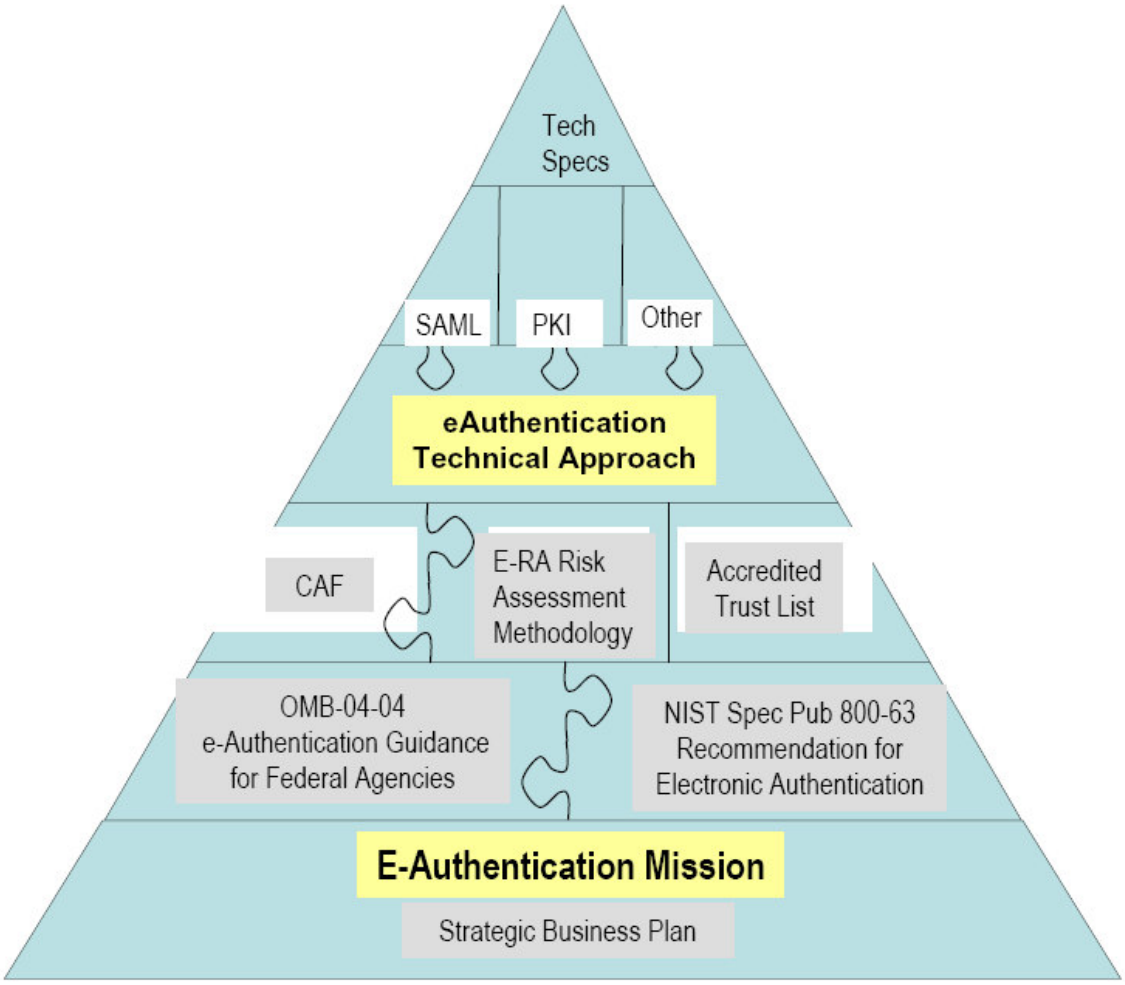
- *Πρότυπα (Standards)*: Το πλαίσιο της αρχιτεκτονικής πρέπει να βασίζεται σε υπάρχοντα πρότυπα της αγοράς και να είναι σε συνεχή παρακολούθηση των ανερχόμενων προτύπων.

- *Εμπορικά Προϊόντα (Commercial off the Shelf – COTS)*: Η αρχιτεκτονική πρέπει να ενσωματώνει εμπορικά προϊόντα, όπου είναι πιθανό.

- *Διάρκεια (Durability)*: Η αρχιτεκτονική θα πρέπει να σχεδιαστεί ώστε να επιτρέπει την τεχνολογική εξέλιξη εξασφαλίζοντας την εύκολη ενσωμάτωση των εξελίξεων.

- *Flexibility*: Η αρχιτεκτονική δε θα πρέπει να βασίζεται σε κάποιο συγκεκριμένο μόνο πρότυπο, προϊόν ή κατασκευαστή.

Πηγή: [138]



Εικόνα 56: Θεμελιώδη Δομικά Τμήματα του *E-Authentication*

Το βασικό πλαίσιο αρχιτεκτονικής του *E-Authentication* βασίζεται στη χρήση δύο σχημάτων αυθεντικοποίησης: της *Βασισμένης σε Βεβαιώσεις Ταυτότητας* (*Assertion – based authentication*) και της *Βασισμένης σε Ψηφιακά «Πιστοποιητικά»* (*Certificate – based authentication*). Το *Assertion – based* σχήμα αυθεντικοποίησης προτείνεται για υπηρεσίες όπου τα επιθυμητά *Επίπεδα Διασφάλισης* είναι χαμηλά (Επίπεδα 1 & 2), ενώ το *Certificate – based* σχήμα εφαρμόζεται σε υπηρεσίες υψηλής απαιτούμενης *Διασφάλισης* (*Επίπεδα* 3 & 4). Η διατύπωση της αρχιτεκτονικής του *E-Authentication* βασίζεται στην εξέταση σε ανώτερο επίπεδο συγκεκριμένων «σεναρίων» *Federated Identity Management* μεταξύ των βασικών οντοτήτων του έργου [32]:

- *Agency Application – AA*: Είναι οι δικτυακές εφαρμογές των Κρατικών Υπηρεσιών τις οποίες θα προσπελαύνουν μέσω του Internet οι πολίτες. Καθώς το *E-Authentication* αφορά μόνο υπηρεσίες αυθεντικοποίησης, οι εφαρμογές θα πρέπει να φροντίσουν μόνες τους για τον έλεγχο πρόσβασης και την εξουσιοδότηση (*authorization*) των χρηστών.

- *Credential Services – CS*: Είναι υπηρεσίες που προσφέρουν στους τελικούς χρήστες με τα απαραίτητα «πιστοποιητικά» την απαραίτητη έγκριση για την πρόσβαση των *AAs* του δικτύου *E-Authentication* και παρέχονται από τους οργανισμούς *Credential Service Providers – CSP* (Δημόσιοι ή Ιδιωτικοί οργανισμοί παροχής «πιστοποιητικών»).

- *E-Authentication Portal (Portal)*: Είναι το κεντρικό Portal αναφοράς του δικτύου που καλύπτει το *E-Authentication* μέσα από το οποίο ένας χρήστης μπορεί να εντοπίσει τις επιθυμητές *CSs* και *AAs* για την ολοκλήρωση των συναλλαγών τους.

- *End Users*: Κάθε πολίτης, κυβερνητικός υπάλληλος, συμβασιούχος ή ιδιωτική επιχείρηση που επιθυμεί να εισέλθει σε μία *AA* χρησιμοποιώντας το «πιστοποιητικό» που έχει παραλάβει από μία *CS* με τον απλούστερο δυνατό τρόπο.

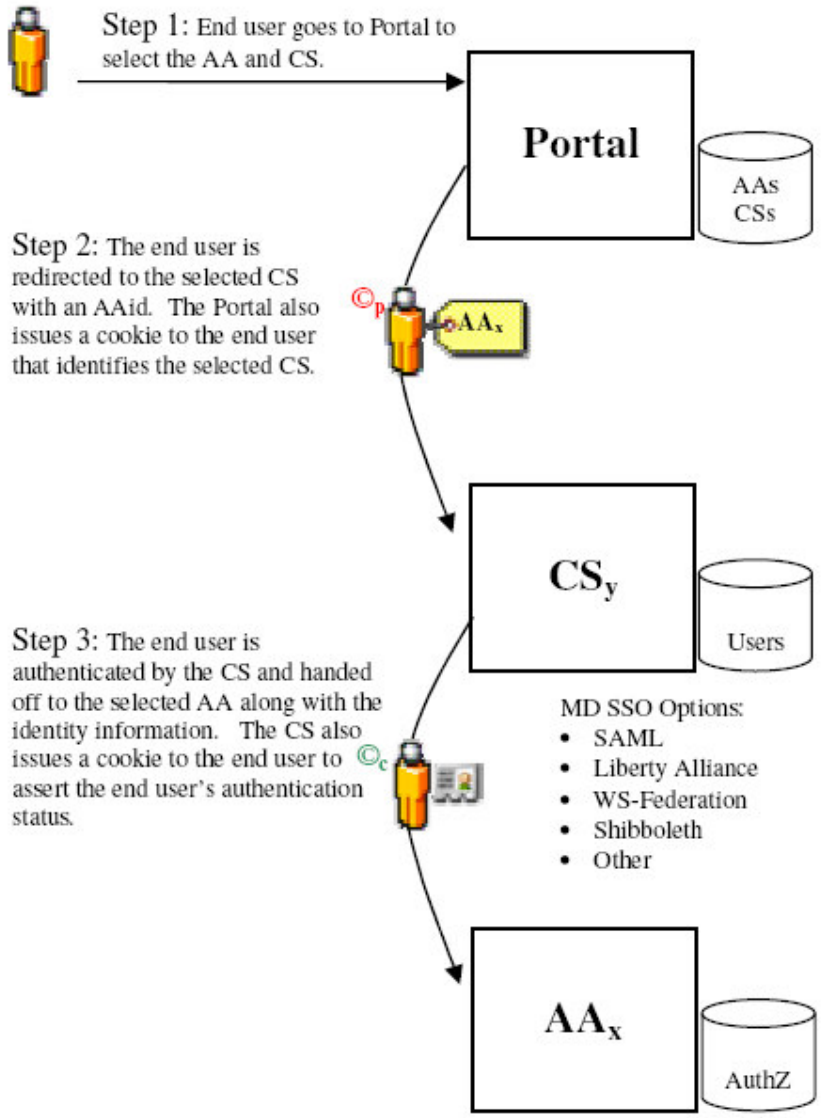
Για την *Assertion – based* αυθεντικοποίηση το βασικό «σενάριο» που υλοποιεί η αρχιτεκτονική του *E-Authentication* είναι (βλ. επόμενη Εικόνα) [32]:

1. *Βήμα 1*: Ο *End – User* συνδέεται στο *Portal* του *E-Authentication* ώστε να επιλέξει την δικτυακή υπηρεσία (*AA*) που επιθυμεί να προσπελάσει και την υπηρεσία που του εξέδωσε το «πιστοποιητικό» (*CS*).

2. *Βήμα 2*: Ο *End – User* ανακατευθύνεται από το *Portal* στην επιλεγμένη *CS* μαζί με τον κωδικό της επιθυμητής *AA*, ενώ παράλληλα δημιουργείται ένα Cookie στον *End – User* όπου αποθηκεύεται η επιλεγμένη *CS* (*Portal Cookie*), ώστε να εξασφαλιστεί το SSO κατά την πρόσβαση του *End – User* σε διαφορετική υπηρεσία.

3. *Βήμα 3*: Ο *End – User* καλείται να καταχωρήσει τα στοιχεία ταυτότητάς του (συνήθως PIN ή password) στην επιλεγμένη *CS* η οποία και εκτελεί τον καθαυτό έλεγχο εγκυρότητας και την αυθεντικοποίηση. Στη συνέχεια η *CS* δημιουργεί το απαραίτητο *Assertion* της ταυτότητας του *End – User* και μεταφέρει τον έλεγχο στην επιθυμητή *AA* μαζί με το συγκεκριμένο *Assertion*. Ταυτόχρονα, δημιουργείται στον *End – User* ένα Cookie με τις πληροφορίες αυθεντικοποίησής του (*CS Cookie*).

Πηγή: [32]

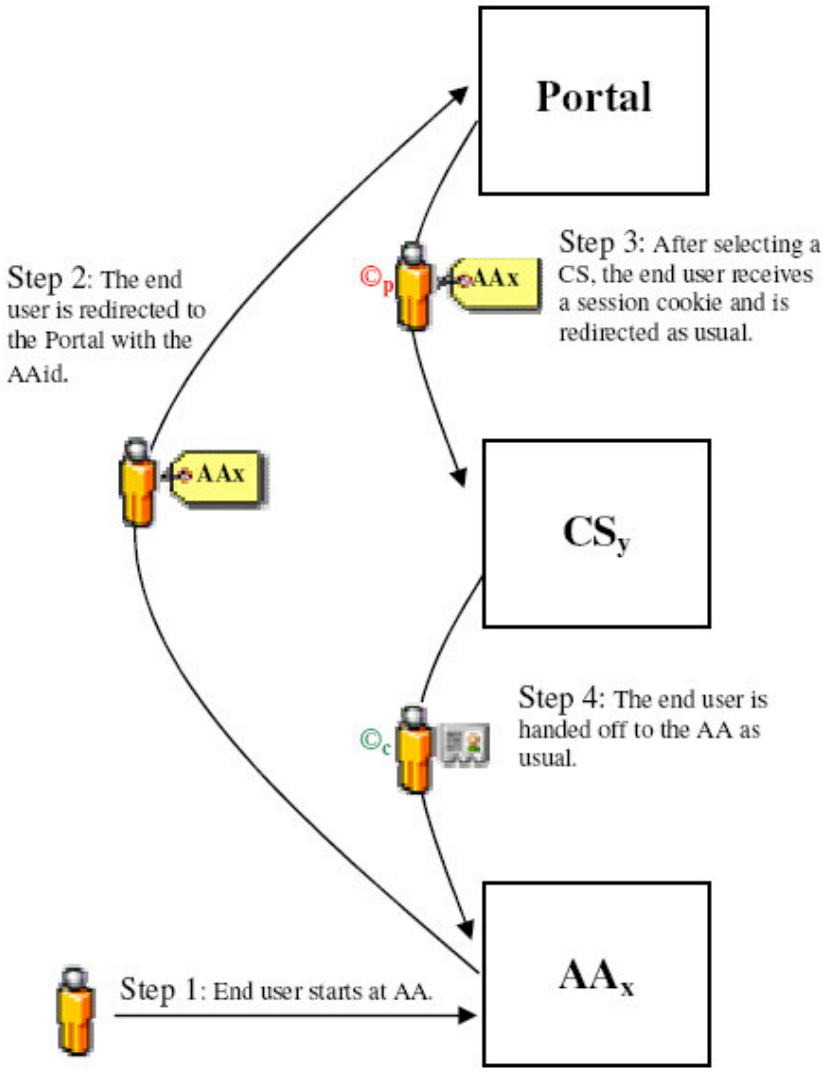


Εικόνα 57: Βασικό «Σενάριο» της *Assertion-based* αυθεντικοποίησης του *E-Authentication*

Η αρχιτεκτονική του *E-Authentication* προβλέπει δύο παραλλαγές του παραπάνω βασικού «σεναρίου»: ο *End – User* ξεκινάει τη συναλλαγή απευθείας στην *AA* ή ο *End – User* ξεκινάει τη συναλλαγή απευθείας στην *CS*. Στην πρώτη περίπτωση (βλ. επόμενη Εικόνα) ο χρήστης ανακατευθύνεται από την *AA* στο *E-Authentication Portal* έχοντας δεδομένο τον κωδικό της *AA*. Αυτό που δεν είναι γνωστό είναι η *CS* που είναι εγγεγραμμένος ο *End – User*. Το *Portal* αναζητά πιθανή ύπαρξη του *Portal Cookie* στον *End – User* από το οποίο εντοπίζει τον κατάλληλο *CS* από προηγούμενη αυθεντικοποίηση, επομένως, συνδέει κατευθείαν το χρήστη στην ίδια *CS*. Στην περίπτωση όπου δεν υπάρχει *CS Cookie*, το *Portal* εμφανίζει στον *End – User* σχετική φόρμα επιλογής *CS*. Ο *End – User* «μεταφέρεται» στην επιλεγμένη *CS* η οποία εξετάζει την ύπαρξη *CS Cookie*. Εφόσον αυτό έχει δημιουργηθεί από προηγούμενη αυθεντικοποίηση του *End – User* και το *Επίπεδο Διασφάλισης* της προηγούμενης αυθεντικοποίησης

είναι συμβατό με το τρέχον, η *CS* διαβάζει τα απαραίτητα στοιχεία και ανακατευθύνει απευθείας τον *End – User* στην αρχική *AA*. Διαφορετικά, ο χρήστης καλείται να εισάγει τα στοιχεία ταυτότητάς του και εφόσον αυθεντικοποιηθεί επιτυχώς, μεταφέρεται πίσω στην αρχική *AA*.

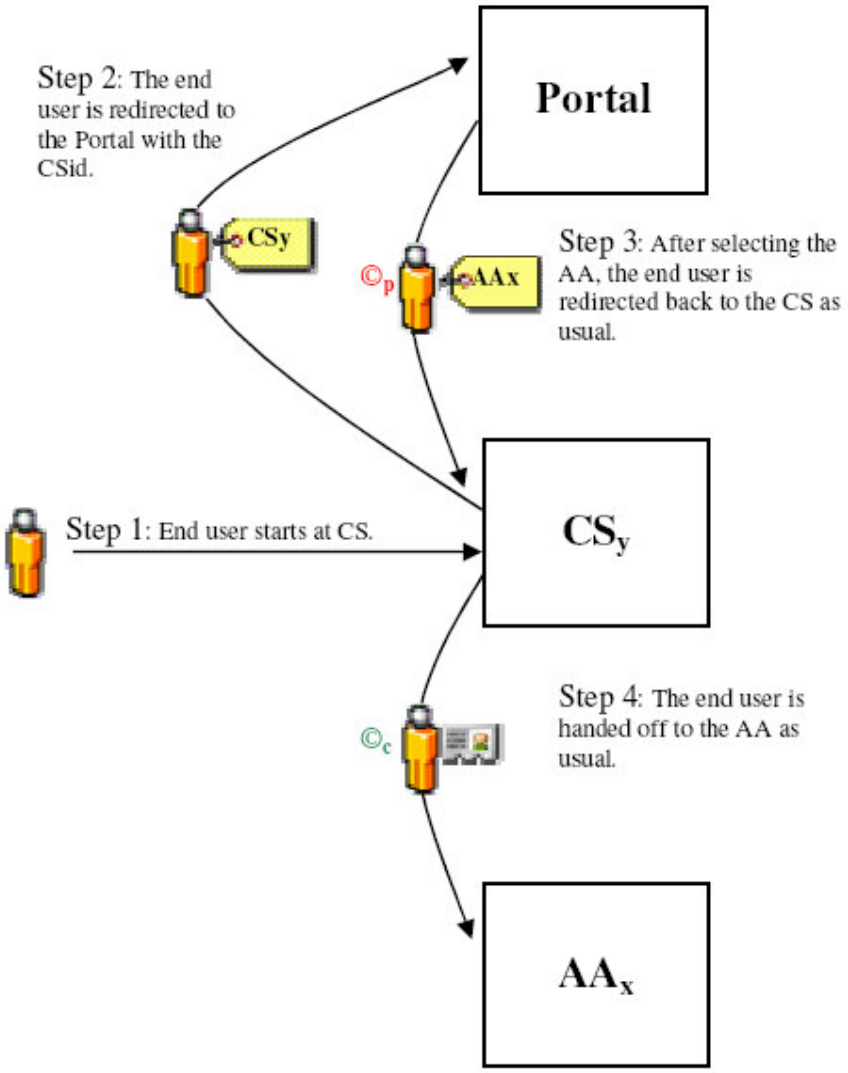
Πηγή: [32]



Εικόνα 58: «Σενάριο» Προσπέλασης της *AA* στην *Assertion-based* αυθεντικοποίηση του *E-Authentication*

Το δεύτερο «σενάριο» προβλέπει την πιθανότητα ο *End – User* να επισκεφτεί πρώτα την *CS*. Στη συγκεκριμένη περίπτωση η άγνωστη παράμετρος είναι η επιθυμητή *AA*, επομένως η *CS* ανακατευθύνει αμέσως τον *End – User* στο *Portal* όπου εκεί καλείται να επιλέξει *AA*. Στη συνέχεια ακολουθούνται τα Βήματα που προβλέπει το βασικό «σενάριο» της αρχιτεκτονικής του *E-Authentication* (βλ. επόμενη Εικόνα).

