ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΣΤΑ ΠΛΗΡΟΦΟΡΙΑΚΑ ΣΥΣΤΗΜΑΤΑ

(M.I.S)

«Ασφάλεια Ηλεκτρονικών Συναλλαγών και Internet. Η περίπτωση των Εικονικών Εταιριών.»

Καθηγητής : Ν.Πρωτόγερος
Εξεταστής : Α.Οικονομίδης
Επιμέλεια Παρουσίασης : Κατσίδου Μαρία Α.Μ.02/05

Φεβρουάριος, Θεσσαλονίκη 2007

Ανάλυση του θέματος-προβλήματος.

Το θέμα μας αποτελείται από δύο μέρη

- Ασφάλεια ηλεκτρονικών συναλλαγών και Internet.
- Η περίπτωση των Εικονικών Εταιριών.

Η ανάλυση που θα ακολουθήσουμε και στα δύο μέρη θα είναι παρόμοια, δηλαδή :

Α. Κατευθυντήριους Ορισμούς (όπως της εμπιστευτικότητας, της ακεραιότητας,της διαθεσιμότητας και της Εικονικής Εταιρίας).

↓

Β. Ανάπτυξη προβλημάτων (που ελλοχεύουν στις ηλεκτρονικές συναλλαγές, στις Εικονικές Εταιρίες).

↓

Γ. Ανάπτυξη Λύσεων (για την αντιμετώπιση των προβλημάτων τόσο στις ηλεκτρονικές συναλλαγές, όσο και στις Εικονικές Εταιρίες).

Ασφάλεια ηλεκτρονικών συναλλαγών και Internet.

- **Εμπιστευτικότητα :** Είναι η μη αποκάλυψη ευαίσθητων πληροφοριών σε χρήστες χωρίς εξουσιοδότηση.
- **Ακεραιότητα :** Είναι η διαφύλαξη της ακρίβειας και της πληρότητας των πληροφοριών.
- **Διαθεσιμότητα :** Είναι η δυνατότητα άμεσης πρόσβασης στις πληροφορίες / υπηρεσίες (χωρίς καθυστέρηση).

Γιατί είναι σημαντικές οι ασφαλείς συναλλαγές; ⟶ Καθιερώνουν την **εμπιστοσύνη**.

Η **εμπιστοσύνη** ορίζεται εφόσον :

- Ορισθεί η ταυτότητα κάθε ομάδας που επικοινωνεί.
- Είναι εγγυημένη η μυστικότητα των συναλλαγών.
- Υπάρχει πίστη ότι η συναλλαγή δεν έχει τροποποιηθεί.
- Δεν αμφισβητείται το γεγονός πραγματοποίησης της συναλλαγής.

Υπάρχει ανασφάλεια στο Διαδίκτυο;

Ναι, διότι σχεδιάστηκε για την διασύνδεση ετερογενών δικτύων, με σκοπό την εκμετάλλευση πόρων / πληροφοριών και όχι την παροχή ασφάλειας, οπότε υπάρχουν πολλοί λόγοι ανασφάλειας σε αυτό.

Οι Κίνδυνοι που απειλούν τις ηλεκτρονικές συναλλαγές.