Πηγή: [32]



Εικόνα 59: «Σενάριο» Προσπέλασης της *CS* στην *Assertion-based* αυθεντικοποίηση του *E-Authentication*

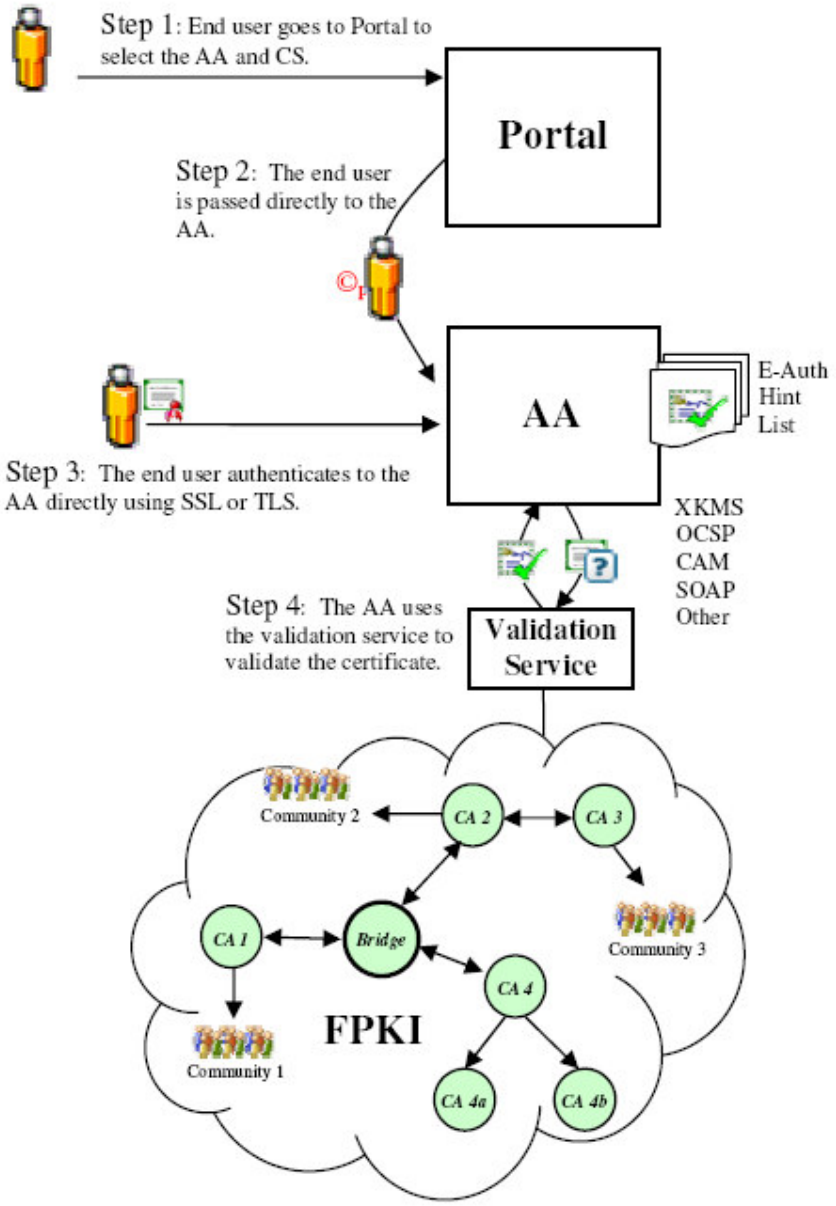
Το δεύτερο σχήμα αυθεντικοποίησης που υποστηρίζεται από το *E-Authentication* είναι το *Certificate – based* κατά το οποίο χρησιμοποιούνται ψηφιακά «πιστοποιητικά» κατά την αυθεντικοποίηση του χρήστη. Το σημαντικότερο ζήτημα στα θέματα των ψηφιακών «πιστοποιητικών» είναι οι προδιαγραφές και οι διαδικασίες έκδοσής τους, καθώς και η διαλειτουργικότητά τους όταν χρησιμοποιούνται για την πολλαπλή πρόσβαση σε όλες τις δικτυακές υπηρεσίες του Δημ. Τομέα. Στο θέμα των προδιαγραφών το *E-Authentication* ακολουθεί τη συνολική κρατική πολιτική PKI, όπως καθορίζεται από τον οργανισμό *Federal Public Key Infrastructure Policy Authority – FPKIPA* [25], ενώ για το θέμα της διαλειτουργικότητας χρησιμοποιείται η υπηρεσία της *Federal Bridge Certification Authority – FBCA* με την οποία ομοιογενοποιούνται οι πολιτικές και οι διαδικασίες των *Certificate Authorities – CAs*. Η *Bridge CA* δημιουργήθηκε από την *FPKIPA* και αποσκοπεί στην εξασφάλιση της υλοποίησης συ-

ναλλαγών των Κρατικών Υπηρεσιών με άλλους Κρατικούς ή Ιδιωτικούς Οργανισμούς με τη χρήση ψηφιακών «πιστοποιητικών» και με τη συνένωση, επομένως, διαφορετικών PKI Ιεραρχιών [32].

Ο σκοπός της αρχιτεκτονικής του *E-Authentication* σε αυτό το σχήμα αυθεντικοποίησης είναι ο καθορισμός μηχανισμών ελέγχου της εγκυρότητας των «πιστοποιητικών» που παρουσιάζουν οι χρήστες, για καθένα «σενάριο» προσπέλασης των δικτακών υπηρεσιών. Το πρώτο «σενάριο» χρήσης φαίνεται στην επόμενη Εικόνα και περιλαμβάνει την ύπαρξη Υπηρεσίας Επικύρωσης (*Validation Service*) των «πιστοποιητικών». Συγκεκριμένα, ο *End – User* επισκέπτεται αρχικά το *Portal* (Βήμα 1) και αφού επιλέξει *AA* και *CS* μεταφέρεται απευθείας στην *AA* (Βήμα 2). Δεν είναι απαραίτητο το ενδιάμεσο «πέρασμα» του *End – User* από την *CS* καθώς με τη χρήση «ασφαλούς καναλιού» μέσω SSL/TLS αποστέλλεται απευθείας στον *AA* το σχετικό «πιστοποιητικό» χωρίς την εισαγωγή ευαίσθητων πληροφοριών ταυτότητας (Βήμα 3). Η *AA* με τη χρήση της *Validation Service* εξασφαλίζει την εγκυρότητα του αποστελλόμενου «πιστοποιητικού» και την αυθεντικοποίηση του χρήστη. Στη συγκεκριμένη διαδικασία υπάρχει μία σημαντική οντότητα, η επονομαζόμενη "*Hint List*" του Web Server της *AA*. Η *Hint List* είναι μία λίστα με *CA*'s των οποίων τα «πιστοποιητικά» μπορούν να είναι αποδεκτά, αλλά μόνο για την ολοκλήρωση της «ασφαλούς» επικοινωνίας μέσω SSL/TLS. Τα συγκεκριμένα πρωτόκολλα λειτουργούν με κρυπτογράφηση Δημοσίου Κλειδιού κατά την πρώτη φάση της «διαπραγμάτευσης» και τα σχετικά κλειδιά υπάρχουν σε ψηφιακά «πιστοποιητικά» υπογεγραμμένα από συγκεκριμένους, αποδεκτούς *CA's*. Αυτοί οι *CA's* είναι και το περιεχόμενο της *Hint List* και αφορά μόνο τη φάση έναρξης της επικοινωνίας μέσω SSL/TLS. Η αυθεντικοποίηση του χρήστη γίνεται με τον έλεγχο του *CA* που υπογράφει το «πιστοποιητικό» του *End – User* μέσα σε μία άλλη λίστα, την *Trust List* του Web Server. Προκειμένου να σχηματιστεί αυτή η λίστα απαιτείται η ανακάλυψη της κατάλληλης διαδρομής (*Path Discovery*) μέσα από τις ιεραρχίες των *CA's*. Ουσιαστικά αυτό υλοποιείται από τη *Validation Service* η οποία είναι κατάλληλα προγραμματισμένη ώστε να «διαπερνά» και τη γέφυρα των ιεραρχιών (*Federal Bridge CA*) και στην πράξη είναι ένα module στους Web Servers [32].

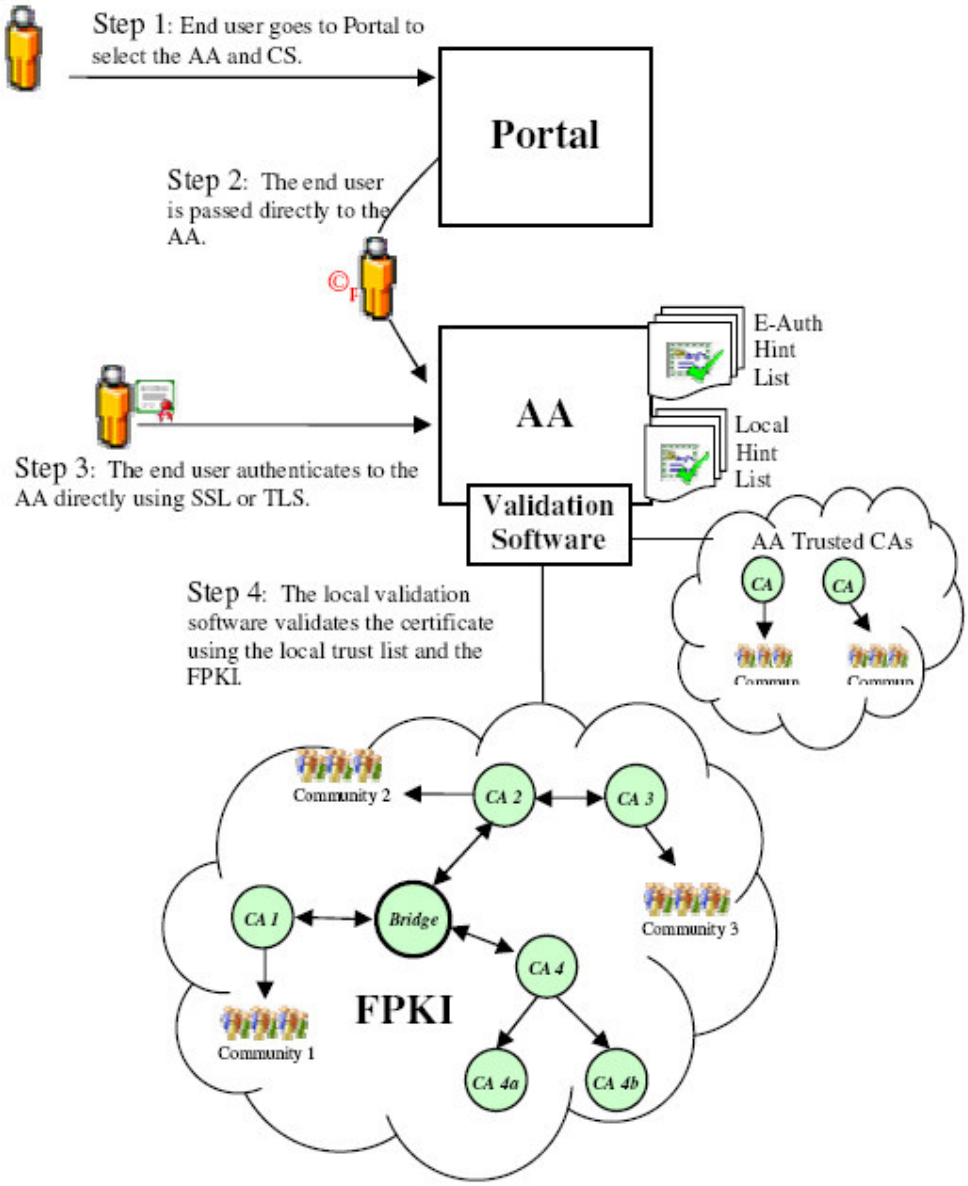
Μία παραλλαγή του παραπάνω «σεναρίου» προκύπτει όταν μία Υπηρεσία επιθυμεί να χρησιμοποιεί «πιστοποιητικά» από μία ιεραρχία *CA's* που δεν είναι εγκεκριμένες από το *Federal Bridge CA* και προτιμάται να υλοποιείται η έλεγχος εγκυρότητας των «πιστοποιητικών» από μία αποκλειστική της *Validation Service*. Σε αυτή την περίπτωση τα συγκεκριμένα *CA's* πρέπει να προστεθούν και στη *Hint List* του Web Server της *AA*, αλλά και η *Trust List* να καταρτιστεί από μία «τοπική» *Validation Service* της *AA*. Το *E-Authentication* μπορεί να προσφέρει υπηρεσίες ελέγχου του «τοπικού» λογισμικού ώστε να πληροί τις προδιαγραφές που θέτει η Αρχή *FPKI* και να προτείνει λίστα με συμβατά προϊόντα της αγοράς (βλ Εικόνα 61).

Πηγή: [32]



Εικόνα 60: «Σενάριο» Λειτουργίας *Υπηρεσίας Επικύρωσης* στην *Certificate-based* αυθεντικοποίηση του *E-Authentication*

Πηγή: [32]

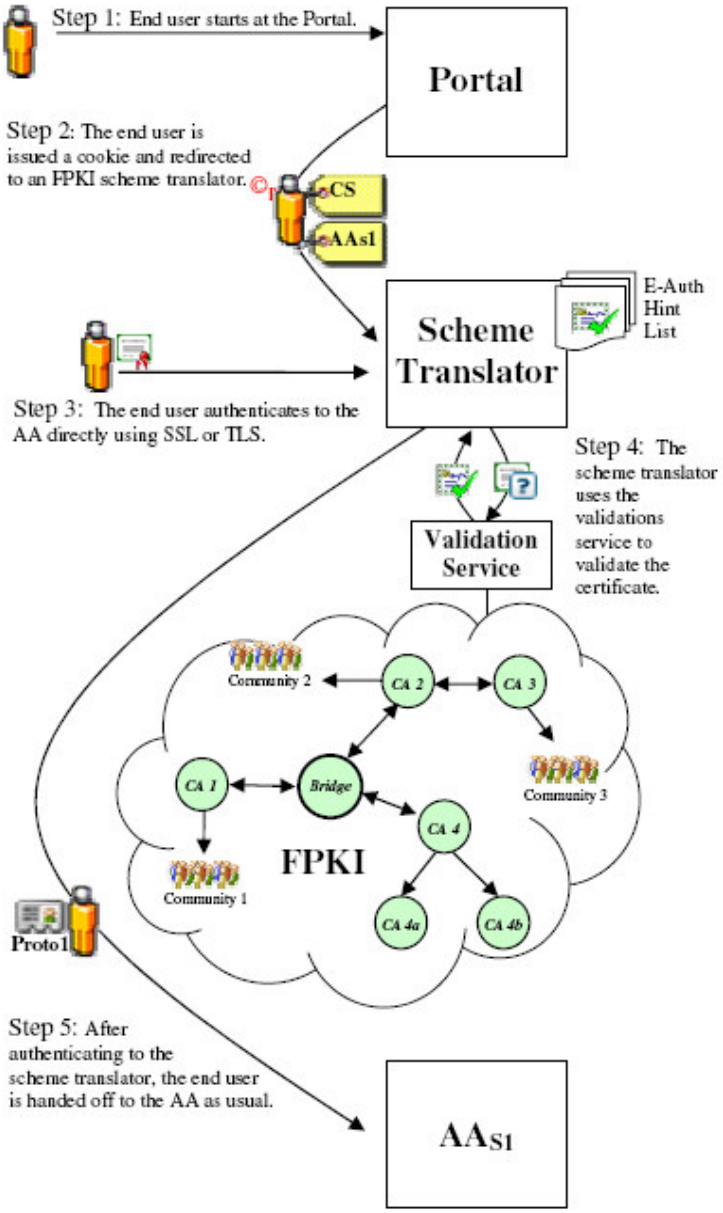


Εικόνα 61: «Σενάριο» Λειτουργίας *Τοπικής Υπηρεσίας Επικύρωσης* στην *Certificate-based* αυθεντικοποίηση του *E-Authentication*

Μία τελευταία παράμετρος που αφορά στην *Certificate – based* αυθεντικοποίηση είναι η βασική απαίτηση της αρχιτεκτονικής του *E-Authentication* για χρήση των συγκεκριμένων «πιστοποιητικών» σε *AA* με χαμηλότερο *Επίπεδο Διασφάλισης*, δηλαδή στις *AA* όπου εφαρμόζεται *Assertion – based* αυθεντικοποίηση. Η προτεινόμενη λύση είναι η ύπαρξη μίας ενδιάμεσης οντότητας, του *Μεταφραστή Σχήματος* (*Scheme Translator*) ο οποίος λειτουργεί με βάση τα πρώτα Βήματα της διαδικασίας *Certificate-based* αυθεντικοποίησης, αλλά στο τελευταίο βήμα πριν την τελική αυθεντικοποίηση στην *AA* λειτουργεί ως *CS* στο βασικό «σενάριο» της *Assertion – based* αυθεντικοποίησης (βλ επόμενη Εικόνα). Μόλις, επομένως, ο χρήστης αποστείλει το «πιστοποιητικό» του στο *Scheme Translator* (Βήμα 3), αυτός το επικυρώνει μέσω

του *Validation Service* (Βήμα 4)και στη συνέχεια δημιουργεί το κατάλληλο *Assertion* με τις πληροφορίες ταυτότητας του χρήστη, γιατί μόνο με αυτό τον τρόπο μπορεί η *AA* να κατανοήσει και αποδεχτεί την ταυτότητα του χρήστη. Συνεπώς, δεν απαιτείται καμία αλλαγή στην υλοποίηση της *AA*.

Πηγή: [32]



Εικόνα 62: *Certificated-based* αυθεντικοποίηση σε *Assertion – based* Εφαρμογές στο *E-Authentication*

Οι Κρατικές Υπηρεσίες που πρόκειται να ενταχθούν στο δίκτυο *E-Authentication* πρέπει πρωτίστως να εγκαταστήσουν ένα εμπορικό προϊόν ή μία *open – source* λύση (πχ *Shibboleth*) που να υποστηρίζει το πρωτόκολλο *SAML 1.0 Artifact Profile*, εφόσον επιθυμούν *Assertion –*

based αυθεντικοποίηση. Τα προϊόντα που μπορούν να ικανοποιήσουν τη συγκεκριμένη απαίτηση είναι ελεγμένα για τη διαλειτουργικότητά τους με την αρχιτεκτονική του *E-Authentication* και υποδεικνύονται από την αρχή διοίκησης του έργου. Στα πλαίσια της στενής παρακολούθησης των τρεχόντων προτύπων, το *E-Authentication* μελετά την υιοθέτηση και του πρωτοκόλλου *SAML 2.0*. Οι Κρατικές Υπηρεσίες που επιθυμούν να εφαρμόσουν *Certificate – based* αυθεντικοποίηση πρέπει να εγκαταστήσουν προϊόντα που υποστηρίζουν ψηφιακά «πιστοποιητικά» X.509v3, την Ομοσπονδιακή υποδομή PKI (*Federal PKI Policy Authority*) και τα πρωτόκολλα αναζήτησης και έγκρισης των «πιστοποιητικών» (*Path Discovery and Validation*). Τα προϊόντα που ικανοποιούν αυτές τις απαιτήσεις είναι επίσης ελεγμένα και δημοσιευμένα από την αρχή διοίκησης του έργου. Σχετικά με την αποδοχή και εφαρμογή της υπηρεσίες *E-Authentication*, στις 04/10/2006 περίπου 17 Κρατικές Υπηρεσίες έχουν ενσωματώσει δικτυακές εφαρμογές τους στο δίκτυο αυθεντικοποίησης του *E-Authentication*, ενώ 6 οργανισμοί (Δημόσιοι και Ιδιωτικοί) έχουν αναλάβει και το ρόλο του *Credential Service Provider – CSP* [33].

3.3.2.2 Government "Gateway" (U.K. Government)

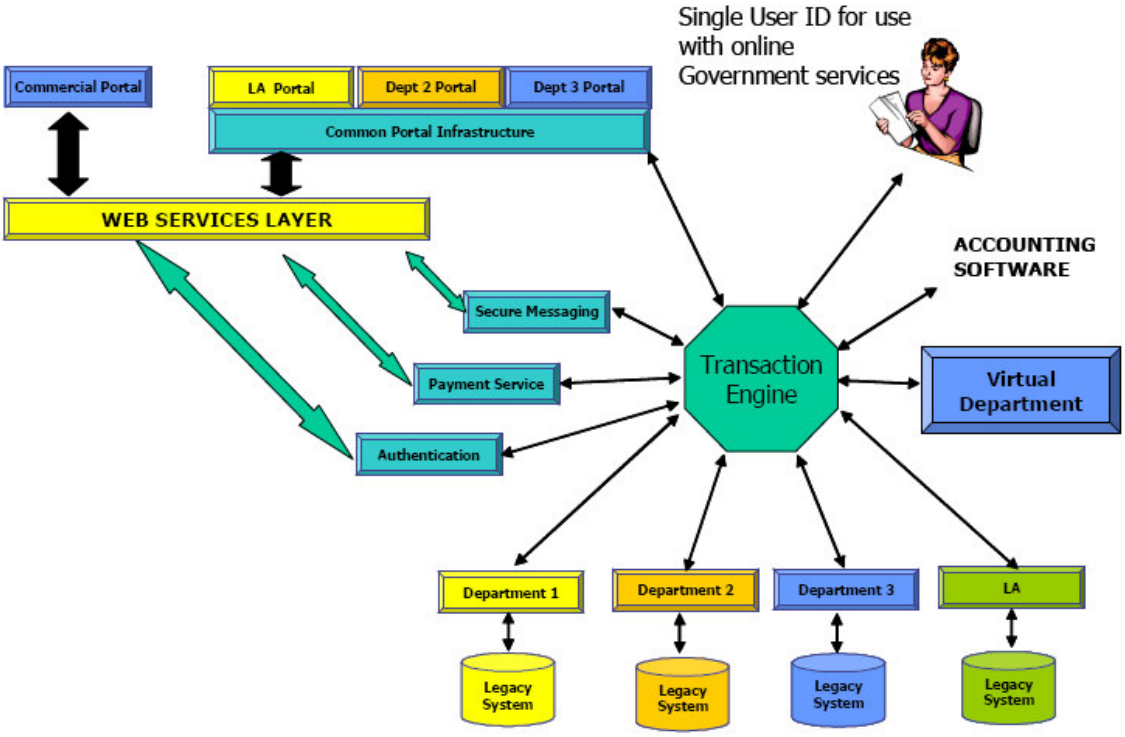
Το έργο *Government "Gateway"* αποτελεί την κεντρική υπηρεσία εγγραφής και ελέγχου πρόσβασης χρηστών στις on-line, δικτυακές υπηρεσίες του Δημόσιου Τομέα του Ηνωμένου Βασιλείου (United Kingdom). Το έργο υλοποιείται από την ομάδα *e-Delivery Team* (*EDT*) για λογαριασμό της Κυβέρνησης του Η.Β. και ξεκίνησε τη λειτουργία του το 2001, στα πλαίσια ευρύτερης πολιτικής εκσυγχρονισμού του Δημόσιου Τομέα και υλοποίησης έργων e-Government για την ηλεκτρονική παροχή υπηρεσιών από την πλευρά του Δημοσίου. Από την έναρξη του έργου έχουν προστεθεί πολλές υπηρεσίες και νέες τεχνολογίες, έτσι ώστε σήμερα το *Gateway* να συνίσταται από ένα σύνολο θεμελιωδών υπηρεσιών προς το σκοπό της ανάπτυξης δημόσιων ηλεκτρονικών υπηρεσιών με ασφαλή και προσοδοφόρο για το Δημόσιο τρόπο. Οι ηλεκτρονικές υπηρεσίες του Δημοσίου, επομένως, δεν απασχολούνται από την επίλυση ζητημάτων διαχείρισης χρηστών ή των συναλλαγών τους, τα οποία εξασφαλίζονται από το *Gateway*. Οι βασικές υπηρεσίες που περιλαμβάνει το *Gateway* είναι (βλ. παρακάτω Εικόνα) [20]:

- *Authentication & Authorisation*: οι υποστηριζόμενοι χρήστες (Πολίτες, Επιχειρήσεις και Ενδιάμεσοι πχ Λογιστές) μπορούν να εισέρχονται σε όλες τις δημόσιες, ηλεκτρονικές υπηρεσίες με τα ίδια «πιστοποιητικά» που έχουν παραλάβει από την υπηρεσία εγγραφής (*Registration & Enrolment*) του *Gateway* με τους μηχανισμούς αυθεντικοποίησης:
  - "*User ID/password*"
  - "*User ID/password*" σε συνδυασμό με μία μυστική φράση για επιπρόσθετη ασφάλεια
  - Ψηφιακά «Πιστοποιητικά»

  Οι συγκεκριμένες υπηρεσίες παρέχονται είτε μέσω της Web διεπαφής (*Web User Interface*) που προσφέρει το *Gateway* είτε μέσω των προγραμματιστικών διεπαφών (APIs) των υπηρεσιών του *Gateway* προς τα συμβεβλημένα Portals. Συνεπώς, εκτός από την τυχαία (ad-hoc) επίσκεψη ενός χρήστη σε μία Δημόσια, ηλεκτρονική υπηρεσία υποστηρίζεται και το μοντέλο της μόνιμης σύνδεσης ενός συμβεβλημένου οργανισμού (Δημόσιου ή Ιδιωτικού) με τις κατάλληλες διεπαφές του *Gateway* μέσω εξοπλισμού και λογισμικού που

προδιαγράφεται από το *Gateway* και πρέπει να εγκαταστήσει ο οργανισμός στις εγκαταστάσεις του (*Departmental Interface Server - DIS*).

Πηγή: [21]



Εικόνα 63: Γενική Επισκόπηση της Αρχιτεκτονικής του *Government Gateway*

- *Transaction & Routing Messaging Facility*: ονομάζεται και "*Transaction Engine*" και εξασφαλίζει ασφαλή ανταλλαγή εγγράφων και συμπληρωμένων ηλεκτρονικών εντύπων μεταξύ των Δημ. Υπηρεσιών και των πολιτών, επιχειρήσεων ή και άλλων Δημ. Υπηρεσιών.

- *Secure Mail*: προσφέρει ασφαλές, Web – based ηλεκτρονικό ταχυδρομείο στις Δημ. Υπηρεσίες.

- *Payments Facility*: παρέχει ένα ευέλικτο υπόβαθρο για την υλοποίηση ασφαλών ηλεκτρονικών πληρωμών από τις συμβεβλημένες Δημ. Υπηρεσίες με πολλούς εναλλακτικούς τρόπους.

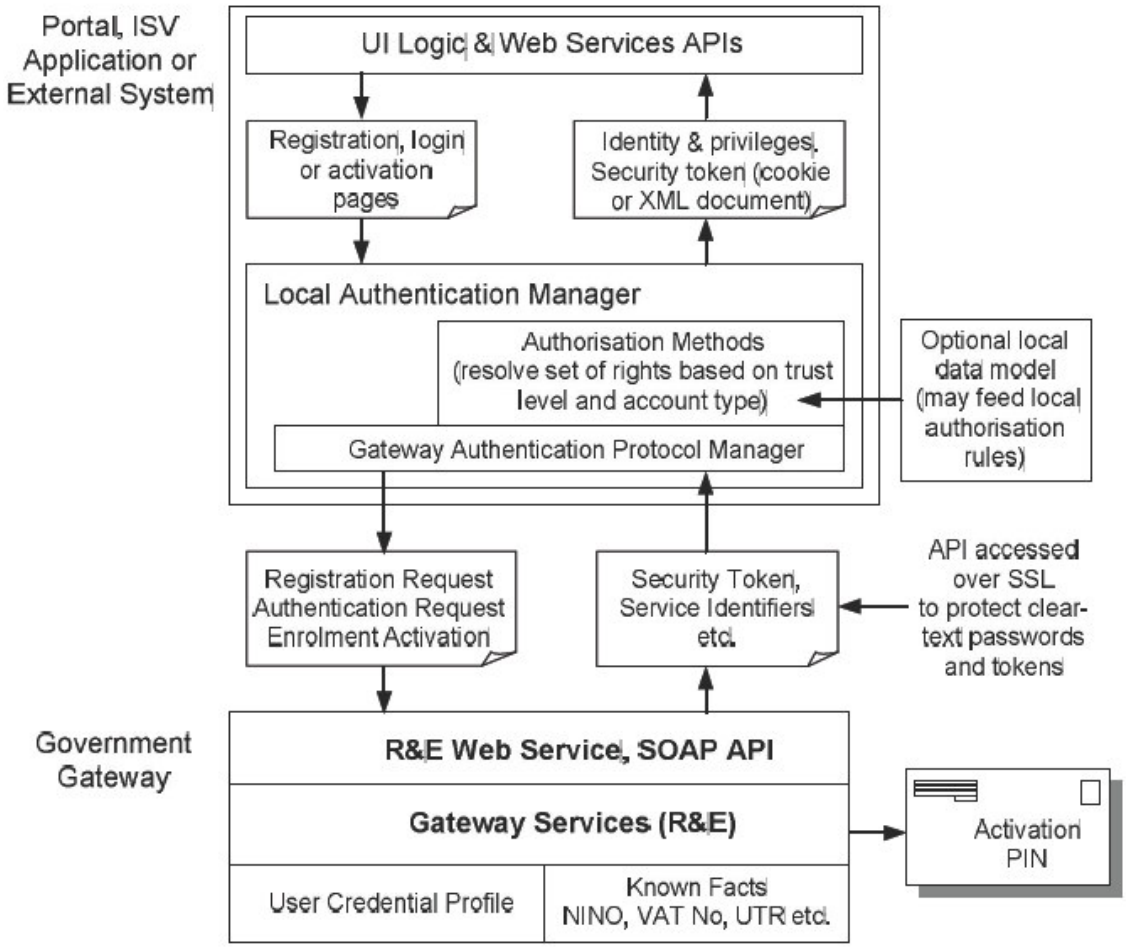
- *Integration*: παρέχει μεθόδους επικοινωνίας των συνδεδεμένων Δημ. Υπηρεσιών με τα πρότυπα διαλειτουργικότητας που έχει θέσει η Κυβέρνηση του Η.Β. με υπάρχουσες προδιαγραφές ηλεκτρονικής επικοινωνίας στο Δημόσιο Τομέα.

- *Test Environments*: εξασφαλίζει το κατάλληλο «υπολογιστικό» περιβάλλον δοκιμών εμπορικών προϊόντων ή τρίτων λύσεων για την επιβεβαίωση της ορθής επικοινωνίας τους με τις υπηρεσίες του *Gateway*.

- *Helpdesk*: αποτελεί ένα ολοκληρωμένο Web περιβάλλον όπου οι συμβεβλημένοι παράγοντες (πολίτες, επιχειρήσεις κλπ) μπορούν να έχουν την απαιτούμενη υποστήριξη και καθοδήγηση.

Συνεπώς, η διαδικασία της αυθεντικοποίησης αποτελεί απλώς μία από τις παρεχόμενες υπηρεσίες του *Gateway*, η οποία συνδέεται άμεσα με τις εφαρμοζόμενες διαδικασίες εγγραφής των οντοτήτων στο σύστημα (*Registration & Enrolment*). Η στενή σχέση των συγκεκριμένων φάσεων φαίνεται και στο παρακάτω διάγραμμα των βασικών λειτουργιών που πρέπει να παρέχει ένα Portal που επιθυμεί τη χρήση της *Gateway* εγγραφής και αυθεντικοποίησης χρηστών, οι οποίες χρησιμοποιούν το μοντέλο WS-Trust.

Πηγή: [21]



Εικόνα 64: Γενική Επισκόπηση της Αρχιτεκτονικής των Υπηρεσιών Αυθεντικοποίησης του *Government Gateway*

Αναλυτικότερα, στο θέμα της αυθεντικοποίησης χρηστών από ένα Portal Δημ. Υπηρεσίας είναι απαραίτητη η ανάπτυξη ενός τμήματος διαχείρισης του πρωτοκόλλου αυθεντικοποίησης *Gateway* (*Gateway Authentication Protocol Manager*) από τη μεριά του Portal ώστε να εξασφαλιστεί η επικοινωνία με τις SOAP διεπαφές του *Gateway*. Ο χρήστης, επομένως, καταχωρεί στην αντίστοιχη οθόνη του Portal τα «πιστοποιητικά» του και αποστέλλεται στο *Gateway*

ένα αίτημα αυθεντικοποίησης το οποίο εξετάζεται από τη *Security Token Service – STS* σε σχέση με το αποθηκευμένο προφίλ του χρήστη ή τα υπόλοιπα δεδομένα του χρήστη (*Known Facts*), πχ ΑΦΜ, Αριθμός Κοινωνικής Ασφάλισης κλπ. Δημιουργείται έτσι το απαραίτητο *Security Token* το οποίο επιστρέφεται στο Portal για την αποδοχή του χρήστη και τον περαιτέρω έλεγχο πρόσβασής του [21].

Το *Gateway* ακολουθεί τη λογική των *Επιπέδων Διασφάλισης* (*Assurance Levels*) από τις υπηρεσίες αυθεντικοποίησης τα οποία ορίζονται στο κείμενο θεμελίωσης "*Registration and Authentication: eGovernment Strategy Framework Policy and Guidelines*" της Υπηρεσίας *Office of the e-Envoy* η οποία είναι μέρος του *Cabinet Office* [110]. Ορίζονται επομένως τέσσερα επιθυμητά *Επίπεδα Διασφάλισης* από την αυθεντικοποίηση:

- *Επίπεδο 0*: Δεν απαιτείται αυθεντικοποίηση καθώς η πιθανή μη εγκεκριμένη χρήση της συγκεκριμένης υπηρεσίας θα επιφέρει ελάχιστες ζημιές στους πολίτες ή τη Δημ. Υπηρεσία.

- *Επίπεδο 1*: Απαιτείται αυθεντικοποίηση τέτοια ώστε ακόμα και αν αποτύχει θα προκληθούν περιορισμένες ζημιές στις ηλεκτρονικές πληροφορίες της Δημ. Υπηρεσίας ή στα δικαιώματα του πολίτη.

- *Επίπεδο 2*: Απαιτείται «ισχυρή» αυθεντικοποίηση καθώς η ενδεχόμενη εισβολή τρίτων μερών στις συγκεκριμένες υπηρεσίες θα επιφέρει σημαντικές ζημιές (οικονομική απώλεια, διαρροή σημαντικών πληροφοριών κλπ).

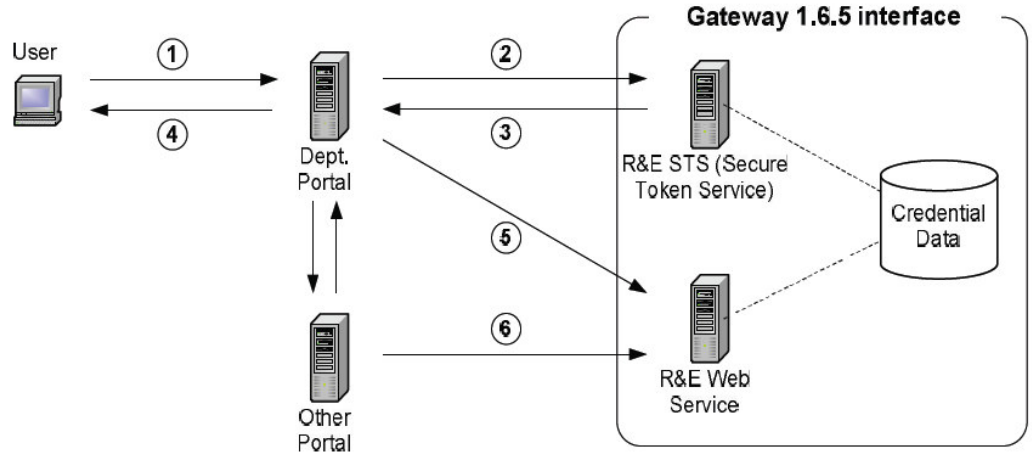
- *Επίπεδο 3*: Απαιτείται πολύ αυστηρή διαδικασία αυθεντικοποίησης καθώς η ενδεχόμενη εισβολή τρίτων μερών στις συγκεκριμένες υπηρεσίες θα επιφέρει μεγάλου μεγέθους ζημιές (απειλή ασφαλείας, σημαντική οικονομική απώλεια, διαρροή πολύ ευαίσθητων προσωπικών ή Κρατικών πληροφοριών κλπ).

Σχετικά με τη χρήση των κατάλληλων μηχανισμών αυθεντικοποίησης ανά *Επίπεδο Διασφάλισης*, τα ζεύγη User ID/Password χρησιμοποιούνται σε ηλεκτρονικές υπηρεσίες *Επιπέδου* 1, ενώ τα Ψηφιακά «Πιστοποιητικά» μπορούν να χρησιμοποιηθούν σε υπηρεσίες όλων των *Επιπέδων*. Η έκδοση 1.6.7 του *Gateway* προσθέτει ένα ενδιάμεσο *Επίπεδο* 1.5 που αντιστοιχεί σε μηχανισμό αυθεντικοποίησης ο οποίος εκτός από το ζευγάρι User ID/Password χρησιμοποιεί και μία μυστική φράση ασφαλείας [21].

Από την έκδοση 1.6.5 του *Gateway* υλοποιείται μία νέα διεπαφή των Web Services του *Gateway* η οποία στηρίζεται στα διαδεδομένα, ανοιχτά πρότυπα *WS-Security*, *WS-Trust*, *WS-Policy*. Με την εφαρμογή των συγκεκριμένων προτύπων έγινε εφικτή η ανάπτυξη και επιβολή πολιτικών ασφαλείας για τις συνδέσεις των χρηστών, τις ανταλλαγές δεδομένων, το διαχωρισμό χρηστών σε κατηγορίες, την καθιέρωση πολιτικών στη μορφή των «πιστοποιητικών» κλπ. Η σημαντικότερη αλλαγή στη διαδικασία αυθεντικοποίησης του *Gateway* με την εφαρμογή των συγκεκριμένων προτύπων είναι η εισαγωγή της έννοιας του *Security Token* ως αποδεικτικό μέσο αυθεντικοποίησης. Συνεπώς, μαζί με τη διεπαφή *Registration & Enrolment – R&E* του *Gateway* εγκαθίσταται και η υπηρεσία *Security Token Service – STS* η οποία σύμφωνα με τις ανωτέρω προδιαγραφές διαχειρίζεται τις αιτήσεις αυθεντικοποίησης από τα συμβεβλημένα Portals και δημιουργεί τα σχετικά *Security Tokens* που περιέχουν τα στοιχεία ταυτότητας των αυθεντικοποιημένων χρηστών και στην περίπτωση του *Gateway* ονομάζονται

Gateway Tokens. Σε γενικές γραμμές η αλληλουχία των βημάτων για την αυθεντικοποίηση των χρηστών από ένα Portal είναι (βλ. επόμενη Εικόνα) [21]:

Πηγή: [21]



Εικόνα 65: Γενική Διαδικασία Αυθεντικοποίησης Χρηστών στο *Government Gateway*

1. Ο χρήστης εισάγει στο Portal της Δημ. Υπηρεσίας τα «πιστοποιητικά» που έχει παραλάβει από την εγγραφή του στο *Gateway* (User ID/Password ή Ψηφιακό «Πιστοποιητικό»).

2. Το Portal αποστέλλει στη *STS* μία αίτηση για *Security Token* ώστε να αυθεντικοποιηθεί ο χρήστης.

3. Η *STS* αποδέχεται την αίτηση και εκτελεί ελέγχους σε σχέση και με τα αποθηκευμένα στοιχεία των χρηστών. Αποστέλλεται πίσω στο Portal απάντηση με το *Gateway Token* το οποίο διατηρείται από το Portal για μελλοντικές κλήσεις.

4. Το *Gateway Token* μπορεί να διατηρηθεί προαιρετικά στο Portal ως Cookie.

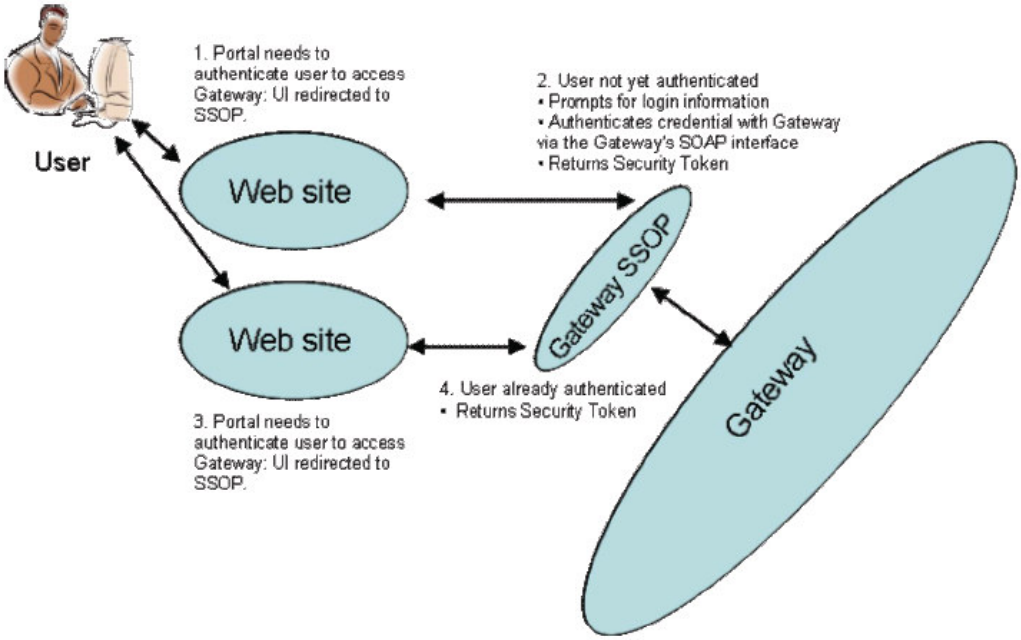
5. Όταν το Portal επιχειρήσει πρόσβαση σε μία δικτυακή υπηρεσία, περιλαμβάνει στο SOAP Header της κλήσης του το *Gateway Token*.

6. Σε περίπτωση όπου το συγκεκριμένο Portal διατηρεί αμοιβαία, «έμπιστη» σχέση (μέσω Ψηφιακών «Πιστοποιητικών») με ένα άλλο Portal και μπορεί επομένως να εφαρμοστεί ανταλλαγή δεδομένων μέσω «ασφαλούς» καναλιού (χρήση πρωτοκόλλου SSL/TLS) ο χρήστης μπορεί να προσπελάσει το δεύτερο Portal και να χρησιμοποιήσει τις υπηρεσίες του. Η αυθεντικοποίηση υλοποιείται με την «επίδειξη» του *Gateway Token* που διατηρεί από τα προηγούμενα βήματα το αρχικό Portal.

Η συνήθης διαδικασία, όμως, μετά την απόκτηση του *Gateway Token* είναι η κλήση του *STS* από το Portal για τον ακριβή προσδιορισμό των συγκεκριμένων υπηρεσιών του Portal στις οποίες έχει εγγραφεί ο συγκεκριμένος χρήστης και επομένως μπορεί να προσπελάσει. Για την ικανοποίηση αυτής της απαίτησης χρησιμοποιούνται τα *SAML Assertions* τα οποία μπορούν να παρέχουν τις απαιτούμενες πληροφορίες χωρίς διαδοχικές κλήσεις του Portal προς το *Gateway*. Με μία κλήση, δηλαδή, του Portal προς την *STS* με παράμετρο "*Target Resource*" (ταυτότητα του Portal) δημιουργείται από την *STS* το κατάλληλο *SAML Assertion* με τις πλη-

ροφορίες του χρήστη και τη λίστα με τις προσπελάσιμες υπηρεσίες του Portal. Η εφαρμοζόμενη έκδοση από το Gateway για τα *SAML Assertions* είναι η OASIS *SAML* 1.1. Εκμεταλλευόμενη τα *SAML Assertions* η έκδοση 1.6.7 εισήγαγε τη λειτουργικότητα πλήρους Single Sign – On των χρηστών ανάμεσα στις ηλεκτρονικές υπηρεσίες των συμβεβλημένων Portals, ενώ μέχρι τη συγκεκριμένη έκδοση το Single Sign – On είχε την έννοια ότι οι χρήστες μπορούσαν να χρησιμοποιήσουν τα ίδια «πιστοποιητικά» για πρόσβαση σε πολλές ηλεκτρονικές υπηρεσίες του Δημ. Τομέα, αλλά θα έπρεπε κάθε φορά να εισάγουν τα στοιχεία τους προκειμένου να αυθεντικοποιηθούν από καθεμιά υπηρεσία κατά τη διάρκεια μίας συνόδου πρόσβασης υπηρεσιών (*Browser Session*). Η υπηρεσία Single Sign – On εξασφαλίζεται με την εισαγωγή στην έκδοση 1.6.7 της λειτουργικότητας του *Single Sign – On Portal* (*SSOP*). Η γενική διαδικασία του SSO είναι (βλ. επόμενη Εικόνα) [21]:

Πηγή: [21]



Εικόνα 66: Επισκόπηση της Διαδικασίας SSO στο *Government Gateway* μέσω του *SSO Portal*

1. Το Portal αντιλαμβάνεται την πρόσβαση του χρήστη σε μία ηλεκτρονική υπηρεσία και είναι προγραμματισμένο έτσι ώστε να προωθεί κάθε τέτοια ενέργεια στο *SSOP* μαζί με ένα σύνολο παραμέτρων οι οποίες εξαρτώνται από το πρωτόκολλο του Portal και είναι συνήθως το *Target Resource* (η ταυτότητα του Portal) και η *Reply Address* (η διεύθυνση αποστολής των απαντήσεων).

2. Το *SSOP* αναζητά στο σταθμό του χρήστη το απαιτούμενο SSO Cookie. Στην περίπτωση όπου αυτό δεν υπάρχει, γιατί είναι η πρώτη είσοδος του χρήστη, το *SSOP* εμφανίζει στο χρήστη τη σελίδα εισαγωγής των στοιχείων του (*Sign – In* σελίδα). Το *SSOP* δέχεται τα «πιστοποιητικά» του χρήστη, προχωρά στην αυθεντικοποίησή του μέσω της υπηρεσίας *STS* του *Gateway* και δέχεται ως απάντηση το *Gateway Token* του συγκεκριμένου χρήστη. Στη συνέχεια επικοινωνεί ξανά με τη *STS* αποστέλλοντας της το *Gateway Token* και

το *Target Resource* του βήματος 1 και δέχεται ως απάντηση από τη *STS* του *Gateway* ένα *SAML Assertion*. Το *SSOP* δημιουργεί ένα SSO Cookie στον Browser του χρήστη τον οποίο και ανακατευθύνει πίσω στη *Reply Address* περνώντας ταυτόχρονα και το *SAML Assertion*.