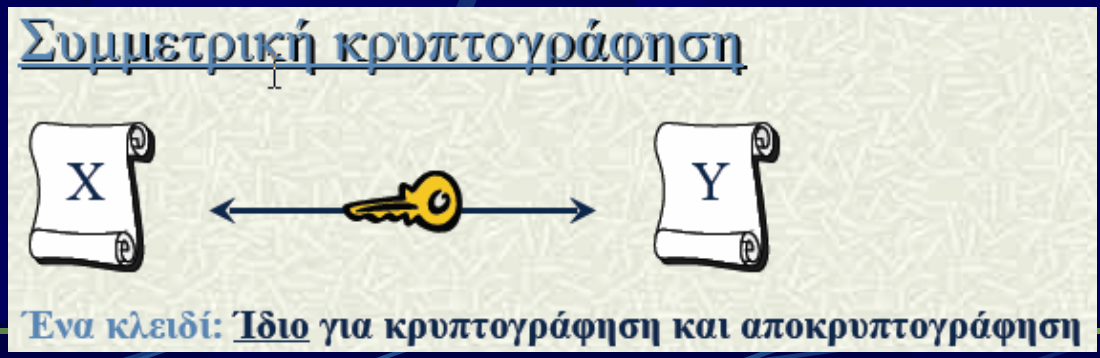
- Υποκλοπή δεδομένων.
- Απάτες / Ψεύτικες συναλλαγές.
- Άρνηση Εξυπηρέτησης.
- Η μεταμφίεση.
- Η κατάχρηση πληροφοριακών αγαθών.
- Η μη εξουσιοδοτημένη πρόσβαση σε η/υ και σε δίκτυα η/υ.
- Προγράμματα Spyware και Dialers.
- Το Phising.
- Τα αυτόνομα κακόβουλα προγράμματα όπως Ιοί, Σκουλήκια και Δούρειοι Ίπποι.

Οι Λύσεις που προβάλλονται για την διασφάλιση των ηλεκτρονικών συναλλαγών.

1. **Κρυπτογράφηση** (Συμμετρική – Ασύμμετρη – Δημοσίου Κλειδιού PKI).

Τα συστήματα κρυπτογράφησης αποτελούνται από το απλό κείμενο, τον κρυπτογραφικό αλγόριθμο, το κρυπτογραφημένο κείμενο και το κλειδί.

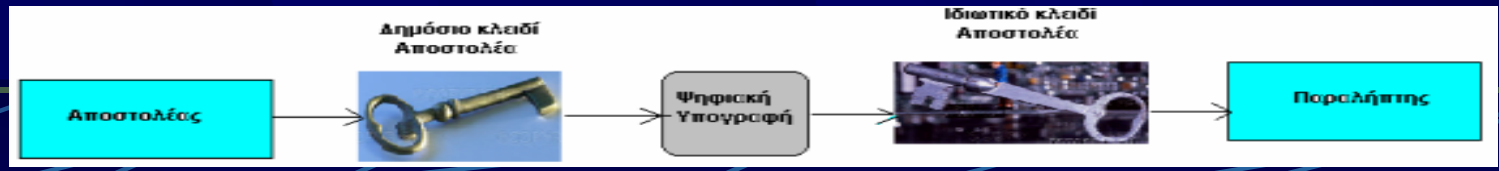
- **Συμμετρική :** Σε αυτή χρησιμοποιείται το ίδιο κλειδί τόσο για την κρυπτογράφηση, όσο και για την αποκρυπτογράφηση.



- **Ασύμμετρη :** Στο σύστημα αυτό χρησιμοποιούνται ζευγάρια κλειδιών (δημόσιο, ιδιωτικό), το ένα χρησιμοποιείται για την κρυπτογράφηση του μηνύματος, ενώ το άλλο για την αποκρυπτογράφηση του.

2. **Υποδομή Δημοσίου Κλειδιού (Public Key Infrastructure) :** Αποτελείται από έξι διαφορετικά μέρη που λειτουργούν μαζί για να δημιουργήσουν βάση ασφάλειας.

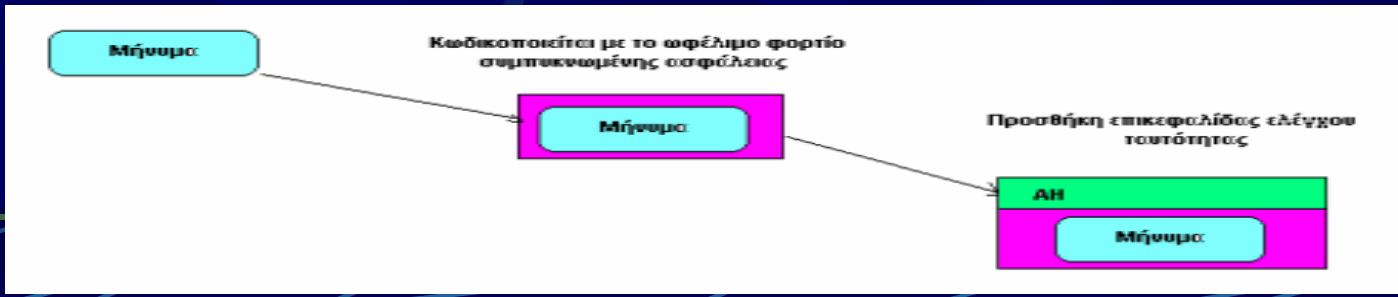
- **Κρυπτογράφηση Δημοσίου Κλειδιού :** Δημιουργείται από ένα μαθηματικό κώδικα που βασίζεται σε έναν αλγόριθμο και σε μία τιμή, με έναν συμπληρωματικό αλγόριθμο και άλλη τιμή. Ο πρώτος κρυπτογραφεί το μήνυμα και ο άλλος το αποκρυπτογραφεί (και αντίστροφα). Επομένως ο ένας θα είναι ο δημόσιος και ο άλλος ο ιδιωτικός.
- **Ψηφιακές Υπογραφές :** Η καθεμιά αποτελεί ένα κρυπτογραφικό μηχανισμό, που βεβαιώνει την πηγή προέλευσης και το περιεχόμενο ενός μηνύματος.



- **Συνάρτηση Ταξινόμησης Μηνύματος (one way hashes) :** Παρέχει πραγματικά αξιόπιστο έλεγχο ακεραιότητας του μηνύματος.

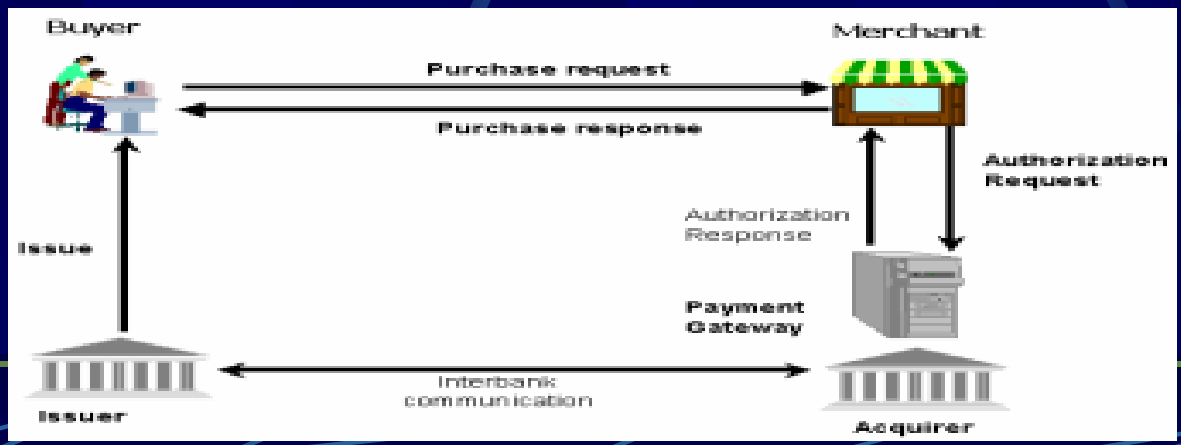
- **Ψηφιακοί Φάκελοι :** Συνδυάζουν και τα δύο συστήματα κρυπτογράφησης, προκειμένου να χρησιμοποιηθούν τα καλύτερα χαρακτηριστικά τους. Χρησιμοποιούνται για την εγκατάσταση αμφίδρομης επικοινωνίας.
- **Αρχές Πιστοποίησης (Certifying Authorities) :** Είναι εμπορικοί οργανισμοί που έχουν σαν κύριο μέλημά τους την επικύρωση της ταυτότητας των χρηστών, αλλά και των ψηφιακών καταστημάτων του Διαδικτύου.
- **Αρχές Έκδοσης Εγγράφων (Registration Authorities) :** Είναι αρχές που εγγράφουν ή ορίζουν νέους χρήστες στο PKI. Αποτελούν τον μεσάζοντα μεταξύ των χρηστών και του CA.