3. Μόλις ο χρήστης προσπελάσει μία δεύτερη ηλεκτρονική υπηρεσία σε άλλο συμβεβλημένο Portal, ο έλεγχος μεταφέρεται αυτόματα από το Portal στο *SSOP*. Όπως και στο προηγούμενο βήμα, το *SSOP* αναζητά στο σταθμό του χρήστη ένα SSO Cookie, το οποίο τώρα πια εντοπίζει.

4. Παρόλο που το *SSOP* θα μπορούσε να προχωρήσει απευθείας στην αυθεντικοποίηση του χρήστη συνήθως εμφανίζει πάλι μία σελίδα διαθέσιμων επιλογών προς το χρήστη, οι οποίες περιλαμβάνουν την είσοδο στη νέα υπηρεσία με άλλο λογαριασμό χρήστη από τον υφιστάμενο (στην περίπτωση όπου ένας χρήστης διατηρεί πολλαπλούς λογαριασμούς στο *Gateway*, δυνατότητα η οποία επιτρέπεται υπό όρους), την προώθηση του χρήστη στη νέα υπηρεσία ή την έξοδό του από την προηγούμενη σύνδεση. Αν ο χρήστης επιλέξει την είσοδο με στοιχεία άλλου λογαριασμού, ακολουθείται η διαδικασία του βήματος 2. Αν ο χρήστης επιλέξει την είσοδό του στη νέα υπηρεσία με τον υπάρχον λογαριασμό, το *SSOP* χρησιμοποιεί το *Gateway Token* από την προηγούμενη σύνδεση του χρήστη για να ζητήσει από τη *STS* το νέο *SAML Assertion* για το νέο Portal. Μόλις το παραλάβει, ανακατευθύνει το χρήστη στη *Reply Address* μεταφέροντας ταυτόχρονα και το *SAML Assertion* του ίδιου χρήστη για το νέο Portal. Με τις διαδοχικές εισόδους του χρήστη σε διαφορετικά Portals αυξάνει η λίστα των συνδέσεών του στο *SSOP*, από την οποία ο χρήστης μπορεί να επιλέξει όποιες επιθυμεί να «κλείσει».

Μία πρόσθετη υπηρεσία του *Gateway* προς τα συμβεβλημένα Portals είναι η δυνατότητα παραμετροποίησης των σελίδων *Sign – In* και *Sign – Out* με τις επιθυμητές μορφοποιήσεις εμφάνισης που ταιριάζουν στο υπόλοιπο Portal και συγκεκριμένο οργανισμό. Αυτές οι παράμετροι υπάρχουν σε ένα διαθέσιμο XML αρχείο ρυθμίσεων στο οποίο κάθε Portal μπορεί να καταχωρήσει παραμετρικές τιμές ή απλώς να χρησιμοποιήσει την προεπιλεγμένη μορφοποίηση του *SSOP* από το *Gateway*. Η υλοποίηση του *SSOP* βασίζεται σε ανοιχτά πρότυπα έτσι ώστε κάθε Portal που πρόκειται να επικοινωνήσει μαζί του μπορεί να χρησιμοποιήσει εμπορικά προϊόντα ή λύσεις που υλοποιούν τις προδιαγραφές *WS-Federation*, *Liberty Alliance* και *SAML 1.1 Post Profile* [21].

Η υπηρεσία *Gateway* εμφανίζει ικανοποιητική αποδοχή από τους πολίτες και τις επιχειρήσεις, είτε σε πλήρως on-line υπηρεσίες είτε σε υπηρεσίες υποβολής ηλεκτρονικών φορμών (πχ υποβολή και πληρωμή φορολογικής δήλωσης, υπολογισμός συντάξεων, λήψη συγκεκριμένων επιδομάτων, υποβολή δηλώσεων ΦΠΑ κλπ). Σύμφωνα με στοιχεία του 2006 υπάρχουν περίπου 9 εκατομμύρια ενεργές εγγραφές χρηστών, ενώ το συνολικό έργο έχει βραβευθεί από κρατικούς ή ιδιωτικούς οργανισμούς για τις καινοτομίες του στο χώρο του e-Government [16].

Μία εμφανής διαφορά με το έργο *E-Authentication* της Κυβέρνησης των Η.Π.Α. είναι ότι το *E-Authentication* έχει μία περισσότερο κατανεμημένη φιλοσοφία στη διαχείριση της αυθεντικοποίησης, ενώ στο *Gateway* υπάρχει ένας σαφής κεντρικός προσανατολισμός. Οι χρήστες στο *E-Authentication* εγγράφονται σε όποια Υπηρεσία έχει εξουσιοδότηση από την κεντρική αρχή του έργου και μπορούν να προσπελάσουν όσες υπηρεσίες έχουν συμβατό *Επίπεδο Διασφάλισης* με την πλήρη εκμετάλλευση των πρωτοκόλλων – λύσεων *Federated Identity Man-*

agement. Στο *Gateway* υπάρχει η κεντρική υπηρεσία εγγραφής των χρηστών για την κεντρικά ελεγχόμενη πρόσβαση σε κρατικές, ηλεκτρονικές υπηρεσίες, όπου τα πρωτόκολλα *Federation Identity* χρησιμοποιούνται για την εξασφάλιση Web SSO μεταξύ των διαφορετικών Δημ. Υπηρεσιών.

3.3.2.3 Project "GUIDE" – Creating a European Identity Management Architecture for e-Government

Το έργο "*GUIDE*" είναι ένα ερευνητικό πρόγραμμα που χρηματοδοτείται από την Ευρωπαϊκή Ένωση (*6FP*) και διεξάγεται από μία διευρυμένη σύμπραξη 22 Ιδιωτικών οργανισμών, επιχειρήσεων και ακαδημαϊκών ιδρυμάτων με συντονιστή την εταιρία BT - British Telecom. Ο σκοπός του έργου είναι η δημιουργία μίας αρχιτεκτονικής για ηλεκτρονικές, e-Government υπηρεσίες διαχείρισης ταυτοτήτων και συναλλαγών μεταξύ των χωρών της Ε.Ε.. Το βασικό αντικείμενο, επομένως, του *GUIDE* είναι η δημιουργία μία ανοιχτής αρχιτεκτονικής η οποία θα αποτελέσει το υπόβαθρο για υπηρεσίες μετάδοσης δεδομένων ταυτοτήτων, ώστε να είναι δυνατή η διαχείριση ταυτοτήτων και η αυθεντικοποίηση πολιτών για την πρόσβαση e-Government υπηρεσιών μεταξύ των χωρών της Ε.Ε.. Η σχεδιαζόμενη αρχιτεκτονική θα καθιστά διαλειτουργικά τα διαφορετικά συστήματα Διαχείρισης Ταυτοτήτων με την ανάπτυξη κοινών πρωτοκόλλων ανταλλαγής πληροφοριών ταυτοτήτων και την ανάπτυξη ενός κατανεμημένου, «ομόσπονδου» μοντέλου. Καθένα τοπικό, περιφερειακό ή εθνικό σύστημα διατηρεί τη διαχείριση των ταυτοτήτων χρηστών του, αλλά το υπόβαθρο εξασφαλίζει υπηρεσίες διαλειτουργικότητάς τους. Το αντικείμενο του έργου είναι αρκετά περίπλοκο καθώς περιλαμβάνει επίσης την επίλυση πολλών, μη-τεχνολογικών προβλημάτων: από τα σοβαρά νομικά και πολιτικά θέματα προστασίας των προσωπικών δεδομένων μέχρι πιο καθημερινά κοινωνικά θέματα, όπως οι προβληματισμοί των πολιτών για την εμπιστευτικότητα που εξασφαλίζει ένα τέτοιο σύστημα. Το έργο, επομένως, καλύπτει πολλούς ερευνητικούς τομείς και ασχολείται με όλες τις πλευρές του προβλήματος ώσπου να καταλήξει στην προτεινόμενη αρχιτεκτονική. Σε αυτή τη φάση του *GUIDE* γίνονται δοκιμαστικές αξιλογήσεις και εφαρμογές της διατυπωμένης πρότασης αρχιτεκτονικής με συγκεκριμένες ενέργειες διαλειτουργικότητας δεδομένων ταυτοτήτων και συναλλαγών μεταξύ διαφορετικών χωρών [34].

Το έργο, λόγω του σύνθετου και πολυεθνικού χαρακτήρα του, ακόμα και μέσα στα πλαίσια της Ε.Ε., περιλαμβάνει ένα σύνολο μελετών σε διαφορετικά πεδία με τελικό σκοπό τη διατύπωση τεχνολογικού σχεδιασμού. Συγκεκριμένα, στα αποτελέσματα του έργου απαριθμούνται:

- <u>*Κοινωνιολογική Έρευνα*</u>: αφορά θέματα της ευρύτερης έννοιας της «*ταυτότητας*» από κοινωνιολογική οπτική στα διάφορα κράτη που θα συμμετέχουν στο σχεδιαζόμενο σύστημα Διαχείρισης Ταυτοτήτων. Σκοπός της έρευνας είναι η τροφοδότηση του τεχνολογικού σχεδιασμού με τις ανησυχίες και τις κυρίαρχες θεωρήσεις σχετικά με την ταυτότητα τόσο των πολιτών όσο και των υπολοίπων οντοτήτων που θα συμμετέχουν στο τελικό σύστημα [38].

- <u>*Πολιτική Δέσμευση*</u>: αφορά τη μελέτη των υπαρχόντων και των εν εξελίξει θεσμικών, πολιτικών πλαισίων που διαμορφώνουν τη Διαχείριση Ταυτοτήτων στις χώρες μέλη. Γίνεται μία συγκριτική παρουσίαση των τάσεων που επικρατούν στα κράτη μέλη σχετικά με τα θέματα ταυτοτήτων και το e-Government. Επίσης, επειδή το έργο αφορά την Ε.Ε. και την δέσμευσή της προς την ανάπτυξη του e-Government, παρουσιάζονται και οι παράμετροι

ενσωμάτωσης του έργου στις υφιστάμενες και σχεδιαζόμενες δομές και πολιτικές της Ε.Ε. [37].

- *Δέσμευση Κυβερνήσεων (Διατύπωση Προτάσεων)*: επιχειρείται η ενημέρωση της Ε.Ε. και των διοικήσεων σε εθνικό επίπεδο για τις απαραίτητες αλλαγές που θα επιφέρει η υλοποίηση του έργου *GUIDE*. Οι αλλαγές αφορούν το θεσμικό, νομικό και τεχνολογικό υπόβαθρο της Δημόσιας Διοίκησης στα κράτη – μέλη [35].

- *Τεχνολογική Μελέτη*: Το πρώτο μέρος της μελέτης περιγράφει το εύρος του έργου και τις θεμελιώδεις υπηρεσίες που πρέπει να παρέχει η υλοποίησή του ώστε να επιτυγχάνει το σκοπό της «δι-Ευρωπαϊκής» αρχιτεκτονικής για τη διαλειτουργικότητα των δεδομένων ταυτοτήτων [36]. Πολλά από τα στοιχεία του τεχνικού κειμένου βασίζονται σε προγενέστερη μελέτη, όπου διατυπώνονταν προτάσεις για τη διαμόρφωση βασικής πολιτικής εφαρμογής κατάλληλων μηχανισμών αυθεντικοποίησης σε δικτυακές εφαρμογές του Δημόσιου Τομέα [128].

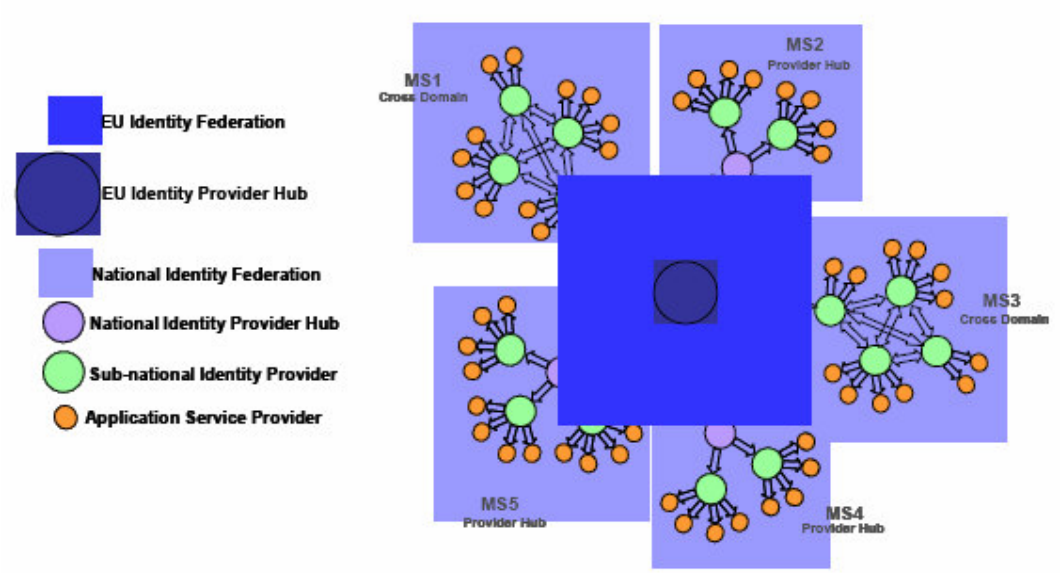
Η ουσία του *GUIDE* είναι η τεχνολογική υποστήριξη Κρατικών, δι-ευρωπαϊκών Υπηρεσιών (*Pan European Government Services – PEGS*) όπου οι ηλεκτρονικές εφαρμογές θα αναγνωρίζουν χρήστες – πολίτες άλλων κρατών – μελών της Ε.Ε. Αυτό σημαίνει εξασφάλιση δύο θεμελιωδών υπηρεσιών [36]:

- Αυθεντικοποίηση χρηστών εκτός εθνικών ορίων: όταν ένας πολίτης μίας χώρα Α επιθυμεί την προσπέλαση μίας ηλεκτρονικής υπηρεσίας μίας χώρας Β, αυτή η υπηρεσία θα αυθεντικοποιήσει τον πολίτη μέσω ενός *Identity Provider* της χώρας Α.

- Παροχή Ιδιοτήτων των χρηστών: εκτός από την αυθεντικοποίηση των χρηστών, οι εφαρμογές είναι πιθανό να ζητήσουν περισσότερα στοιχεία που συνδέονται με την ταυτότητα ενός χρήστη, πχ τη διεύθυνσή του, στοιχεία ονόματός του κλπ.

Στην επόμενη Εικόνα απεικονίζεται η γενική τοπολογία στην οποία βασίζεται η αντίληψη του έργου *GUIDE*.

Πηγή: [36]



Εικόνα 67: Τοπολογία του *GUIDE*

Ουσιαστικά επιδιώκεται η δημιουργία κεντρικών πυλών (*GUIDE Gateways*) μέσω των οποίων θα εξασφαλίζεται η διαλειτουργικότητα μεταξύ των επιμέρους *Federations* Δημοσίων Οργανισμών του εσωτερικού των κρατών – μελών. Προκειμένου να προκύψει η αναλυτική αρχιτεκτονική του *GUIDE* οι υπεύθυνοι του έργου μελέτησαν τις υπάρχουσες τεχνολογίες και λύσεις *Federated Identity Management* (*Liberty Alliance ID-FF*, *Shibboleth*, *WS-Federation*) και τα χαρακτηριστικά αντίστοιχων έργων όπως το *E-Authentication* [36]. Από τις συγκεκριμένες μελέτες προέκυψαν ενδιαφέρουσες προτάσεις σχημάτων και λύσεων που μπορούν να καλύψουν τις απαιτήσεις αυτού του σύνθετου έργου, αλλά η λεπτομερέστερη εξέτασή τους ξεπερνά το εύρος της παρούσας εργασίας.

3.3.3 E-Government και Αυθεντικοποίηση στον Ελληνικό Δημόσιο Τομέα

Στο χώρο της Ελληνικής Δημόσιας Διοίκησης υπάρχουν πολλές προσπάθειες εφαρμογής λύσεων ηλεκτρονικών υπηρεσιών οι οποίες προσφέρουν διαφορετικές δυνατότητες στους πολίτες και κατατάσσονται σε διαφορετικά επίπεδα ολοκλήρωσης (βλ. Πίνακα 4) [165].

Πηγή: [165]

Φορέας	Υπηρεσία	Αποδέκτες	Επίπεδο Ολοκλήρωσης
Υπουργείο Οικονομικών	Κατάθεση περιοδικής δήλωσης ΦΠΑ + Πληρωμή του ΦΠΑ, σε χρεωστικές δηλώσεις	Επιχειρήσεις / Πολίτες	4
	Κατάθεση δήλωσης VIES - ενδοκοινοτικών αποκτήσεων, παραδόσεων	Επιχειρήσεις	4
	Κατάθεση λίστα ΦΜΥ –Φόρος Μισθωτών Υπηρεσιών + Πληρωμή του ΦΜ	Επιχειρήσεις	4
	Κατάθεση δήλωσης Φόρου Εισοδήματος	Επιχειρήσεις / Πολίτες	4

	Κατάθεση συγκεντρωτικής κατάστασης τιμολογίων Πελατών-Προμηθευτών	Επιχειρήσεις	4
	Λήψη πιστοποιητικού Φορολογικής Ενημερότητας	Επιχειρήσεις / Πολίτες	4
	Υπολογισμός αντικειμενικής αξίας ακινήτου	Επιχειρήσεις / Πολίτες	2 (Ηλεκτρονικά Φύλλα)
	Υπολογισμός Φόρου Μεγάλης Ακίνητης Περιουσίας	Επιχειρήσεις / Πολίτες	3
	Αναζήτηση και τροποποίηση στοιχείων οχημάτων	Επιχειρήσεις / Πολίτες	3
	Διάθεση των πιο συχνά χρησιμοποιούμενων εγγράφων	Επιχειρήσεις / Πολίτες	2
	Έλεγχος εγκυρότητας ΑΦΜ και φορολογικής ενημερότητας	Επιχειρήσεις / Πολίτες	3
ΙΚΑ	Κατάθεση ΑΠΔ Αναλυτικής Περιοδικής Δήλωσης + Πληρωμή στο ΙΚΑ	Επιχειρήσεις	4
	Λήψη πιστοποιητικού Ασφαλιστικής Ενημερότητας	Επιχειρήσεις	4
	Εκτύπωση πληθώρας εγγράφων	Επιχειρήσεις / Πολίτες	2
Εμπορικό Βιομηχανικό Επιμελητήριο Αθηνών	Έλεγχος του δικαιώματος χρήσης της επωνυμίας και του διακριτικού τίτλου της επιχείρησης	Επιχειρήσεις	4
Εθνικό Τυπογραφείο	Παραγγελία & παραλαβή Τεύχους ΦΕΚ με ανάλογη χρέωση	Επιχειρήσεις / Πολίτες	4
ΟΑΕΔ	Αναζήτηση Ανέργων	Επιχειρήσεις	3
	Αναζήτηση Θέσεων Εργασίας	Πολίτες	3
Νομαρχία	Καταγραφή δικαιολογητικών για πληθώρα αιτήσεων	Πολίτες / Επιχειρήσεις	1
ΥΠΕΣΔΔΑ - ΚΕΠ	Υπηρεσίες 1ου και 2ου επιπέδου για ένα σύνολο συναλλαγών με την Δημόσια Διοίκηση	Πολίτες / Επιχειρήσεις	1, 2

Πίνακας 4: Παρεχόμενες Υπηρεσίες Ηλεκτρονικής Διακυβέρνησης στην Ελληνική Δημόσια Διοίκηση

Το κοινό χαρακτηριστικό των ανωτέρω υπηρεσιών αλλά και όλων των Πληροφοριακών Συστημάτων που έχουν αναπτυχθεί σε Φορείς και Οργανισμούς του Ελληνικού Δημόσιου Τομέα είναι η έλλειψη έμφασης στο σχεδιαστικό παράγοντα της διαλειτουργικότητας. Συγκεκριμένα, αρκετά από τα Πληροφ. Συστήματα έχουν αναπτυχθεί σε διαφορετικές τεχνολογικές πλατφόρμες, χωρίς υποχρεωτική τήρηση διαδεδομένων προτύπων και χωρίς ενιαία αντιμετώπιση κωδικοποιήσεων βασικών πληροφοριών (πχ Νομοί, Χώρες, Επαγγέλματα κλπ). Τα παραπάνω συστήματα έχουν υλοποιηθεί σε διαφορετικά τεχνολογικά περιβάλλοντα και παρουσιάζουν αυξημένη ανομοιογένεια αρχιτεκτονικής μεταξύ τους, ενώ σε αρκετές περιπτώσεις θεωρούνται παλαιωμένης τεχνολογίας. Επιπρόσθετα, οι διαφοροποιημένες ανάγκες του κάθε Οργανισμού, καθιστούν τα συστήματα αυτά ακόμα περισσότερο ανομοιογενή μεταξύ τους από λειτουργική άποψη, παρά το γεγονός ότι ακολουθούν ένα ενιαίο θεσμικό και λειτουργικό πλαίσιο για την υποστήριξη των διαδικασιών που αυτοματοποιούν. Προκειμένου να αντιμετωπιστεί η ανωτέρω ανομοιογένεια στα υφιστάμενα και μελλοντικά Πληροφ. Συστήματα και ηλεκτρονικές υπηρεσίες του Δημοσίου έχει γίνει μια προσπάθεια θεμελίωσης σε θεωρητικό επίπεδο ενός *Πλαισίου Διαλειτουργικότητας Ηλεκτρονικής Διακυβέρνησης* (*ΠΔΗΔ*) στο πλαίσιο του επιχειρησιακού προγράμματος «Κοινωνία της Πληροφορίας». Το ελληνικό *ΠΔΗΔ* έχει βασιστεί κατά ένα μεγάλο ποσοστό στο αντίστοιχο πλαίσιο του Ηνωμένου Βασιλείου "*e-*

Gif' [145], πάνω στο οποίο στηρίχτηκε η ανάπτυξη των υπηρεσιών Ηλεκτρονικής Διακυβέρνησης της Βρετανίας. Συγκεκριμένα στο Ελληνικό ΠΔΗΔ παρέχονται περιορισμένου εύρους πολιτικές και τεχνικές προδιαγραφές για τα παρακάτω θέματα [165]:

- Διασυνδεσιμότητα.
- Ολοκλήρωση και διαμόρφωση δεδομένων.
- Διαχείριση περιεχομένου και metadata.
- Πρόσβαση πληροφοριών.
- XML για επιχειρησιακούς τομείς.
- Απαιτήσεις τεχνολογικής υποδομής και τεχνικών προδιαγραφών.
- Σχεδιασμός και ανάπτυξη XML Schemas.
- Θεσμικές απαιτήσεις πλαισίου.