3. **IPSec (Internet Protocol Security) :** Αν κάποιος συνδεθεί με την δικτυακή μας τοποθεσία και πραγματοποιήσει μία παραγγελία, το πρωτόκολλο αυτό βεβαιώνει ότι η παραγγελία αυτή φθάνει αμετάβλητη, αδιάβαστη και προερχόμενη από το άτομο που ισχυρίζεται ότι την πραγματοποίησε.



4. **SSL (Secure Socket Layer) :** Είναι μία διαδικτυακή διεπαφή επικοινωνίας που επιτρέπει την ασφαλή επικοινωνία μεταξύ αγοραστή και πωλητή.

5. **SET (Secure Electronic Transaction) :** Είναι ένα πολύπλοκο συμπαγές σύστημα, που βασίζεται στην κρυπτογράφηση με δημόσιο κλειδί και σε ψηφιακά πιστοποιητικά για την προστασία κάθε συναλλαγής.



6. Ηλεκτρονικές Υπηρεσίες :

- **Ηλεκτρονικό Πορτοφόλι :** Είναι η έξυπνη κάρτα που φιλοδοξεί να υποκαταστήσει καθημερινά τις συναλλαγές μικρού ύψους. (CyberCash, χρησιμοποιεί PKI κρυπτογράφηση και έχει αποθηκευμένους αριθμούς πιστωτικών καρτών)
- **Ηλεκτρονικό Χρήμα :** Είναι το σύγχρονο μέσο πληρωμής στο Διαδίκτυο, που βασίζεται στην ανταλλαγή πραγματικού χρήματος με ηλεκτρονικό τρόπο.
- **Ηλεκτρονικές Επιταγές :** Είναι η εξέλιξη των παραδοσιακών επιταγών, που υπογράφονται και μεταβιβάζονται ηλεκτρονικά. (CheckFee, προσφέρει την λύση ηλεκτρονικών πληρωμών για μηνιαίους λογαριασμούς)
- **Ψηφιακά Μετρητά :** Βασίζονται σε λογαριασμούς χρέωσης και πίστωσης και επιτρέπει τις παρορμητικές αγορές. (NetCash, CyberCoin)

7. **Firewalls (Τείχη Προστασίας) :** Είναι προγράμματα προστασίας που έχουν την δυνατότητα :

- Να εμποδίζουν ιούς, σκουλήκια, δούρειους ίππους και προγράμματα τύπου spyware, από το να εγκατασταθούν στον η/υ μας.
- Να εμποδίζουν αγνώστους, από το να έχουν πρόσβαση στον η/υ μας.
- Να παρουσιάζουν στατιστικά στοιχεία με την κίνηση από και προς τον η/υ μας.
- Να εμποδίζουν προγράμματα τύπου Dialers, από το να πραγματοποιούν τηλεφωνικές κλήσεις, μέσω της τηλεφωνικής μας γραμμής.
- Να μας ειδοποιούν, όταν ο η/υ μας δέχεται κάποια επίθεση.

Η περίπτωση των Εικονικών Εταιριών (Virtual Enterprises).

- **Εικονική Εταιρία :** Είναι η προσωρινή συνεργασία γεωγραφικά απομακρυσμένων εταιριών στις αλυσίδες αξιών, για να μοιραστούν ικανότητες και πόρους, ώστε να ανταποκρίνονται ταχύτερα και με μεγαλύτερη επάρκεια στις επιχειρηματικές ευκαιρίες. Η συνεργασία αύτη, αποτελεί τον καίριο παράγοντα για την επιβίωση στο ανταγωνιστικό επιχειρηματικό περιβάλλον.

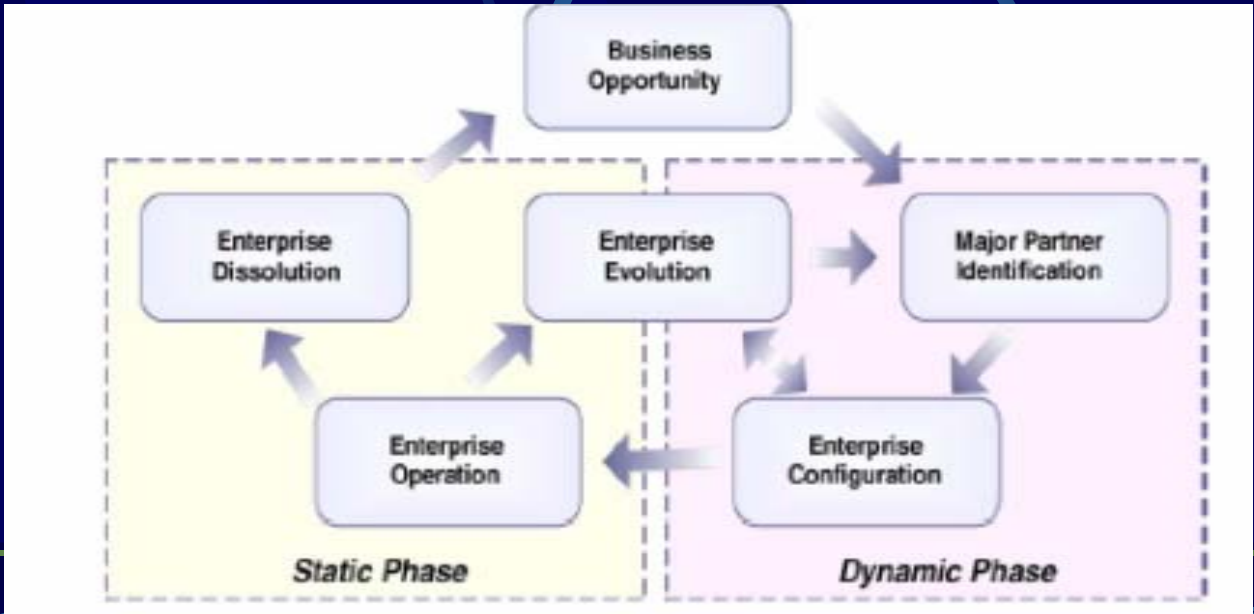
Οι λόγοι δημιουργίας των VEs είναι :

- Για να αυξήσουν τον ανταγωνισμό, την χρηστικότητα των πόρων, την κλίμακα των επιχειρήσεων και να διαμοιράσουν τις ικανότητες των συνεργατών τους.
- Για να μειώσουν το κόστος παραγωγής, να βελτιώσουν την ποιότητα και να μειώσουν τον χρόνο που απαιτείται για την μεταφορά των προ'ι'όντων από την παραγωγή στην αγορά.
- Για να αντεπεξέρχονται άμεσα σε μία επιχειρηματική ευκαιρία, αναπτύσσοντας εργασιακό περιβάλλον και διαχειρίζοντας τους πόρους που προέρχονται από τις συνεργαζόμενες εταιρίες.

Ο κύκλος ζωής της VE.