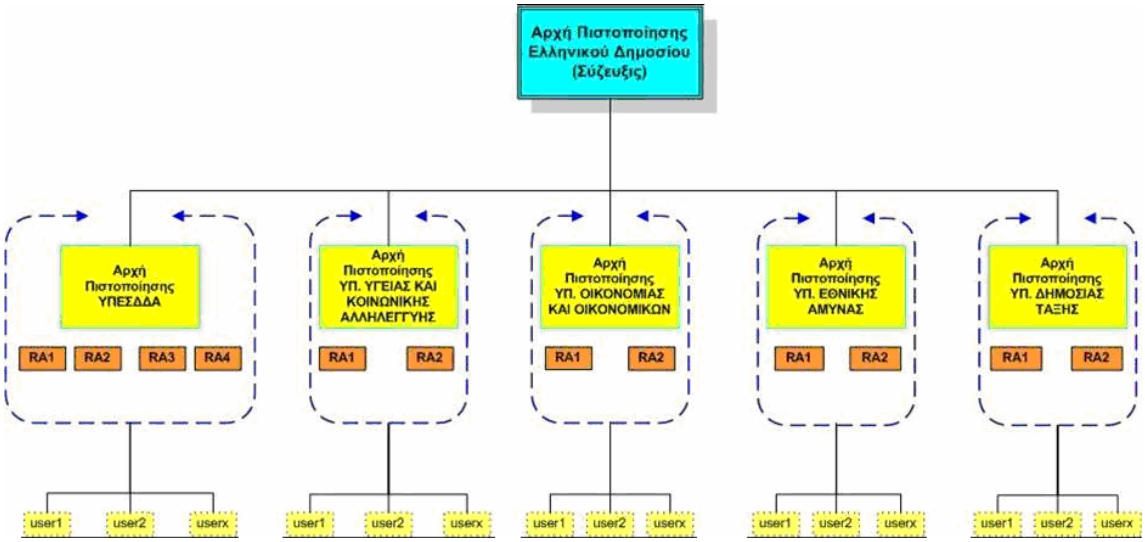
Κατά συνέπεια και στο θέμα της αυθεντικοποίησης οι υφιστάμενες, διαφορετικές δικτυακές εφαρμογές των Δημοσίων Φορέων δεν έχουν τηρήσει ενιαία τεχνολογική πλατφόρμα ή τουλάχιστον φιλοσοφία. Έχουν γίνει, όμως, σημαντικά βήματα στο θεσμικό πλαίσιο που αφορά θέματα ψηφιακών «πιστοποιητικών» και των προδιαγραφών τους, σε συμμόρφωση με τις αντίστοιχες Κοινοτικές Οδηγίες, όπως το Π.Δ. 150/2001 «Προσαρμογή στην Οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές». Σύμφωνα με το Π.Δ. 150/2001 η αρμόδια αρχή για τον έλεγχο και την εποπτεία των εγκατεστημένων στην Ελλάδα παρόχων υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής είναι η Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων (ΕΕΤΤ). Με την απόφαση 248/71 (ΦΕΚ 603/Β'/16-5-2002), η ΕΕΤΤ εξέδωσε «Κανονισμό Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής», ρυθμίζοντας θέματα σχετικά με [165]:

- Αναγνωρισμένα πιστοποιητικά.
- Την εποπτεία και τον έλεγχο των εγκατεστημένων στην Ελλάδα παρόχων υπηρεσιών πιστοποίησης ηλεκτρονικής υπογραφής, οι οποίοι εκδίδουν αναγνωρισμένα ή μη «πιστοποιητικά» ή παρέχουν άλλες σχετικές με την ηλεκτρονική υπογραφή υπηρεσίες πιστοποίησης.

Σχετικά με την υποδομή ενιαίας, ισχυρής αυθεντικοποίησης χρηστών σε ηλεκτρονικές υπηρεσίες του Δημοσίου Τομέα σημαντικά βήματα έχουν ξεκινήσει μέσω του έργου «ΣΥΖΕΥΞΙΣ». Το «ΣΥΖΕΥΞΙΣ» αποτελεί έργο παροχής τηλεπικοινωνιακών και τηλεματικών υπηρεσιών μεγάλης έκτασης και κλίμακας σε Φορείς του Ελληνικού Δημόσιου Τομέα, οι ανάγκες των οποίων δεν περιορίζονται σε απλές τηλεφωνικές συνδέσεις αλλά επεκτείνονται περιλαμβάνοντας προηγμένες υπηρεσίες φωνής, δεδομένων και εικόνας. Σήμερα είναι συνδεδεμένα περίπου 1.800 σημεία Δημοσίων Υπηρεσιών σε όλη τη χώρα για την παροχή υπηρεσιών ευρυζωνικών μεταδόσεων. Μέρος του έργου αποτελεί και η υπηρεσία «*Υποδομή Δημοσίου κλειδιού*» ("*Public Key Infrastructure – PKI*"), με την οποία αρχικά θα εκδίδονται Ψηφιακά «Πιστοποιητικά» για επιλεγμένους χρήστες - υπαλλήλους των φορέων που συνδέονται στο δίκτυο. Συνολικά θα υλοποιηθεί η έκδοση ψηφιακών πιστοποιητικών σε έξυπνες κάρτες για

50.000 στελέχη της Ελληνικής Δημόσιας Διοίκησης, καθώς και η έκδοση 2.000 ψηφιακών πιστοποιητικών εξυπηρετητή για τη χρησιμοποίηση του πρωτοκόλλου SSL. Οι έξυπνες κάρτες θα χρησιμοποιηθούν για την ψηφιακή υπογραφή εγγράφων και του ηλεκτρονικού ταχυδρομείου. Προκειμένου να λειτουργήσει η συγκεκριμένη υποδομή υλοποιείται «Αρχή Πιστοποίησης» (*Certification Authority*) και εγγραφής (*Registration Authority*), η οποία διαχειρίζεται και εκδίδει Ψηφιακά «Πιστοποιητικά» για τους Φορείς της Ελληνικής Δημόσιας Διοίκησης και τους χρήστες τους. Η λειτουργία αυτή στηρίζεται σε «Υποδομή Δημοσίου κλειδιού» (PKI) που εξυπηρετεί τη διοικητική διάρθρωση της Ελληνικής Δημόσιας Διοίκησης. Η συγκεκριμένη υποδομή θα λειτουργεί ως Πάροχος Υπηρεσιών Πιστοποίησης για τους Φορείς μέλη του «ΣΥΖΕΥΞΙΣ». Η επιδιωκόμενη ιεραρχία *CA's* κατά την πρώτη εφαρμογή του έργου φαίνεται στην παρακάτω Εικόνα και περιλαμβάνει τους ευρύτερους Φορείς (Υπουργεία) των οποίων οι περισσότερες Υπηρεσίες συνδέονται στο δίκτυο του «ΣΥΖΕΥΞΙΣ» [166].

Πηγή: [166]



Εικόνα 68: Διάρθρωση «*Αρχών Πιστοποίησης*» (*CA*'s) Υπηρεσίας PKI του Δικτύου «ΣΥΖΕΥΞΙΣ»

Η υποδομή PKI που δημιουργείται με το «ΣΥΖΕΥΞΙΣ», παρόλο που αφορά Ψηφιακά «Πιστοποιητικά» υπογραφής εγγράφων και μόνο τους Φορείς που ανήκουν στο δίκτυο του έργου, αποτελεί το υπόβαθρο για να αποτελέσει την Εθνική υποδομή PKI για όλο τον Ελληνικό Δημόσιο Τομέα. Η συγκεκριμένη παρατήρηση ενισχύεται και από το γεγονός ότι στο υπό εξέλιξη έργο «Εθνική Πύλη ΕΡΜΗΣ» με αντικείμενο τη «Μελέτη και Ανάπτυξη της Κεντρικής Κυβερνητικής Διαδικτυακής Πύλης της Δημόσιας Διοίκησης για την Πληροφόρηση & Ασφαλή Διεκπεραίωση Ηλεκτρονικών Συναλλαγών των Πολιτών / Επιχειρήσεων» η υποδομή PKI που πρόκειται να αναπτυχθεί προδιαγράφεται να αποτελέσει υπό-δέντρο της παραπάνω ιεραρχίας *CA's* του «ΣΥΖΕΥΞΙΣ» [165]. Το έργο «Εθνική Πύλη ΕΡΜΗΣ» περιλαμβάνει και την κάλυψη πολλών ζητημάτων ενιαίας αυθεντικοποίησης χρηστών στις ηλεκτρονικές υπηρεσίες των Δημοσίων Οργανισμών μέσω της επιδιωκόμενης Πύλης (Portal) και προσεγγίζει σε πολλά θέματα τα παραπάνω έργα Κρατικών Φορέων του εξωτερικού, αλλά η τρέχουσα φάση της εξέλιξής του δεν επιτρέπει την τεχνική ανάλυση του έργου μόνο από το τεύχος της διακήρυξής του, προτού υπάρχουν ολοκληρωμένα δείγματα των αποτελεσμάτων του.

4. ΠΡΟΤΑΣΕΙΣ

Όπως αναφέρθηκε στην Εισαγωγή της παρούσας εργασίας, οι Προτάσεις που διατυπώνονται μετά τη μελέτη των θεωρητικών χαρακτηριστικών και των εφαρμοσμένων περιπτώσεων έχουν ως άξονα τη διερεύνηση εφαρμογής συστήματος ενιαίας αυθεντικοποίησης των πολιτών – χρηστών σε ηλεκτρονικές υπηρεσίες της Ελληνικής Δημόσιας Διοίκησης. Τα παραδείγματα των υπολοίπων Κρατών και η υφιστάμενη κατάσταση στις εξελίξεις του e-Government στην Ελλάδα καταδεικνύουν ότι απαιτούνται κάποια βασικά στάδια τεχνολογικής και θεσμικής υποδομής αλλά είναι εφικτή η μελέτη εφαρμογή ενιαίας αυθεντικοποίησης στους εθνικούς Δημόσιους Οργανισμούς. Ένα ενδεικτικό παράδειγμα δυνατής εξέλιξης στο θεσμικό και τεχνολογικό πλαίσιο στην Ελληνική Δημόσια Διοίκηση είναι ο καθορισμός των επιθυμητών προδιαγραφών αυθεντικοποίησης στις Κρατικές ηλεκτρονικές υπηρεσίες, κατά τα πρότυπα των κειμένων:

- "*E-Authentication Guidance for Federal Agencies*" του Γραφείου του Προέδρου των Η.Π.Α. [143] και της μελέτης "*Electronic Authentication Guideline*" του κρατικού οργανισμού των Ην. Πολιτειών *National Institute of Standards and Technology* [93]. Τα δύο κείμενα αποτέλεσαν τη βάση για το έργο *E-Authentication* αλλά και για πολλά εθνικά έργα άλλων κρατών.

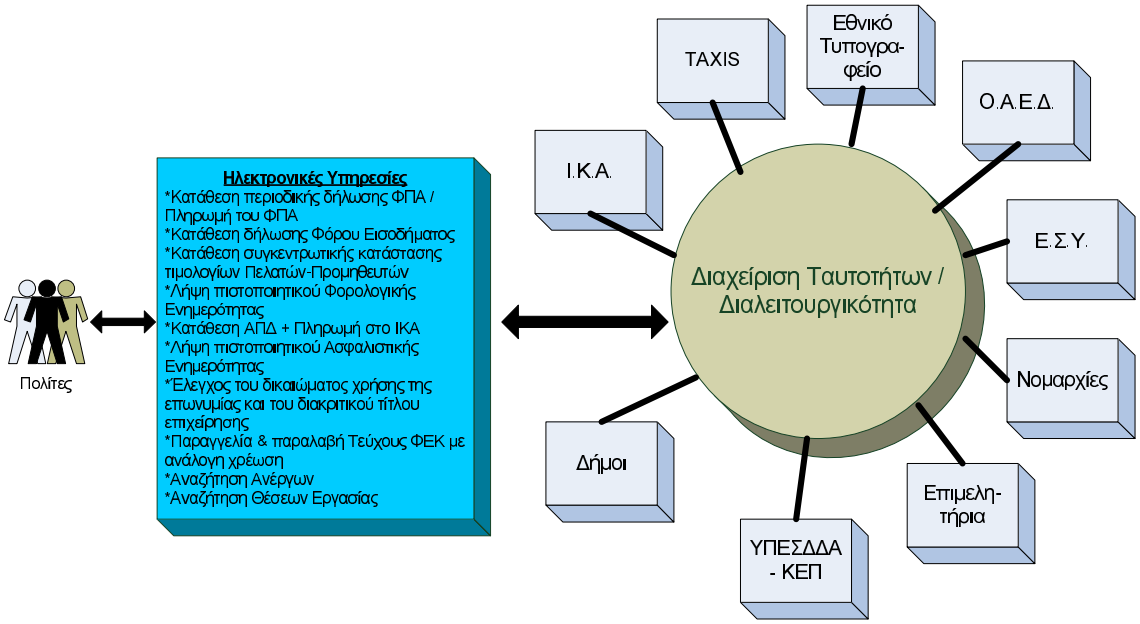
- "*Registration and Authentication: eGovernment Strategy Framework Policy and Guidelines*" [110] της κυβέρνησης του Ηνωμ. Βασιλείου που χρησιμοποιήθηκε από το έργο *Gateway*.

Το πρώτο στάδιο στην υποδομή προτύπων για το Ελληνικό e-Government έχει γίνει με τη διατύπωση του *Πλαισίου Διαλειτουργικότητας Ηλεκτρονικής Διακυβέρνησης* (*ΠΔΗΔ*) στο πλαίσιο του επιχειρησιακού προγράμματος «Κοινωνία της Πληροφορίας». Το γεγονός ότι το Ελληνικό *ΠΔΗΔ* έχει στοιχεία από το αντίστοιχο πλαίσιο του Ηνωμένου Βασιλείου "*e-Gif*" μπορεί να οδηγήσει στη διατύπωση προτάσεων περαιτέρω αξιοποίησης των αποτελεσμάτων του Βρετανικού παραδείγματος. Το *e-Gif* αποτελεί για το e-Government του Ηνωμ. Βασιλείου μία από τις προδιαγραφές διαλειτουργικότητας των Δημοσίων Οργανισμών, η οποία αποτελεί μέρος ενός ευρύτερου έργου ανάπτυξης του e-Government με το «κωδικό» όνομα "*UK GovTalk*" στο οποίο διατυπώνονται επιμέρους προδιαγραφές e-Government, παρουσιάζονται βέλτιστες πρακτικές και επεκτάσεις του σχήματος XML για εξειδικευμένες εφαρμογές κλπ [146]. Συνεπώς, μία ανάλογη προσπάθεια στον Ελληνικό χώρο μπορεί να οικοδομήσει το κατάλληλο τεχνολογικό υπόβαθρο ομοιόμορφων προδιαγραφών ανάπτυξης ηλεκτρονικών υπηρεσιών από τους εθνικούς Δημόσιους Οργανισμούς, ώστε να προκύψει το κατάλληλο περιβάλλον εφαρμογής ενιαίων πολιτικών e-Government.

Μετά το πρώτο βήμα, επομένως, της τεχνολογικής προτυποποίησης της διαλειτουργικότητας στη Δημόσια Διοίκηση, ειδικότερα στα θέματα της αυθεντικοποίησης συναλλασσομένων των ηλεκτρονικών υπηρεσιών του Ελληνικού Δημοσίου Τομέα μπορεί να ακολουθηθεί το παράδειγμα του έργου *Government Gateway* του Ηνωμένου Βασιλείου. Η συγκεκριμένη πρόταση αφορά στην υιοθέτηση της γενικής τεχνολογικής και διοικητικής φιλοσοφίας και αρχιτεκτονικής του έργου χωρίς να υπεισέρχεται στις εξειδικευμένες τεχνολογικές λεπτομέρειες υλοποίησής του, για τις οποίες άλλωστε δεν υπάρχει επαρκής, διαθέσιμη τεκμηρίωση και ενδεχομένως να περιλαμβάνουν απαγορευτικές παραμέτρους ή απαιτήσεις υλοποίησης ενός παρόμοιου έργου στα Ελληνικά δεδομένα.

Συνεπώς, κατά μία γενική προσέγγιση, θα μπορούσε να εφαρμοστεί στην Ελληνική Δημόσια Διοίκηση ένα κεντρικό σύστημα αυθεντικοποίησης των χρηστών όλων των ηλεκτρονικών υπηρεσιών των Δημ. Οργανισμών, κατά τα πρότυπα του Βρετανικού *Gateway*, και η γενική αναπαράσταση και τα βασικά χαρακτηριστικά ενός τέτοιου συστήματος είναι:

Πηγή: [Επεξεργασία στοιχείων από 21, 165]



Εικόνα 69: Γενικό Διάγραμμα Πρότασης Κεντρικής Αυθεντικοποίησης Ηλεκτρονικών Υπηρεσιών Ελληνικού Δημόσιου Τομέα

- Οι επιμέρους Οργανισμοί δε διατηρούν λογαριασμούς χρηστών των ηλεκτρονικών τους υπηρεσιών, αλλά όλοι οι χρήστες (πολίτες, επιχειρήσεις, στελέχη των Οργανισμών) απευθύνονται στην Κεντρική Υπηρεσία αυθεντικοποίησης. Εκτός των πολλών τεχνολογικών ζητημάτων λειτουργίας μίας τέτοιας Υπηρεσίας είναι αυτονόητη η συνεχής επανεξέταση και ανανέωση του νομικού πλαισίου προστασίας των προσωπικών δεδομένων των πολιτών από το Κράτος, ειδικότερα για τα θέματα ηλεκτρονικής διαχείρισής τους.

- Η Κεντρική Υπηρεσία συγκεντρώνει, ελέγχει και διατηρεί τα στοιχεία ταυτότητας των χρηστών μαζί με όλα τα πρόσθετα στοιχεία που μπορεί να χρησιμοποιηθούν κατά την πρόσβασή τους στις επιμέρους υπηρεσίες (πχ. για τις υπηρεσίες του Ι.Κ.Α. είναι απαραίτητος ο ΑΜ ΙΚΑ, για τις Δ.Ο.Υ. και την Εφορία είναι απαραίτητο το Α.Φ.Μ. κοκ). Αυτά τα πρόσθετα στοιχεία είναι απαραίτητα και για τη περαιτέρω διασταύρωση της ταυτότητας του χρήστη κατά την πρώτη φάση εγγραφής του στο σύστημα.

- Οι επιμέρους Δημ. Οργανισμοί που διαθέτουν ηλεκτρονικές υπηρεσίες στο Internet θα πρέπει να διεξάγουν μελέτη: των πιθανών «απειλών» εναντίον τους και της κρισιμότητας των δεδομένων τους, οπότε και θα καταλήξουν στο κατάλληλο *Επίπεδο Διασφάλισης* που επιθυμούν από τις διαδικασίες αυθεντικοποίησης. Με αυτό τον τρόπο είναι δυνατός ο καθορισμός του είδους των «πιστοποιητικών» που μπορούν να χρησιμοποιηθούν από τους χρήστες των εφαρμογών τους, δηλαδή ένα ζευγάρι username/password ή ψηφιακά «πιστοποιητικά». Βασισμένη σε αυτές τις αποφάσεις η Κεντρική Υπηρεσία διαχείρισης των

ταυτοτήτων μπορεί να αποδώσει τα κατάλληλα «πιστοποιητικά» στον κάθε χρήστη, ανάλογα με τις ηλεκτρονικές υπηρεσίες στις οποίες αιτείται πρόσβαση.

- Οι επιμέρους ηλεκτρονικές υπηρεσίες και τα Portals των Δημ. Οργανισμών μπορούν να αναπτυχθούν σε οποιαδήποτε τεχνολογία του Internet με την απαίτηση όμως της εφαρμογής των προτύπων διαλειτουργικότητας μεταξύ των Δημ. Οργανισμών και των απαραίτητων προτύπων διεπαφών που θα απαιτήσει η Κεντρική Υπηρεσία αυθεντικοποίησης για τη διεξαγωγή των βασικών υπηρεσιών αυθεντικοποίησης και του Web Single Sign – On των χρηστών. Η αυθεντικοποίηση των χρηστών και οι υπόλοιπες υπηρεσίες διαχείρισης ταυτοτήτων θα υλοποιούνται μέσω on – line κλήσεων στην Κεντρική Υπηρεσία από τα επιμέρους Δημόσια Portals, οι οποίες κλήσεις θα είναι ενσωματωμένες στην υλοποίηση των Portals και θα βασίζονται σε συγκεκριμένες προγραμματιστικές διεπαφές της Κεντρικής Υπηρεσίας.

- Σχετικά με τα τεχνολογικά ζητήματα, η διαλειτουργικότητα μεταξύ των Δημ. Οργανισμών μπορεί να βασιστεί στις προδιαγραφές του διατυπωμένου *Πλαισίου Διαλειτουργικότητας Ηλεκτρονικής Διακυβέρνησης* (*ΠΔΗΔ*). Σε σχέση, όμως, με τη διεπαφή των επιμέρους Portals με την Κεντρική Υπηρεσία αυθεντικοποίησης, η ανωτέρω μελέτη περιπτώσεων ξένων χωρών ανέδειξε τα οφέλη της εφαρμογής των βασικών προτύπων *Federated Identity Management* οπότε και σε αυτή την περίπτωση της Ελληνικής Κεντρικής Υπηρεσίας αυθεντικοποίησης είναι δυνατή η εφαρμογή των προαναφερθέντων προδιαγραφών (γλώσσα *SAML*, οικογένεια *WS-Federation*), καθώς η επικοινωνία των επιμέρους Portals με την Κεντρική Υπηρεσία είναι κατεξοχήν πρόβλημα *Identity Federation*. Η εφαρμογή των προδιαγραφών μπορεί να γίνει είτε με τη μορφή της εκ νέου ανάπτυξης λύσεων που να τις υλοποιούν είτε με την εγκατάσταση διαδεδομένων εμπορικών προϊόντων που μετά από κατάλληλους ελέγχους θα επιβεβαιωθεί ότι ενσωματώνουν επιτυχώς και αποδοτικά τα συγκεκριμένα πρότυπα.

- Η συγκεκριμένη γενική πρόταση βασίζεται σε μία Κεντρική Υπηρεσία παροχής υπηρεσιών αυθεντικοποίησης, αλλά είναι προφανές ότι μία υπηρεσία που αποτελεί κόμβο αναφοράς όλων των ηλεκτρονικών υπηρεσιών του Δημοσίου Τομέα θα μπορούσε να αξιοποιηθεί για την παροχή επιπρόσθετων υπηρεσιών e-Government, πάλι κατά τα πρότυπα του *Gateway*, όπως η εξασφάλιση ασφαλών ηλεκτρονικών πληρωμών, υπηρεσία κεντρικού e-Mail, υπηρεσία ασφαλούς ανταλλαγής μηνυμάτων κλπ.

Η αιτιολόγηση των ανωτέρω προτάσεων βασίζεται στα παρακάτω επιχειρήματα:

- Η διοικητική οργάνωση της χώρας και του Ελληνικού Δημόσιου Τομέα επιτρέπει την ύπαρξη μίας Κεντρικής Υπηρεσίας αναφοράς, κάτι που δε θα ήταν εύκολο σε μία Ομοσπονδία Κρατιδίων ή Πολιτειών, στην οποία πιθανώς να υπεισέρχονται διοικητικά εμπόδια πρόσβασης μία κοινής, κεντρικής υπηρεσίας.

- Υπάρχουν κάποιες πρώτες εξελίξεις οικοδόμησης κεντρικής υποδομής και διαλειτουργικότητας μεταξύ των Δημοσίων Υπηρεσιών με τα έργα: «ΣΥΖΕΥΞΙΣ», το εν εξελίξει έργο «Εθνική Πύλη ΕΡΜΗΣ» και τις μελέτες Διαλειτουργικότητας της «*Κοινωνίας της Πληροφορίας*». Ειδικότερα με το «ΣΥΖΕΥΞΙΣ» η υποδομή PKI που αναπτύσσεται στα πλαίσιά του μπορεί να επεκταθεί και αξιοποιηθεί ως την εθνική υποδομή PKI, η οποία θα μπορούσε να χρησιμοποιηθεί από μία Κεντρική Υπηρεσία αυθεντικοποίησης με ψηφιακά «πιστοποιητικά».

- Οι υπάρχουσες εφαρμογές e-Government δεν είναι ακόμα αρκετές σε πλήθος, άρα η αποσύνδεση των επιμέρους συστημάτων Διαχείρισης των λογαριασμών των χρηστών τους και η μεταφορά τους σε μία νέα Κεντρική Υπηρεσία δε θα προκαλούσε μεγάλη αστάθεια στην εύρυθμη λειτουργία του Δημοσίου Τομέα. Σε περίπτωση όπου υπήρχε μεγάλος αριθμός ηλεκτρονικών υπηρεσιών και εγγεγραμμένων χρηστών που καθημερινά χρησιμοποιούν και εξαρτώνται από αυτές τις υπηρεσίες, μία πρόταση ενιαίας αυθεντικοποίησης θα έπρεπε να ακολουθήσει άλλη κατεύθυνση, περισσότερο κατανεμημένης διαχείρισης των ταυτοτήτων.

- Από τη γενική παρουσίαση των υπαρχουσών ηλεκτρονικών υπηρεσιών στον Ελληνικό Δημόσιο Τομέα προκύπτει το συμπέρασμα ότι αυτές βασίζονται σε διαφορετικές και συχνά ξεπερασμένες τεχνολογίες, επομένως είναι συνήθως ανέφικτη η μεταξύ τους επικοινωνία όποτε υπάρχει σχετική απαίτηση. Επίσης, σχετικά με τα επιμέρους συστήματα Διαχείρισης Ταυτοτήτων, δεν υπάρχουν στοιχεία τεκμηρίωσης για την τήρηση ενιαίων προδιαγραφών ώστε να μπορούν να ενοποιούνται τα δεδομένα ταυτοτήτων των διαφορετικών λογαριασμών που ενδεχομένως διατηρεί ο ίδιος πολίτης.

Τα πλεονεκτήματα από τη λειτουργία μίας Κεντρικής Υπηρεσίας αυθεντικοποίησης είναι:

- Η ανάπτυξη επανα-χρησιμοποιήσιμων υπηρεσιών αυθεντικοποίησης για την ενιαία εξυπηρέτηση και εξασφάλιση Single Sign – On των πολιτών στις υπηρεσίες e-Government.

- Η μείωση του κόστους ανάπτυξης ηλεκτρονικών εφαρμογών για το Internet στο Δημόσιο Τομέα, καθώς τα επιμέρους έργα δε θα ασχολούνται με θέματα διαχείρισης χρηστών, αλλά θα εστιάζουν στο ίδιο το περιεχόμενο των εφαρμογών.

- Οι πολίτες κατέχουν μοναδικό «πιστοποιητικό» για την απόδειξη της ταυτότητάς τους στις ηλεκτρονικές υπηρεσίες του Δημοσίου και δε χρειάζεται να διατηρούν πολλαπλούς λογαριασμούς σε κάθε Οργανισμό.

- Η εφαρμογή διαδεδομένων προτύπων εξασφαλίζει την ανεξαρτησία των υλοποιημένων έργων από συγκεκριμένες προδιαγραφές ή εμπορικά προϊόντα, ενώ υπάρχει πάντα η ευκολία ασφαλούς επικοινωνίας με τρίτα συστήματα που βασίζονται στα ίδια κοινώς αποδεκτά πρότυπα.

- Οι πολίτες και οι επιχειρήσεις που συναλλάσσονται ηλεκτρονικά με το Κράτος δεν αντιλαμβάνονται την πολυπλοκότητα των συστημάτων , αλλά βιώνουν τη δυνατότητα ταυτόχρονης προσπέλασης πολλών Κρατικών Υπηρεσιών και την άμεση ολοκλήρωση πολλαπλών συναλλαγών.

5. ΣΥΜΠΕΡΑΣΜΑΤΑ

Από την παρουσίαση των θεμάτων της παρούσας εργασίας και τη διατύπωση των ανωτέρω προτάσεων πρακτικής εφαρμογής τους, προκύπτουν τα παρακάτω γενικά συμπεράσματα:

- Η αυθεντικοποίηση των χρηστών σε δικτυακές υπηρεσίες τεχνολογιών του Internet καταλαμβάνει πρωτεύουσα σημασία στα αντίστοιχα πληροφοριακά συστήματα. Η συγκεκριμένη διαπίστωση προκύπτει από το μεγάλο αριθμό των «απειλών» που εμφανίζονται με σκοπό την αποτυχία ή παραπλάνηση ειδικά της διαδικασίας της αυθεντικοποίησης. Οι κακόβουλοι χρήστες, επομένως, απομονώνουν τις λεπτομέρειες των διαδικασιών αυθεντικοποίησης και επιδιώκουν την υποκλοπή ή παραβίαση των στοιχείων ταυτότητας των χρηστών, καθώς με την κατοχή τους είναι εύκολη η περαιτέρω, παράτυπη εκμετάλλευση δικτυακών πόρων και υπηρεσιών. Επιπροσθέτως, η ανάπτυξη αυτόνομων συστημάτων διαχείρισης των ταυτοτήτων που ενσωματώνονται ή συνεργάζονται με τις κύριες εφαρμογές φανερώνει την ιδιαίτερη φροντίδα που απαιτείται για τα θέματα ασφαλούς και εμπιστευτικής διαχείρισης των λογαριασμών χρηστών ενός συστήματος.

- Κατά την ανάπτυξη δικτυακών εφαρμογών δίνεται συνήθως έμφαση στο περιεχόμενο των εφαρμογών και της τεχνολογικής πλατφόρμας όπου θα αναπτυχθούν και λιγότερο στους τρόπους εισόδου και ελέγχου πρόσβασης των χρηστών. Η απλή λύση του ζευγαριού username/password για την αναγνώριση και την επιβεβαίωση της ταυτότητας των χρηστών διακρίνεται: από πολλά κενά στα θέματα ασφάλειας, ειδικότερα αν δεν εφαρμόζεται ούτε η κρυπτογραφημένη μεταδοσή τους, από μεγάλα κόστη συντήρησης των λογαριασμών χρηστών και από δυσχέρανση της αξιοποίησης των εφαρμογών από την πλευρά των χρηστών, καθώς είναι υποχρεωμένοι να απομνημονεύουν τόσα passwords όσα και οι εφαρμογές που χρησιμοποιούν. Συνεπώς, είναι απαραίτητο οι σχεδιαστές των ηλεκτρονικών συστημάτων να μελετούν ισότιμα τα θέματα διαχείρισης των χρηστών τους, ενσωματώνοντας κάποιους από τους πολλούς μηχανισμούς και πρωτόκολλα «ισχυρής» αυθεντικοποίησης που παρουσιάστηκαν παραπάνω, ανάλογα με την κρισιμότητα των δεδομένων που διαχειρίζονται.

- Στα θέματα της χρήσης μηχανισμών και συσκευών ενίσχυσης της ασφάλειας της αυθεντικοποίησης είναι σαφές ότι οι Smart Cards με αποθηκευμένα ψηφιακά «πιστοποιητικά» είναι ο δημοφιλέστερος μηχανισμός «ισχυρής» αυθεντικοποίησης. Ο συγγενικός, όμως, μηχανισμός των USB Tokens κερδίζει έδαφος, καθώς διακρίνεται από μεγαλύτερη ευκολία στη χρήση, αφού δεν απαιτούνται ειδικές συσκευές ανάγνωσης. Επιπροσθέτως, απλές αλλά «έξυπνες» συσκευές όπως τα *One – Time Passwords* μπορούν να ενισχύσουν την ασφάλεια ενός συστήματος με μικρό οικονομικό και διαχειριστικό κόστος.

- Στα θέματα των βασικών πρωτόκολλων που σχετίζονται με την αυθεντικοποίηση, φαίνεταο ότι το *Kerberos* κυριαρχεί στις εφαρμογές «ισχυρής» αυθεντικοποίησης σε περιβάλλοντα μικρών δικτύων. Αυτό προκύπτει από το γενονός ότι αποτελεί το βασικό πρωτόκολλο στα Server λειτουργικά συστήματα των Microsoft Windows και ότι όλες σχεδόν οι λύσεις Web SSO επιλέγουν τη διεξαγωγή της τελικής αυθεντικοποίησης των χρηστών με το *Kerberos* v5. Ταυτόχρονα, στα θέματα των ηλεκτρονικών καταλόγων, το *LDAP* εμφανίζεται ως το κοινώς αποδεκτό πρότυπο και άλλες λύσεις καταλόγων φροντίζουν για την ανάπτυξη διεπαφής τους με συστήματα *LDAP*.

- Δύο σχετικά καινούριες έννοιες πρωτοστατούν στις εξελίξεις της αυθεντικοποίησης στα δικτυακά περιβάλλοντα: το Single Sign-On και το *Federated Identity Management*. Με τις δύο αυτές τάσεις η αυθεντικοποίηση στο Internet ξεφεύγει από τη στενή διαδικασία του ελέγχου εγκυρότητας των στοιχείων ταυτότητας των χρηστών και εμπλουτίζεται με μηχανισμούς γενικότερης διαχείρισης των δεδομένων ταυτότητας των χρηστών και ασφαλούς τροφοδότησής τους στις δικτυακές εφαρμογές.

- Από όλες τις κατηγορίες υπηρεσιών SSO το Web SSO στηρίζεται κυρίως στην ανάπτυξη μηχανισμών παρά σε διατύπωση πρωτοκόλλων και η επικρατέστερη λύση είναι η χρήση των Cookies στους Web Browsers των χρηστών. Παρόλο που όλες σχεδόν οι λύσεις Web SSO χρησιμοποιούν τα Cookies για να αποθηκεύουν πληροφορίες της πρώτης αυθεντικοποίησης του χρήστη, παρουσιάζουν σημαντικές διαφορές στο είδος των πληροφοριών που διατηρούν στα Cookies ή στον τρόπο που τα μεταχειρίζονται με αποτέλεσμα να παρουσιάζουν αποκλίσεις στην απόδοση και ασφάλειά τους.

- Το Web SSO διευκολύνει τους χρήστες κατά την πρόσβασή τους σε πολλές ηλεκτρονικές εφαρμογές, αλλά το *Federated Identity Management* θεωρείται ότι μπορεί να δώσει μία νέα ώθηση στην αξιοποίηση του Internet. Δεν αντιμετωπίζεται, δηλαδή, ως μία λύση εξυπηρέτησης απλώς των χρηστών, αλλά ως εργαλείο οικοδόμησης νέων μοντέλων ηλεκτρονικών εφαρμογών. Φυσικά, τα προβλήματα που περιβάλλουν το *Federated Identity Management* είναι πολλά και σύνθετα, καθώς αγγίζουν τεχνολικά θέματα, νομικά εμπόδια μέχρι επιχειρηματικές και εμπορικές συμφωνίες συνεργασιών μεταξύ «έμπιστων» οργανισμών. Γι αυτό το λόγο μόλις πριν λίγα χρόνια ξεκίνησε η εφαρμογή σχετικών λύσεων ή η ανάπτυξη εμπορικών προϊόντων με ενσωματωμένες τις διατυπωμένες προδιαγραφές, ενώ οι προσπάθειες ανάπτυξης σχετικών προδιαγραφών είχαν ξεκινήσει από τις αρχές του 2000. Ο χώρος των προτύπων του *Federated Identity Management* διαμορφώνεται από δύο μεγάλα «ρεύματα» συμπράξεων οργανισμών του ακαδημαϊκού και του επιχειρηματικού κόσμου αντίστοιχα.

- Ειδικότερα στο e-Government, η εφαρμογή των διαδικασιών *Federated Identity Management* μπορεί να λύσει πολλά δύσκολα θέματα διαχείρισης των λογαριασμών των πολιτών στις κρατικές ηλεκτρονικές υπηρεσίες. Η δυνατότητα, δηλαδή, της χρήσης ενός λογαριασμού για την πρόσβαση σε ηλεκτρονικές εφαρμογές πολλών διαφορετικών Οργανισμών μπορεί να εξασφαλίσει την ανάπτυξη του «ηλεκτρονικού» Δημόσιου Τομέα, καθώς θα εξοικονομείται χρόνος και κόστος διαχείρισης των χρηστών από τις επιμέρους υπάρχουσες ή αναπτυσσόμενες εφαρμογές. Επειδή, όμως, πρόκειται για υπηρεσίες Δημοσίων Οργανισμών και για στοιχεία ταυτότητας των πολιτών, η ανάπτυξη των σχετικών συστημάτων γίνεται με την προηγούμενη διατύπωση αυστηρού τεχνολογικού και θεσμικού πλαισίου καθορισμού του τρόπου εφαρμογής των μηχανισμών αυθεντικοποίησης και των προδιαγραφών *Identity Federations*. Όσα, δηλαδή, μπορούν απλώς να συμφωνήσουν μεταξύ τους δύο ή περισσότεροι εμπορικοί οργανισμοί για τους τρόπους και τις διαδικασίες προσδιορισμού της «έμπιστης» σχέσης τους, οι Κρατικοί Φορείς πρέπει να το θεσπίσουν με συγκεκριμένες μελέτες και διατάξεις. Η αυθεντικοποίηση μπορεί να αποτελέσει πυρήνα των ηλεκτρονικών εφαρμογών του Δημοσίου Τομέα και με τον ορισμό και κατοχύρωσή της με συγκεκριμένους κανόνες και πρότυπα μπορεί να προσφέρει την απαραίτητη ασφάλεια στις Δημόσιες ηλεκτρονικές εφαρμογές και τη συνακόλουθη εμπιστοσύνη των πολιτών στις δράσεις του e-Government.

6. ΑΝΑΦΟΡΕΣ

[1] **Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H. (Ed)**: "RFC 3748 - Extensible Authentication Protocol (EAP)". The Internet Engineering Task Force (2004). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc3748.txt [Τελευταία Πρόσβαση 05/02/2007].

[2] **Aladdin Knowledge Systems**: "Aladdin Knowledge Systems, Inc. Web Site" (2007). Διαθέσιμο On-Line: http://www.aladdin.com [Τελευταία Πρόσβαση 05/02/2007].

[3] **Aubry, P., Mathieu, V. and Marchal, J.**: "ESUP-Portail: open source Single Sign-On with CAS (Central Authentication Service)". ESUP Portail Consortium (2004). Διαθέσιμο On-Line: http://www.esup-portail.org/consortium/espace/SSO_1B/cas/eunis2004/cas-eunis2004-article.pdf [Τελευταία Πρόσβαση 05/02/2007].

[4] **BEA Systems, BMC Software, CA Inc., IBM, Layer 7 Technologies, Microsoft, Novell and VeriSign**: "Web Services Federation Language (WSFederation) v1.1". (2006). Διαθέσιμο On-Line: http://dev2dev.bea.com/webservices/WS_Federation.html [Τελευταία Πρόσβαση 05/02/2007].

[5] **BEA Systems, IBM, Microsoft and SAP**: "Web Services Policy Assertions Language (WS-PolicyAssertions) v1.0". (2002). Διαθέσιμο On-Line: http://www-128.ibm.com/developerworks/library/specification/ws-polas/ [Τελευταία Πρόσβαση 05/02/2007].

[6] **BEA Systems, IBM, Microsoft, SAP, Sonic Software and VeriSign**: "Web Services Policy Attachment (WSPolicyAttachment) v1.2". (2006). Διαθέσιμο On-Line: http://www-128.ibm.com/developerworks/library/specification/ws-polatt/ [Τελευταία Πρόσβαση 05/02/2007].

[7] **BEA Systems, IBM, Microsoft, SAP, Sonic Software and VeriSign**: "Web Services Policy Framework (WS-Policy) v1.2". (2006). Διαθέσιμο On-Line: http://www-128.ibm.com/developerworks/library/specification/ws-polfram/ [Τελευταία Πρόσβαση 05/02/2007].

[8] **BEA, IBM, Microsoft, RSA Security and VeriSign**: "WS-Federation: Passive Requestor Profile v1.0". (2003). Διαθέσιμο On-Line: ftp://www6.software.ibm.com/software/developer/library/ws-fedpass.pdf [Τελευταία Πρόσβαση 05/02/2007].

[9] **Berners-Lee, T., Fielding, R. and Masinter, L.**: "RFC 3986 - Uniform Resource Identifier (URI): Generic Syntax". The Internet Engineering Task Force (2005). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc3986.txt [Τελευταία Πρόσβαση 05/02/2007].

[10] **Blum,D., Gebel, G. and Moench, D.**: "Burton Group Report on the Federal E-Authentication Initiative". Burton Group, Midvale UT (2004). Διαθέσιμο On-Line: http://www.cio.gov/eauthentication/documents/BurtonGroupEAreport.pdf [Τελευταία Πρόσβαση 05/02/2005].

[11] **Camenisch, J. and Van Herreweghen, E.**: "Design and Implementation of the Idemix Anonymous Credential System". In Proceedings of the 9th ACM Conference on Computer and Communications Security, p.21–30, (2002).

[12] **Centrify:** "Centrify Corporation Web Site". (2007). Διαθέσιμο On-Line: http://www.centrify.com [Τελευταία Πρόσβαση 05/02/2007].

[13] **Chaffe T. & Lomas B.**: "The University Login: Authentication for Web Applications - Implementation Comparison". Technical report. University of Auckland (2004). Διαθέσιμο On-Line: http://www.umich.edu/~umweb/downloads/WebSSOImplementationComparision.pdf [Τελευταία Πρόσβαση 05/02/2007].

[14] **Clercq, J.**: "Smart Cards". Identity and Access Management. Microsoft TechNet. Microsoft Corporation, Redmond (2007). Διαθέσιμο On-Line: http://www.microsoft.com/technet/security/guidance/identitymanagement/scard.mspx [Τελευταία Πρόσβαση 05/02/2007].

[15] **Crispin, M.**: "RFC 3501 - INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1". The Internet Engineering Task Force (2003). Διαθέσιμο On-Line: http://www.isi.edu/in-notes/rfc3501.txt [Τελευταία Πρόσβαση 05/02/2007].

[16] **Dattani, B.**: "The UK Cabinet Office Government Gateway Project". Sun Microsystems. Liberty Alliance IDDY Awards Webcast (2006). Διαθέσιμο On-Line: http://www.projectliberty.org/liberty/content/download/2290/15088/file/IDDY-%20UK%20Cabinet.pdf [Τελευταία Πρόσβαση 05/02/2007].

[17] **Dierks, T. & Allen, C.**: "RFC 2246 - The TLS Protocol, Version 1.0". The Internet Engineering Task Force (1999). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc2246.txt [Τελευταία Πρόσβαση 05/02/2007].

[18] **Dierks, T. & Rescorla, E.**: "RFC 4346 - The Transport Layer Security (TLS) Protocol, V1.1". The Internet Engineering Task Force (2006). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc4346.txt [Τελευταία Πρόσβαση 05/02/2007].

[19] **Duke University**: "Webauth Authentication Protocol". Duke University, Durham (2003). Διαθέσιμο On-Line: http://webauth.duke.edu [Τελευταία Πρόσβαση 05/02/2007].

[20] **EDT**: "Central Infrastructure - Government Gateway (Overview)". e-Delivery Team. Cabinet Office. UK Government, London (2007). Διαθέσιμο On-Line: http://www.cabinetoffice.gov.uk/e-government/docs/responsibilities/document_library/pdf/government_gateway_flyer.pdf [Τελευταία Πρόσβαση 05/02/2007].

[21] **EDT**: "UK Government Gateway - Gateway Technical Briefing (EP03) v10.0". e-Delivery Team. Cabinet Office. UK Government, London (2006). Διαθέσιμο On-Line: http://www.cabinetoffice.gov.uk/e-government/docs/responsibilities/document_library/pdf/EP03_technical_briefing_v10.pdf [Τελευταία Πρόσβαση 05/02/2007].

[22] **EDUCAUSE:** "CAMP Shibboleth Implementation Workshop 2004". Broomfield, Colorado (2004). Διαθέσιμο On-Line:

http://www.educause.edu/CAMPShibbolethImplementationWorkshop2004/2477 [Τελευταία Πρόσβαση 05/02/2007].

[23] **Enterprise Wiki**: "Shibboleth Wiki". Atlassian Confluence (2007). Διαθέσιμο On-Line: https://spaces.internet2.edu/display/SHIB/WebHome [Τελευταία Πρόσβαση 05/02/2007].

[24] **Evidian:** "Evidian SA Web Site". (2007). Διαθέσιμο On-Line: http://www.evidian.com [Τελευταία Πρόσβαση 05/02/2007].

[25] **Federal CIO Council:** "Federal Public Key Infrastructure (FPKI) Policy Authority". (2007). Διαθέσιμο On-Line: http://www.cio.gov/fpkipa/ [Τελευταία Πρόσβαση 05/02/2007].

[26] **Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., Berners-Lee, T.**: "RFC 2616 - Hypertext Transfer Protocol -- HTTP/1.1". The Internet Engineering Task Force (1999). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc2616.txt [Τελευταία Πρόσβαση 05/02/2007].