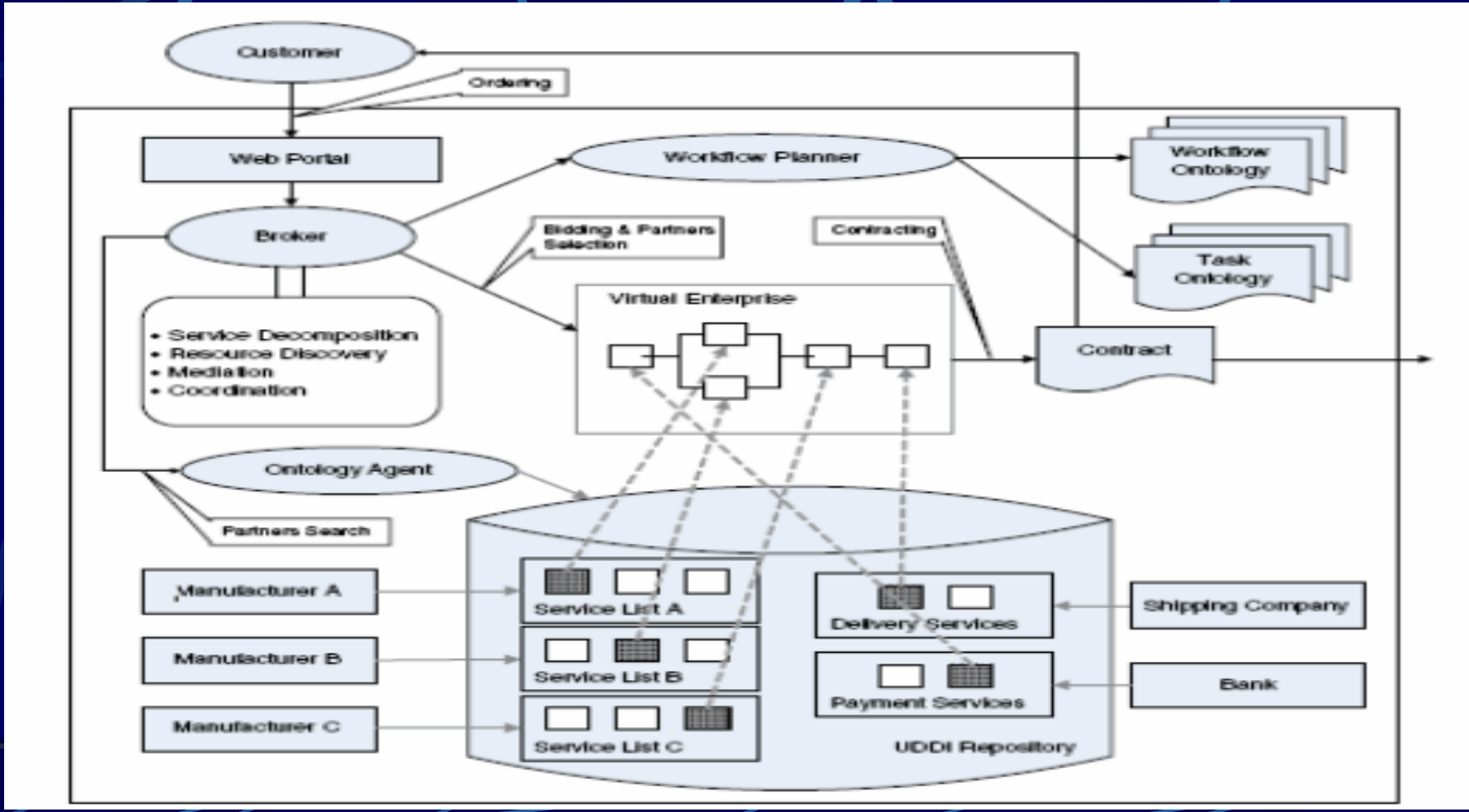
Ο κύκλος ζωής της VE αποτελείται από τα έξι ακόλουθα στάδια, όπως διαφαίνεται από την παρακάτω εικόνα :

- **Επιχειρηματική Ευκαιρία.**
- **Αναγνώριση Συνεργατών.**
- **Εταιρική Διαμόρφωση.**
- **Εταιρική Λειτουργία.**
- **Εταιρική Εξέλιξη.**
- **Εταιρική Διάλυση.**



Η διαδικασία δημιουργίας της VE.

Περιγράφουμε την διαδικασία αυτή με μία αρχιτεκτονική που βασίζεται σε τέσσερις πράκτορες τον Σχεδιαστή ροής εργασίας, τον Μεσίτη, τον Οντολογικό και των Υπηρεσιών.



Προβλήματα που αντιμετωπίζουν οι VEs.

Α. Της Συγχώνευσης : Οι δομές που αναπτύσσουν οι VEs αντιμετωπίζουν μεγάλες προκλήσεις όπως :

- **Ετερογένεια** : Οφείλεται στην ύπαρξη ασύμμετρων προοπτικών, δομών λογισμικού, πρακτικών μεταξύ των συμμετέχουσων εταιριών.
- **Ευελιξία** : Οφείλεται στην ανάγκη για μάθηση, αλλαγή και εξαιρετικό χειρισμό ειδικών περιπτώσεων.
- **Πολυπλοκότητα** : Οφείλεται στον μεγάλο αριθμό και στην ασάφεια των ενδο-εξαρτήσεων μεταξύ των συνεργατών, των ενεργειών, των πόρων και των ικανοτήτων τους.