[27] **Gilmore, B., Farvis, K. and Maddock, J.**: "Core Middleware and Shared Services Studies: Single Sign-On Report". Joint Information Systems Committee - JISC. The Higher Education Funding Council for England - HEFCE, Bristol London (2004). Διαθέσιμο On-Line: http://www.jisc.ac.uk/uploaded_documents/CMSS-Gilmore.pdf [Τελευταία Πρόσβαση 05/02/2006].

[28] **Glass, E.**: "The NTLM Authentication Protocol and Security Support Provider". Source Forge.Net (2006). Διαθέσιμο On-Line: http://davenport.sourceforge.net/ntlm.html [Τελευταία Πρόσβαση 05/02/2006].

[29] **Gross, T. & Pfitzmann, B.**: "Proving a WS-Federation passive requestor profile". *In* Proceedings of the ACM Secure Web Services Workshop (p.77 - 86). Washington (2004). Διαθέσιμο On-Line: http://www.zurich.ibm.com/security/publications/2004/GroPfi04WSFPI-proof-ACMSWS.pdf [Τελευταία Πρόσβαση 05/02/2007].

[30] **Gross, T.**: "Security analysis of the SAML Single Sign-on Browser/Artifact profile". *In* Proceedings of the 19th Annual Computer Security Applications Conference, Las Vegas (2003). Διαθέσιμο On-Line: http://www.acsac.org/2003/papers/73.pdf [Τελευταία Πρόσβαση 05/02/2007].

[31] **GSA**: "E-Authentication Federation Interim Legal Document Suite v4.0.7". The E-Authentication Initiative. General Services Administration (2005). Διαθέσιμο On-Line: http://www.cio.gov/eauthentication/index.htm [Τελευταία Πρόσβαση 04/11/2006].

[32] **GSA**: "Technical Approach for the Authentication Service Component v1.0.0". The E-Authentication Initiative. General Services Administration (2004). Διαθέσιμο On-Line: http://www.cio.gov/eauthentication/index.htm [Τελευταία Πρόσβαση 04/11/2006].

[33] **GSA**: "The E-Authentication Initiative Web Site".General Services Administration (2007). Διαθέσιμο On-Line: http://www.cio.gov/eauthentication/index.htm [Τελευταία Πρόσβαση 05/02/2007].

[34] **GUIDE**: "Creating a European Identity Management Architecture for e-Government". GUIDE Consortium (2007). Διαθέσιμο On-Line: http://istrg.som.surrey.ac.uk/projects/guide/ [Τελευταία Πρόσβαση 05/02/2007].

[35] **GUIDE**: "Face to Face Consultations with Governments of Member States (D2.3.2.A) v.1". GUIDE Consortium (2005). Διαθέσιμο On-Line: http://istrg.som.surrey.ac.uk/projects/guide/files/documents/D2.3.2.A.pdf [Τελευταία Πρόσβαση 05/02/2007].

[36] **GUIDE**: "Identity Interoperability Services Report: Core Services Descriptions (D1.2.1.B)". GUIDE Consortium (2005). Διαθέσιμο On-Line: http://istrg.som.surrey.ac.uk/projects/guide/documents.html [Τελευταία Πρόσβαση 04/02/2007].

[37] **GUIDE**: "Institutional, political, and policy frameworks affecting IdM for eGovernment (D2.1.1.A) v.1". GUIDE Consortium (2004). Διαθέσιμο On-Line: http://istrg.som.surrey.ac.uk/projects/guide/files/documents/D2.1.1.A.pdf [Τελευταία Πρόσβαση 05/02/2007].

[38] **GUIDE**: " Sociological study of IdM issues in Europe: Theoretical underpinnings v.1 (D2.1.2.A)". GUIDE Consortium (2004). Διαθέσιμο On-Line: http://istrg.som.surrey.ac.uk/projects/guide/documents.html [Τελευταία Πρόσβαση 04/02/2007].

[39] **Haller, N., Metz, C., Nesser, P., Straw, M.**: "RFC 2289 - A One-Time Password System". The Internet Engineering Task Force (1998). Διαθέσιμο On-Line: http://www.rfc-editor.org/rfc/rfc2289.txt [Τελευταία Πρόσβαση 05/02/2007].

[40] **Haller, N.**: "RFC 1760 - The S/KEY One-Time Password System". The Internet Engineering Task Force (1995). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc1760.txt [Τελευταία Πρόσβαση 05/02/2007].

[41] **Harrison, R.(Ed.)**: "RFC 4513 - Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms". The Internet Engineering Task Force (2006). Διαθέσιμο On-Line: http://www.isi.edu/in-notes/rfc4513.txt [Τελευταία Πρόσβαση 05/02/2007].

[42] **Housley, R., Polk, W., Ford, W., Solo, D.**: "RFC 3280 - Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile". The Internet Engineering Task Force (2002). Διαθέσιμο On-Line: http://tools.ietf.org/html/rfc3280 [Τελευταία Πρόσβαση 05/02/2007].

[43] **IBM Corporation & Microsoft Corporation**: "Federation of Identities in a Web Services World v1.0 - A joint whitepaper". (2003). Διαθέσιμο On-Line: http://www.ibm.com/developerworks/webservices/library/specification/ws-fedworld/ [Τελευταία Πρόσβαση 05/11/2006].

[44] **IBM Corporation & Microsoft Corporation**: "Passive Requestor Federation Interop Scenario v0.4". (2004). Διαθέσιμο On-Line: http://msdn2.microsoft.com/en-us/library/ms996532.aspx [Τελευταία Πρόσβαση 05/02/2007].

[45] **IBM Corporation & Microsoft Corporation**: "Security in a Web Services World: A Proposed Architecture and Roadmap - A joint whitepaper". (2002). Διαθέσιμο On-Line: http://www-128.ibm.com/developerworks/library/specification/ws-secmap/ [Τελευταία Πρόσβαση 05/02/2007].

[46] **IBM Corporation**: "Enterprise Security Architecture using IBM Tivoli Security Solutions". RedBooks. IBM Corporation (2002). Διαθέσιμο On-Line: http://www.redbooks.ibm.com/abstracts/sg246014.html [Τελευταία Πρόσβαση 05/02/2007].

[47] **IBM, BEA Systems, Microsoft, VeriSign, RSA Security**: "WS-Federation: Active Requestor Profile v1.0". (2003). Διαθέσιμο On-Line: http://www-128.ibm.com/developerworks/library/ws-fedact/ [Τελευταία Πρόσβαση 05/02/2007].

[48] **IBM, Microsoft and Actional, BEA, Computer Associates, Layer 7, Oblix, OpenNetwork, Ping Identity, Reactivity, and Verisign**: "Web Services Secure Conversation Language (WS-SecureConversation)". (2005). Διαθέσιμο On-Line: http://www-128.ibm.com/developerworks/library/specification/ws-secon/ [Τελευταία Πρόσβαση 05/02/2007].

[49] **IBM, Microsoft and Actional, BEA, Computer Associates, Layer 7, Oblix, OpenNetwork, Ping Identity, Reactivity, and Verisign**: "Web Services Trust Language (WS-Trust)". (2005). Διαθέσιμο On-Line: http://www-128.ibm.com/developerworks/library/specification/ws-trust/ [Τελευταία Πρόσβαση 05/02/2007].

[50] **IBM, Microsoft, RSA Security Inc. and VeriSign**: "Web Services Security Policy Language (WS-SecurityPolicy) v1.1". (2005). Διαθέσιμο On-Line: http://www-128.ibm.com/developerworks/library/specification/ws-secpol/ [Τελευταία Πρόσβαση 05/02/2007].

[51] **Internet2**: "InCommon Federation Web Site". (2007). Διαθέσιμο On-Line: http://www.incommonfederation.org [Τελευταία Πρόσβαση 05/02/2005].

[52] **Internet2**: "Internet2 Consortium Web Site". (2007). Διαθέσιμο On-Line: http://www.internet2.edu [Τελευταία Πρόσβαση 05/02/2007].

[53] **Internet2**: "Project Shibboleth Introduction". Middleware Architecture Committee for Education. Internet2 Consortium (2004). Διαθέσιμο On-Line: http://shibboleth.internet2.edu [Τελευταία Πρόσβαση 05/02/2007].

[54] **Internet2**: "Project Shibboleth". Middleware Architecture Committee for Education. Internet2 Consortium (2007). Διαθέσιμο On-Line: http://shibboleth.internet2.edu [Τελευταία Πρόσβαση 05/02/2007].

[55] **Internet2**: "Shibboleth Architecture Technical Overview (Working Draft)". Middleware Architecture Committee for Education. Internet2 Consortium (2007). Διαθέσιμο On-Line: http://shibboleth.internet2.edu/shibboleth-documents.html [Τελευταία Πρόσβαση 05/02/2005].

[56] **ITU**: "International Telecommunication Union Web Site". (2007). Διαθέσιμο On-Line: http://www.itu.int [Τελευταία Πρόσβαση 05/02/2007].

[57] **JA-SIG**: "Central Authentication Service - CAS". JA-SIG Collaborative (2007). Διαθέσιμο On-Line: http://www.ja-sig.org/products/cas/index.html [Τελευταία Πρόσβαση 05/02/2007].

[58] **JOSSO:** "Java Open Single Sign-On Project". The JOSSO Team (2004). Διαθέσιμο On-Line: http://www.josso.org [Τελευταία Πρόσβαση 05/02/2007]

[59] **Kearns, D.**: "Liberty Alliance vs. WS-Federation: Should we care? Who is clamoring for a single federated identity specification?". Identity Management Newsletter. Network World (2003). Διαθέσιμο On-Line: http://www.networkworld.com/newsletters/dir/2003/1103id1.html [Τελευταία Πρόσβαση 05/02/2005].

[60] **Klensin, J. (Editor)**: "RFC 2821 - Simple Mail Transfer Protocol". The Internet Engineering Task Force (2001). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc2821.txt [Τελευταία Πρόσβαση 05/02/2007].

[61] **Klensin, J., Catoe, R. and Krumviede, P.**: "RFC 2195 - IMAP/POP AUTHorize Extension for Simple Challenge/Response". The Internet Engineering Task Force (1997). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc2195.txt [Τελευταία Πρόσβαση 05/02/2007].

[62] **Kohl, J. T., Neuman, B. C. and T'so, T. Y.**: "The evolution of the Kerberos authentication system". *In Distributed Open Systems (*σελ.78-94). Brazier, F.M. T. & Johansen, D. (Editors). IEEE Computer Society Press (1994). Διαθέσιμο On-Line: ftp://athena-dist.mit.edu/pub/kerberos/doc/krb_evol.lpt [Τελευταία Πρόσβαση 05/02/2007].

[63] **Kolodgy, J.C.**: "Identity Management in a Virtual World (White Paper)". External Publication of IDC Information and Data. IDC (2003). Διαθέσιμο On-Line: http://www.securitymanagement.com/library/Identity_management1003.pdf [Τελευταία Πρόσβαση 05/02/2007].

[64] **Kurose, J. & Ross, K.**: "Computer Networking". 3rd Edition. Pearson Education Inc, Boston (2005).

[65] **Laudon, K.C. & Laudon, J.P.**: "Management Information Systems". 9th Edition. Prentice Hall, Upper Saddle River, NJ (2006).

[66] **Leach, P. and Newman, C.**: "RFC 2831 - Using Digest Authentication as a SASL Mechanism". The Internet Engineering Task Force (2000). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc2831.txt [Τελευταία Πρόσβαση 05/02/2007].

[67] **Legg, S. (Ed.)**: "RFC 4517 - Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules". The Internet Engineering Task Force (2006). Διαθέσιμο On-Line: http://www.isi.edu/in-notes/rfc4517.txt [Τελευταία Πρόσβαση 05/02/2007].

[68] **Liberty Alliance Project**: "Introduction to the Liberty Alliance Identity Architecture, Revision 1.0". (2003). Διαθέσιμο On-Line: http://xml.coverpages.org/LibertyAllianceArchitecture200303.pdf [Τελευταία Πρόσβαση 05/02/2007].

[69] **Liberty Alliance Project**: "Liberty Identity Federation Framework Architecture Overview v1.2, errata v1.0". (2005). Διαθέσιμο On-Line: http://www.projectliberty.org [Τελευταία Πρόσβαση 05/02/2007].

[70] **Liberty Alliance Project**: "Liberty Specs Tutorial v2". (2007). Διαθέσιμο On-Line: http://www.projectliberty.org/liberty/content/download/423/2832/file/tutorialv2.pdf [Τελευταία Πρόσβαση 05/02/2007].

[71] **Liberty Alliance Project**: "Liberty Technical Glossary v1.4". (2005). Διαθέσιμο On-Line: http://www.projectliberty.org/liberty/content/download/1233/8003/file/liberty-glossary-v1.4.pdf [Τελευταία Πρόσβαση 05/02/2007].

[72] **Liberty Alliance Project**: "Liberty Trust Models Guidelines v1.0". (2003). Διαθέσιμο On-Line: http://www.projectliberty.org/liberty/content/download/1232/8000/file/liberty-trust-models-guidelines-v1.0.pdf [Τελευταία Πρόσβαση 05/02/2007].

[73] **Liberty Alliance Project**: "The Liberty Alliance Web Site". (2007). Διαθέσιμο On-Line: http://www.projectliberty.org [Τελευταία Πρόσβαση 05/02/2007].

[74] **Liberty Alliance Project**: "Whitepaper: Benefits of Federated Identity to Government". (2004). Διαθέσιμο On-Line: http://www.projectliberty.org [Τελευταία Πρόσβαση 05/02/2007].

[75] **Linn, J.**: "RFC 2743 - Generic Security Service Application Program Interface Version 2, Update 1". The Internet Engineering Task Force (2000). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc2743.txt [Τελευταία Πρόσβαση 05/02/2007].

[76] **Lloyd, B. & Simpson, W.**: "RFC 1334 - PPP Authentication Protocols". The Internet Engineering Task Force (1992). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc1334.txt [Τελευταία Πρόσβαση 05/02/2007].

[77] **McMillan, R. and Cowley, S.**: "Liberty Alliance holdout IBM ends resistance, joins". IDG News Service. Network World (2004). Διαθέσιμο On-Line: http://www.networkworld.com/news/2004/1020liberty.html [Τελευταία Πρόσβαση 05/02/2005].

[78] **Melnikov, A. (Ed.) & Zeilenga, K. (Ed.)**: "RFC 4422 - Simple Authentication and Security Layer (SASL)". The Internet Engineering Task Force (2006). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc4422.txt [Τελευταία Πρόσβαση 05/02/2007].

[79] **Microsoft Corporation**: "Active Directory Collection". Microsoft Windows Server TechCenter. Microsoft TechNet. Microsoft Corporation, Redmond WA (2003). Διαθέσιμο On-Line: http://technet2.microsoft.com/WindowsServer/en/library/6f8a7c80-45fc-4916-80d9-16e6d46241f91033.mspx?mfr=true [Τελευταία Πρόσβαση 05/02/2007].

[80] **Microsoft Corporation**: "Active Directory Concepts". Microsoft Windows Server TechCenter. Microsoft TechNet. Microsoft Corporation, Redmond WA (2005). Διαθέσιμο On-Line: http://technet2.microsoft.com/WindowsServer/f/?en/library/77a19ae8-bffe-42ca-a841-3d18ea62dc9b1033.mspx [Τελευταία Πρόσβαση 05/02/2007].

[81] **Microsoft Corporation**: "Active Directory LDAP Compliance". Microsoft Windows Server 2003. Microsoft Corporation, Redmond WA (2003). Διαθέσιμο On-Line: http://download.microsoft.com/download/d/c/8/dc83e0b8-fc2c-4af4-bd27-45b5963ad98d/AD%20LDAP%20Compliance.doc [Τελευταία Πρόσβαση 05/02/2007].

[82] **Microsoft Corporation**: "How To Implement Forms-Based Authentication in Your ASP.NET Application by Using C# .NET". Microsoft Help and Support. Micro-

soft Corporation, Redmond WA (2006). Διαθέσιμο On-Line: http://support.microsoft.com/kb/301240 [Τελευταία Πρόσβαση 05/02/2007].

[83] **Microsoft Corporation**: "IIS 6.0 Documentation (IIS 6.0)". Microsoft Windows Server 2003 TechCenter. Microsoft TechNet. Microsoft Corporation, Redmond WA (2007). Διαθέσιμο On-Line: http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/848968f3-baa0-46f9-b1e6-ef81dd09b015.mspx?mfr=true [Τελευταία Πρόσβαση 05/02/2007].

[84] **Microsoft Corporation**: "Integrated Windows Authentication (IIS 6.0)". Microsoft Windows Server 2003 TechCenter. Microsoft TechNet. Microsoft Corporation, Redmond WA (2007). Διαθέσιμο On-Line: http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/523ae943-5e6a-4200-9103-9808baa00157.mspx?mfr=true [Τελευταία Πρόσβαση 05/02/2007].

[85] **Microsoft Corporation**: "Microsoft Corporation Web Site". (2007). Διαθέσιμο On-Line: http://www.microsoft.com [Τελευταία Πρόσβαση 05/02/2007].

[86] **Microsoft Corporation:** "Microsoft Identity and Access Management Series v1.4 - Fundamental Concepts". Microsoft Solutions for Security and Compliance. Microsoft Corporation, Redmond WA (2006). Διαθέσιμο On-Line: http://www.microsoft.com/downloads/details.aspx?familyid=794571E9-0926-4C59-BFA9-B4BFE54D8DD8&displaylang=en [Τελευταία Πρόσβαση 04/02/2007].

[87] **Microsoft Corporation**: "Microsoft Identity and Access Management Series v1.4 - Password Management". Microsoft Solutions for Security and Compliance. Microsoft Corporation, Redmond WA (2006). Διαθέσιμο On-Line: http://www.microsoft.com/downloads/details.aspx?familyid=794571E9-0926-4C59-BFA9-B4BFE54D8DD8&displaylang=en [Τελευταία Πρόσβαση 04/02/2007].

[88] **Microsoft Corporation**: "What Are Security Identifiers?". Microsoft Windows Server TechCenter. Microsoft TechNet. Microsoft Corporation, Redmond WA (2003). Διαθέσιμο On-Line: http://technet2.microsoft.com/WindowsServer/f/?en/library/c9bfc4c3-7aaf-4ca0-b818-db0de3a6fc871033.mspx [Τελευταία Πρόσβαση 05/02/2007].

[89] **Mozilla Developer Center**: "JavaScript". Mozilla.org (2007). Διαθέσιμο On-Line: http://developer.mozilla.org/en/docs/JavaScript [Τελευταία Πρόσβαση 05/02/2007].

[90] **Myers, J. and Rose, M.**: "RFC 1939 - Post Office Protocol - Version 3". The Internet Engineering Task Force (1996). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc1939.txt [Τελευταία Πρόσβαση 05/02/2007].

[91] **National Bureau of Standards**: "Data Encryption Standard". Federal Information Processing Standards Publication 46. Government Printing Office, Washington, D.C. (1977).

[92] **National Institute of Standards and Technology**: "Advanced Encryption Standard (AES)". Federal Information Processing Standards Publication 197. Department

of Commerce. U.S. Government, Washington, D.C. (2001). Διαθέσιμο On-Line: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf [Τελευταία Πρόσβαση 05/02/2006].

[93] **National Institute of Standards and Technology**: "Electronic Authentication Guideline - Special Publication 800-63". National Institute of Standards and Technology. Technology Administration. U.S. Department of Commerce, Gaithersburg (2006) . Διαθέσιμο On-Line: http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf [Τελευταία Πρόσβαση 04/02/2007]

[94] **Netscape**: "Persistent Client State HTTP Cookies (Preliminary Specification)". Netscape (1999). Διαθέσιμο On-Line: http://wp.netscape.com/newsref/std/cookie_spec.html [Τελευταία Πρόσβαση 05/02/2006].

[95] **Neuman, C. & Ts'o, T.**: "Kerberos: An Authentication Service for Computer Networks". IEEE Communications Magazine. 32(9):33-38 (1994). Διαθέσιμο On-Line από το Information Sciences Institute/University of Southern California: http://gost.isi.edu/publications/kerberos-neuman-tso.html [Τελευταία Πρόσβαση 05/02/2006].

[96] **Neuman, C., Yu, T., Hartman, S., Raeburn, K.**: "RFC 4120 - The Kerberos Network Authentication Service (V5)". The Internet Engineering Task Force (2005). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc4120.txt [Τελευταία Πρόσβαση 05/02/2007].

[97] **Newman, C.**: "RFC 2444 - The One-Time-Password SASL Mechanism". The Internet Engineering Task Force (1998). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc2444.txt [Τελευταία Πρόσβαση 05/02/2007].

[98] **Norway.No**: "Mypage". Ministry of Government Administration and Reform. Government of Norway (2007). Διαθέσιμο On-Line: http://www.norway.no [Τελευταία Πρόσβαση 05/02/2007].

[99] **Nystrom, M.**: "RFC 2808 - The SecurID(r) SASL Mechanism". The Internet Engineering Task Force (2000). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc2808.txt [Τελευταία Πρόσβαση 05/02/2007].

[100] **OASIS**: "Organization for the Advancement of Structured Information Standards Web Site". (2007). Διαθέσιμο On-Line: http://www.oasis-open.org [Τελευταία Πρόσβαση 05/02/2007].

[101] **OASIS**: "SAML v2.0 Executive Overview (Committee Draft 01)". Security Services Technical Committee. Organization for the Advancement of Structured Information Standards (2005). Διαθέσιμο On-Line: http://www.oasis-open.org/committees/documents.php?wg_abbrev=security [Τελευταία Πρόσβαση 05/02/2007].

[102] **OASIS**: "Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) v2.0". Security Services Technical Committee. Organization for the Advancement of Structured Information Standards (2005). Διαθέσιμο On-Line: http://docs.oasis-open.org/security/saml/v2.0/ [Τελευταία Πρόσβαση 05/02/2007].

[103] **OASIS**: "Security Assertion Markup Language (SAML) v2.0 - Technical Overview (Working Draft)". Organization for the Advancement of Structured Information Standards (2006). Διαθέσιμο On-Line: http://www.oasis-open.org/committees/documents.php?wg_abbrev=security [Τελευταία Πρόσβαση 05/02/2007]

[104] **OASIS**: "Security Assertion Markup Language (SAML)". Security Services Technical Committee. Organization for the Advancement of Structured Information Standards (2007). Διαθέσιμο On-Line: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security [Τελευταία Πρόσβαση 05/02/2007].

[105] **OASIS**: "Trust Models Guidelines". Organization for the Advancement of Structured Information Standards (2004). Διαθέσιμο On-Line: http://www.oasis-open.org/committees/documents.php?wg_abbrev=security [Τελευταία Πρόσβαση 05/02/2007]

[106] **OASIS**: "Web Services Security: SOAP Message Security 1.0 (WS-Security)". Web Services Security (WSS) Technical Committee. Organization for the Advancement of Structured Information Standards (2004). Διαθέσιμο On-Line: http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0 [Τελευταία Πρόσβαση 05/02/2007].