Β. Της Νομοθεσίας : Πολλά παραδοσιακά σημεία αναφοράς στην νομοθεσία, όπως η εθνικότητα, τα κεντρικά γραφεία, η νομική προσωπικότητα καθώς και άλλα δεν επαρκούν για να καλύψουν την VE.

Γ. Της Εμπιστευτικότητας – Ασφάλειας : Η επιτυχία κάθε VE βασίζεται στην πλήρη διαπερατότητα της πληροφορίας και στον ορθό διαμοιρασμό των πόρων της, γεγονός που οδηγεί στην εμφάνιση προβλημάτων ασφάλειας και διαχείρισης εξουσίας.

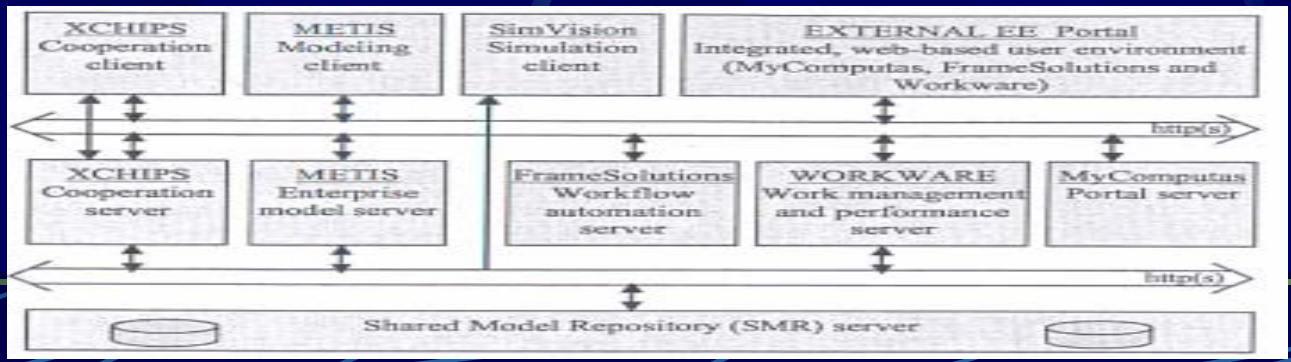
Οι λύσεις που προτάσσονται για την αντιμετώπιση των προβλημάτων των VEs.

αντιμετωπίζει

Α. Τα αλληλεπιδραστικά μοντέλα ⟶ τις προκλήσεις της **συγχώνευσης.**

Το γεγονός αυτό γίνεται αντιληπτό, αν αναφέρουμε την δομή του EXTERNAL που συγχωνεύει τα εξής πέντε αλληλεπιδραστικά μοντέλα :

- **WORKWARE :** Παρέχει λίστες εργασίας, νομοθεσία δικαιοδοσίας, σημειώσεις ενημέρωσης, έλεγχο πρόσβασης και διαχείριση εγγράφων.
- **METIS :** Βοηθά στην κατασκευή και οπτικοποίηση σύγχρονων μοντέλων στην εταιρία παρέχοντας κατανόηση στους συνεργάτες και βοηθά στον σχεδιασμό της συνεργασίας.
- **XCHIPS :** Παρέχει συνεργατικές συνεδρίες πραγματικού χρόνου και στενή συνεργασία για συγκεκριμένα καθήκοντα.
- **FRAMESOLUTIONS :** Είναι πλαίσιο εργασίας για την δημιουργία εφαρμογών παραδοσιακών ροών εργασίας.
- **SIM VISION :** Παρέχει αναγνώριση των πιθανών αιτίων καθυστέρησης, προβάλλοντας τα τρέχοντα σχέδια δουλειάς και εντοπισμού προσωπικού.