[107] **OATH**: "OATH - Intiative For Open Authentication Web Site" (2007). Διαθέσιμο On-Line: http://www.openauthentication.org [Τελευταία Πρόσβαση 05/02/2007].

[108] **OATH**: "Reference Architecture, Release 1.0". Initiative for Open AuTHentication - OATH (2005). Διαθέσιμο On-Line: http://www.audiosmartcard.com/communique/OATHReferenceArchitecturev1.pdf [Τελευταία Πρόσβαση 05/02/2007].

[109] **Offentlig Information Online**: "Federated Identity and Access Management in the Danish Public Sector". Government of Danmark (2007). Διαθέσιμο On-Line: http://www.oio.dk/arkitektur/brugerstyring/English [Τελευταία Πρόσβαση 05/02/2007].

[110] **Office of the e-Envoy**: "Registration and Authentication e-Government Strategy Framework Policy and Guidelines v3.0".Cabinet Office. UK Government, London (2002). Διαθέσιμο On-Line: http://www.cabinetoffice.gov.uk/csia/documents/pdf/RegAndAuthentn0209v3.pdf [Τελευταία Πρόσβαση 05/02/2007].

[111] **OpenSSO:** "Open Web SSO Project (OpenSSO)". The OpenSSO Project (2007). Διαθέσιμο On-Line: http://opensso.dev.java.net [Τελευταία Πρόσβαση 05/02/2007]

[112] **Oracle**: "Oracle Corporation Web Site". (2007). Διαθέσιμο On-Line: http://www.oracle.com [Τελευταία Πρόσβαση 05/02/2007].

[113] **Passlogix**: "Passlogix, Inc. Web Site". (2007). Διαθέσιμο On-Line: http://www.passlogix.com [Τελευταία Πρόσβαση 05/02/2007].

[114] **Pfitzmann, B. and Waidner, M.**: "Federated Identity-Management Protocols - Where User Authentication Protocols May Go". *In* Security Protocols — 11th International Workshop, Cambridge UK (2003). Lecture Notes in Computer Sci-

ence. Springer-Verlag, Berlin Germany (To appear, 2004). Διαθέσιμο On-Line: http://www.zurich.ibm.com/security/publications/2003/PfiWai2003FIM-BBAE-Cambridge.pdf [Τελευταία Πρόσβαση 05/02/2007].

[115] **Pierson, N.:** "Overview of Active Directory Federation Services in Windows Server 2003 R2". Microsoft Windows Server 2003 R2. Windows Server System. Microsoft Corporation, Redmond WA (2005). Διαθέσιμο On-Line: http://download.microsoft.com/download/d/8/2/d827e89e-760a-40e5-a69a-4e75723998c5/ADFS_Overview.doc [Τελευταία Πρόσβαση 05/02/2007].

[116] **Rivest, R.**: "RFC 1321 - The MD5 Message-Digest Algorithm". The Internet Engineering Task Force (1992). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc1321.txt [Τελευταία Πρόσβαση 05/02/2007].

[117] **Rose, M.**: "RFC 3080 - The Blocks Extensible Exchange Protocol Core". The Internet Engineering Task Force (2001). Διαθέσιμο On-Line: http://www.rfc-editor.org/rfc/rfc3080.txt [Τελευταία Πρόσβαση 05/02/2007].

[118] **RSA Security**: "RSA SecurID® USB Tokens: Consolidating Digital Credentials onto a Single Device". A white paper for IT and business managers. RSA Security Inc, Ireland (2003). Διαθέσιμο On-Line: http://www.indevis.de/dokumente/rsa_securid_usb_wp.pdf [Τελευταία Πρόσβαση 05/02/2007].

[119] **RSA Security**: "RSA Security Inc. Web Site". (2007). Διαθέσιμο On-Line: http://www.rsa.com [Τελευταία Πρόσβαση 05/02/2007].

[120] **RSA Security**: "Single Sign-on: Putting an End to the Password Management Nightmare". White Paper. RSA Security Inc, Ireland (2005). Διαθέσιμο On-Line: http://www.internetworking.ch/display.cfm?id=101280 [Τελευταία Πρόσβαση 05/02/2007].

[121] **Saint-Andre, P. (Ed.)**: "RFC 3920 - Extensible Messaging and Presence Protocol (XMPP): Core". The Internet Engineering Task Force (2004). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc3920.txt [Τελευταία Πρόσβαση 05/02/2007].

[122] **Sciberras, A. (Ed.)**: "RFC 4519 - Lightweight Directory Access Protocol (LDAP): Schema for User Applications". The Internet Engineering Task Force (2006). Διαθέσιμο On-Line: http://www.isi.edu/in-notes/rfc4519.txt [Τελευταία Πρόσβαση 05/02/2007].

[123] **Secure Computing**: "Secure Computing Corporation Web Site" (2007). Διαθέσιμο On-Line: http://www.securecomputing.com [Τελευταία Πρόσβαση 05/02/2007].

[124] **Sermersheim, J.(Ed.)**: "RFC 4511 - Lightweight Directory Access Protocol (LDAP): The Protocol". The Internet Engineering Task Force (2006). Διαθέσιμο On-Line: http://rfc.net/rfc4511.html [Τελευταία Πρόσβαση 05/02/2007].

[125] **Shannon, C. E.**: "A mathematical theory of communication". Bell System Technical Journal. 27:.379-423 & 623-656 (1948). Διαθέσιμο On-Line: http://cm.bell-labs.com/cm/ms/what/shannonday/paper.html [Τελευταία Πρόσβαση 04/02/2007].

[126] **Shirey, R.**: "RFC 2828 - Internet Security Glossary". The Internet Engineering Task Force (2000). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc2828.txt [Τελευταία Πρόσβαση 03/02/2007]

[127] **Shodjai, P.:** "Web Services and the Microsoft Platform".Web Services Technical Articles. Microsoft Developer Network - MSDN. Microsoft Corporation, Redmond WA (2006). Διαθέσιμο On-Line: http://msdn2.microsoft.com/en-us/library/aa480728.aspx [Τελευταία Πρόσβαση 05/02/2007].

[128] **SIEMENS**: "Interchange of Data between Administrations: Authentication Policy". Directorate General Enterprise. European Commission, Brussels (2004). Διαθέσιμο On-Line: http://ec.europa.eu/idabc/servlets/Doc?id=18227 [Τελευταία Πρόσβαση 04/02/2007].

[129] **Simpson, W.**: "RFC 1994 - PPP Challenge Handshake Authentication Protocol (CHAP)". The Internet Engineering Task Force (1996). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc1994.txt [Τελευταία Πρόσβαση 05/02/2007].

[130] **Smith, M. (Ed.) & Howes, T.**: "RFC 4515 - Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters". The Internet Engineering Task Force (2006). Διαθέσιμο On-Line: http://www.rfc-editor.org/rfc/rfc4515.txt [Τελευταία Πρόσβαση 05/02/2007].

[131] **Smith, M. (Ed.) & Howes, T.**: "RFC 4516 - Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator". The Internet Engineering Task Force (2006). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc4516.txt [Τελευταία Πρόσβαση 05/02/2007].

[132] **Stanford University**: "Stanford WebAuth". IT Services. Stanford University, Stanford, CA (2006). Διαθέσιμο On-Line: http://webauth.stanford.edu/ [Τελευταία Πρόσβαση 05/02/2006].

[133] **Steiner, J. G., Neuman, B. C. and Schiller, J. I.**: "Kerberos: An authentication service for open network systems". *In* Proceedings of the Winter 1988 Usenix Conference (σελ.191-201). (1988). Διαθέσιμο On-Line: ftp://athena-dist.mit.edu/pub/kerberos/doc/usenix.txt [Τελευταία Πρόσβαση 05/02/2007].

[134] **Stepka, J.**: "SSO and Identity Management". TheServerSide.COM (2005). Διαθέσιμο On-Line: http://www.theserverside.com/tt/articles/article.tss?l=SSOIdentityManagement [Τελευταία Πρόσβαση 05/02/2006].

[135] **Sun Developer Network**: "Java 2 Platform, Enterprise Edition (J2EE) 1.4". Sun Microsystems, Inc. (2006). Διαθέσιμο On-Line: http://java.sun.com/j2ee/1.4/ [Τελευταία Πρόσβαση 05/02/2006].

[136] **Sun Developer Network**: "Java Platform, Enterprise Edition (Java EE)". Sun Microsystems, Inc. (2007). Διαθέσιμο On-Line: http://java.sun.com/javaee/index.jsp [Τελευταία Πρόσβαση 05/02/2006].

[137] **Symlabs**: "Symlabs, Inc.Web Site". (2007). Διαθέσιμο On-Line: http://www.symlabs.com [Τελευταία Πρόσβαση 05/02/2007].

[138] **Temoshok, D.**: "E-Authentication Services and Components". Executive Session - Getting to Green with E-Authentication. The E-Authentication Initiative. General

Services Administration (2004). Διαθέσιμο On-Line: http://www.cio.gov/eauthentication/index.htm [Τελευταία Πρόσβαση 04/11/2006].

[139] **The E-Authentication Initiative**: "Electronic Risk and Requirements Assessment (e-RA)". General Services Administration (2007). Διαθέσιμο On-Line: http://www.cio.gov/eauthentication/era.htm [Τελευταία Πρόσβαση 05/02/2007].

[140] **The E-Authentication Initiative**: "The E-Authentication Credential Assessment Suite". General Services Administration (2007). Διαθέσιμο On-Line: http://www.cio.gov/eauthentication/CredSuite.htm [Τελευταία Πρόσβαση 05/02/2007].

[141] **Tung, B.**: " The Moron's Guide to Kerberos, v2.0". Information Sciences Institute. The University of Southern California (2006). Διαθέσιμο On-Line: http://www.isi.edu/~brian/security/kerberos.html [Τελευταία Πρόσβαση 05/02/2006].

[142] **U.S. General Services Administration**: "Smart Card Technology – A Tutorial". U.S. Federal Government, Washington, DC (2007). Διαθέσιμο On-Line: http://www.smartcard.gov/tutorial/tutorial_text.doc [Τελευταία Πρόσβαση 05/02/2007].

[143] **U.S. Office of Management and Budget**: "E-Authentication Guidance for Federal Agencies". Memorandum M-04-04 to the Heads of all Departments and Agencies. Executive Office of the President, WASHINGTON, D.C. (2003) . Διαθέσιμο On-Line: http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf [Τελευταία Πρόσβαση 05/02/2007]

[144] **U.S. Office of Management and Budget**: "Presidential Initiatives". E-Government Web Site. Executive Office of the President (2007). Διαθέσιμο On-Line: http://www.whitehouse.gov/omb/egov/index.html [Τελευταία Πρόσβαση 05/02/2007]

[145] **UK GovTalk**: "e-Government Interoperability Framework (e-GIF)". Cabinet Office. UK Government, London (2007). Διαθέσιμο On-Line: http://www.govtalk.gov.uk/schemasstandards/egif.asp [Τελευταία Πρόσβαση 05/02/2007].

[146] **UK GovTalk**: "GovTalk: Information on policies and standards for e-government". Cabinet Office. UK Government, London (2007). Διαθέσιμο On-Line: http://www.govtalk.gov.uk/[Τελευταία Πρόσβαση 05/02/2007].

[147] **University of Michigan**: "CoSign: Secure, Intra-Institutional Web Authentication". The University of Michigan, Ann Arbor, MI (2004). Διαθέσιμο On-Line: http://www.umich.edu/~umweb/software/cosign/ [Τελευταία Πρόσβαση 05/02/2006].

[148] **University of Washington**: "Pubcookie: open-source software for intra-institutional web authentication". Computing & Communications. University of Washington, Seattle (2003). Διαθέσιμο On-Line: http://www.pubcookie.org/ [Τελευταία Πρόσβαση 05/02/2006].

[149] **Verisign**: "VeriSign Inc. Web Site" (2007). Διαθέσιμο On-Line: http://www.verisign.com [Τελευταία Πρόσβαση 05/02/2007].

[150] **Wikipedia contributors**: "HTTP cookie". Wikipedia, The Free Encyclopedia (2007). Διαθέσιμο On-Line: http://en.wikipedia.org/w/index.php?title=HTTP_cookie&oldid=105254991 [Τελευταία Πρόσβαση 05/02/2007].

[151] **Wikipedia contributors**: "Phishing". Wikipedia, The Free Encyclopedia (2007). Διαθέσιμο On-Line: http://en.wikipedia.org/w/index.php?title=Phishing&oldid=105622164 [Τελευταία Πρόσβαση 05/02/2007].

[152] **Wikipedia contributors:** "Security token". Wikipedia, The Free Encyclopedia (2007). Διαθέσιμο On-Line: http://en.wikipedia.org/w/index.php?title=Security_token&oldid=104325445 [Τελευταία Πρόσβαση 05/02/2007].

[153] **World Wide Web Consortium:** " XML-Signature Syntax and Processing". XML Signature Working Group. World Wide Web Consortium (2002). Διαθέσιμο On-Line: http://www.w3.org/TR/xmldsig-core/ [Τελευταία Πρόσβαση 05/02/2006].

[154] **World Wide Web Consortium**: "Simple Object Access Protocol (SOAP) v1.2". XML Protocol Working Group. World Wide Web Consortium (2003). Διαθέσιμο On-Line: http://www.w3.org/TR/2003/REC-soap12-part0-20030624/ [Τελευταία Πρόσβαση 05/02/2006].

[155] **Zeilenga, K.(Ed.)**: "RFC 4505 - Anonymous Simple Authentication and Security Layer (SASL) Mechanism". The Internet Engineering Task Force (2006). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc4505.txt [Τελευταία Πρόσβαση 05/02/2007].

[156] **Zeilenga, K.(Ed.)**: "RFC 4510 - Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map". The Internet Engineering Task Force (2006). Διαθέσιμο On-Line: http://www.rfc-editor.org/rfc/rfc4510.txt [Τελευταία Πρόσβαση 05/02/2007].

[157] **Zeilenga, K.(Ed.)**: "RFC 4512 - Lightweight Directory Access Protocol (LDAP): Directory Information Models". The Internet Engineering Task Force (2006). Διαθέσιμο On-Line: http://www.rfc-editor.org/rfc/rfc4512.txt [Τελευταία Πρόσβαση 05/02/2007].

[158] **Zeilenga, K.(Ed.)**: "RFC 4514 -Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names". The Internet Engineering Task Force (2006). Διαθέσιμο On-Line: http://www.rfc-editor.org/rfc/rfc4514.txt [Τελευταία Πρόσβαση 05/02/2007].

[159] **Zeilenga, K.(Ed.)**: "RFC 4518 - Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation". The Internet Engineering Task Force (2006). Διαθέσιμο On-Line: http://www.isi.edu/in-notes/rfc4518.txt [Τελευταία Πρόσβαση 05/02/2007].

[160] **Zeilenga, K.(Ed.)**: "RFC 4616 - The PLAIN Simple Authentication and Security Layer (SASL) Mechanism". The Internet Engineering Task Force (2006). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc4616.txt [Τελευταία Πρόσβαση 05/02/2007].

[161] **Zhu, L., Leach, P., Jaganathan, K. and Ingersoll, W.**: "RFC 4178 - The Simple and Protected Generic Security Service Application Program Interface (GSS-API) Negotiation Mechanism". The Internet Engineering Task Force (2005). Διαθέσιμο On-Line:http://www.ietf.org/rfc/rfc4178.txt [Τελευταία Πρόσβαση 05/02/2007].

[162] **Zorn, G. & Cobb, S.**: "RFC 2433 - Microsoft PPP CHAP Extensions". The Internet Engineering Task Force (1998). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc2433.txt [Τελευταία Πρόσβαση 05/02/2007].

[163] **Zorn, G.**: "RFC 2759 - Microsoft PPP CHAP Extensions, Version 2". The Internet Engineering Task Force (2000). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc2759.txt [Τελευταία Πρόσβαση 05/02/2007].

[164] **Zuccherato, R. and Nystrom, M.**: "RFC 3163 - ISO/IEC 9798-3 Authentication SASL Mechanism". The Internet Engineering Task Force (2001). Διαθέσιμο On-Line: http://www.ietf.org/rfc/rfc3163.txt [Τελευταία Πρόσβαση 05/02/2007].

[165] **ΚτΠ Α.Ε.**: "Διακήρυξη Ανοικτού Διαγωνισμού για το Έργο «Μελέτη και Ανάπτυξη της Κεντρικής Κυβερνητικής Διαδικτυακής Πύλης της Δημόσιας Διοίκησης για την Πληροφόρηση & Ασφαλή Διεκπεραίωση Ηλεκτρονικών Συναλλαγών των Πολιτών / Επιχειρήσεων» - «Εθνική Πύλη ΕΡΜΗΣ»". Κοινωνία της Πληροφορί-ας Α.Ε.. ΥΠ.ΕΣ.Δ.Δ.Α., Αθήνα (2006). Διαθέσιμο On-Line: http://www.ktpae.gr/dec_archive.php?dec_id=127 [Τελευταία Πρόσβαση 04/02/2007].

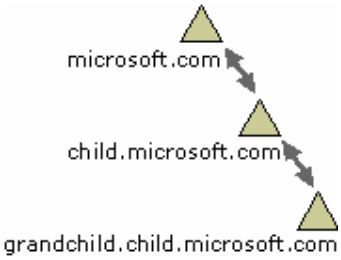
[166] **ΥΠ.ΕΣ.Δ.Δ.Α.**: "ΣΥΖΕΥΞΙΣ - Εθνικό Δίκτυο Δημόσιας Διοίκησης", ΥΠ.ΕΣ.Δ.Δ.Α., Ελληνική Δημοκρατία, Αθήνα (2007). Διαθέσιμο On-Line: http://www.syzefxis.gov.gr [Τελευταία Πρόσβαση 05/02/2007].

ΠΑΡΑΡΤΗΜΑ Α

Έννοιες των Server Εκδόσεων των Λειτουργικών Συστημάτων Microsoft Windows

Το *Domain* είναι ένα σύνολο υπολογιστών και άλλων δικτυακών πόρων οι οποίοι μπορούν να αντιμετωπιστούν στη διαχείρισή τους ως μία ενότητα και διατηρούν μία εγκατάσταση του *Active Directory*, ενώ το *Forest* είναι μία συλλογή από θεωρούμενα ισότιμα *Domains* τα οποία συνδέονται με αμοιβαίες, ασφαλείς συνδέσεις. Βασική προϋπόθεση για τον προσδιορισμό ενός *Forest* είναι η ύπαρξη κοινού σχήματος και καταλόγου. Κάθε *Domain* χαρακτηρίζεται από ένα όνομα, το *DNS* (*Domain Name System*) *Name*. Πολλά *Domains* τα οποία έχουν διαδοχικά ονόματα αποτελούν ένα *Domain Tree* όπως φαίνεται στην παρακάτω Εικόνα.

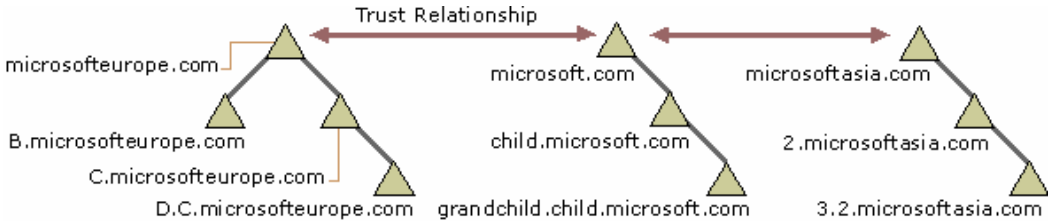
Πηγή: [80]



Εικόνα 70: Το Domain Tree *microsoft.com*

Τα *Forests* των Microsoft Servers είναι ουσιαστικά οι «Σχέσεις Εμπιστοσύνης» (*Trust Relationship*) μεταξύ *Domain Trees*, όπως φαίνεται στην παρακάτω Εικόνα. Οι *Trust Relationships* είναι «δίοδοι αυθεντικοποίησης» οι οποίοι πρέπει να εγκαθίστανται, ώστε οι χρήστες ενός *Domain* να προσπελαύνουν πόρους σε κάποιο άλλο *Domain*

Πηγή:[80]



Εικόνα 71: Ενδεικτική Παράσταση ενός Microsoft *Forest*

Το πρώτο *Domain* που δημιουργείται σε ένα *Domain Tree* ονομάζεται *Tree Root Domain*, ενώ το πρώτο *Domain* ενός *Forest* ονομάζεται *Forest Root Domain*. Η σύνδεση των *Domains* μέσα σε ένα *Tree* και μέσα σε ένα *Forest* βασίζεται στις *Trust Relationships* οι οποίες καθορίζονται μέσω του *Active Directory*. Με κάθε εγκατάσταση *Active Directory* σε ένα νέο *Do-*

main Controller (άρα σε ένα νέο *Domain*) δημιουργούνται αυτόματα *Trusts* ανάλογα με τη θέση του νέου *Domain* στο τρέχον *Forest* [80]:

- *Parent - Child Trust*: Όταν το νέο *Domain* είναι «παιδί» σε ένα *Domain Tree* αυτόματα αποκτά *Trust Relationship* με το αμέσως συνδεδεμένο του *Domain* («πατέρας»). Το συγκεκριμένο *Trust* είναι διπλής κατεύθυνσης, δηλαδή οι χρήστες και των δύο *Domains* μπορούν να προσπελαύνουν πόρους του άλλου *Domain*. Επίσης, η συγκεκριμένη σχέση είναι μεταβατική, με αποτέλεσμα το καθένα νέο «παιδί» *Domain* να αποκτά μέσω των «προγόνων» του *Trust Relationship* με το *Tree Root Domain* του *Tree* στο οποίο εισάγεται.

- *Tree – Root Trust*: Όταν ένα νέο *Tree* δημιουργείται μέσα σε ένα υπάρχον *Forest* τότε αυτόματα δημιουργείται *Trust Relationship* μεταξύ του νέου *Tree Root Domain* και όλων των υπαρχόντων *Tree Root Domains*. Το συγκεκριμένο *Trust* είναι διπλής κατεύθυνσης και χαρακτηρίζεται από μεταβατικότητα, οπότε, μέσω και του παραπάνω *Trust*, κάθε *Domain* μέσα σε ένα *Tree* αποκτά *Trust Relationship* με οποιοδήποτε άλλο *Domain* μέσα στο ίδιο *Forest*.