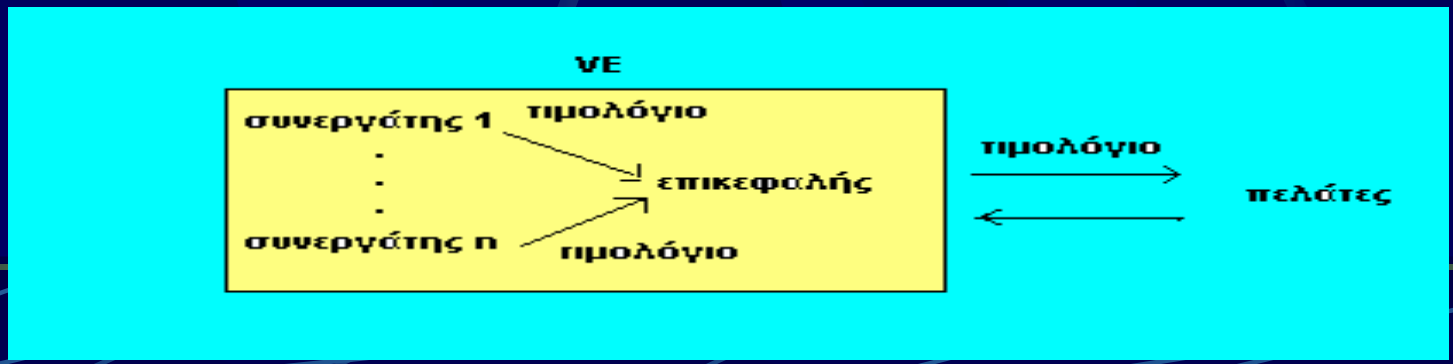


Β. Ο Πορτογαλικός νόμος ανταποκρίνεται στην δημιουργία **νομοθετικού πλαισίου.**

Η Πορτογαλική νομοθεσία εμπεριέχει νόμους, όσον αφορά την συνεργασία των εταιριών, που ανταποκρίνονται στην μορφή της VE, όπως :

- **Ο Βαθμωτός Νόμος :** Εισήγαγε την συμφωνία των εταιριών. Η περίληψη αυτού αναφέρει «η νομική δημιουργία παρέχει το νομικό πλαίσιο για μία μορφή συνεργασίας εταιριών, που μπορεί να αποσκοπεί σε αρκετούς στόχους, αλλά απαιτεί απλότητα». Περαιτέρω προκαταβάλλει τον αποκλεισμό μελών από την εκάστοτε συνεργασία εταιριών, αναφέροντας «το συμβόλαιο συνεργασίας εταιριών μπορεί να διαλυθεί για κάποιο από τα συμβαλλόμενα μέλη, αν υπάρχουν αναφορές άλλων μελών, εμφανίζοντας την αιτία».

Το πλαίσιο εργασίας της, όπως προβλέπεται από αυτόν, επιτρέπει μία πλευρά της Εικονικότητας που είναι πολύ σημαντική για την VE, το ότι εμφανίζεται ως μία εταιρία. **Πως επιτυγχάνεται;**



διαφυλάττει

Γ. Η Οργάνωση πολιτικής ασφάλειας μέσω μοντέλων → την ασφάλεια – εμπιστευτικότητα.

Η **πολιτική ασφάλειας** αφορά τόσο την **ασφάλεια επικοινωνίας του δικτύου**, όσο και την **ασφάλεια των πληροφοριακών συστημάτων**.

↓

Η οργάνωση πολιτικής ασφάλειας στις VEs :

- Καθορίζουμε την επιχειρηματική διαδικασία που ικανοποιεί αντίθετους στόχους, όπως την διατήρηση της αυτονομίας κάθε εταιρίας, καθώς και την δημιουργία εταιρίας με ένα πληροφοριακό σύστημα.
- Δίνουμε βαρύτητα στον τρόπο διαμοιρασμού της πληροφορίας και πως έχουμε πρόσβαση σε αυτήν.

↓

Γι’ αυτό και πρώτα ορίζουμε τις ενδο-εταιρικές διαδικασίες πιστοποίησης, εν συνεχεία γίνεται συγχώνευση των ορισμών των επιχειρησιακών διαδικασιών και τέλος λαμβάνουμε υπόψιν τους περιορισμούς ιδιωτικότητας δεδομένων.

↓

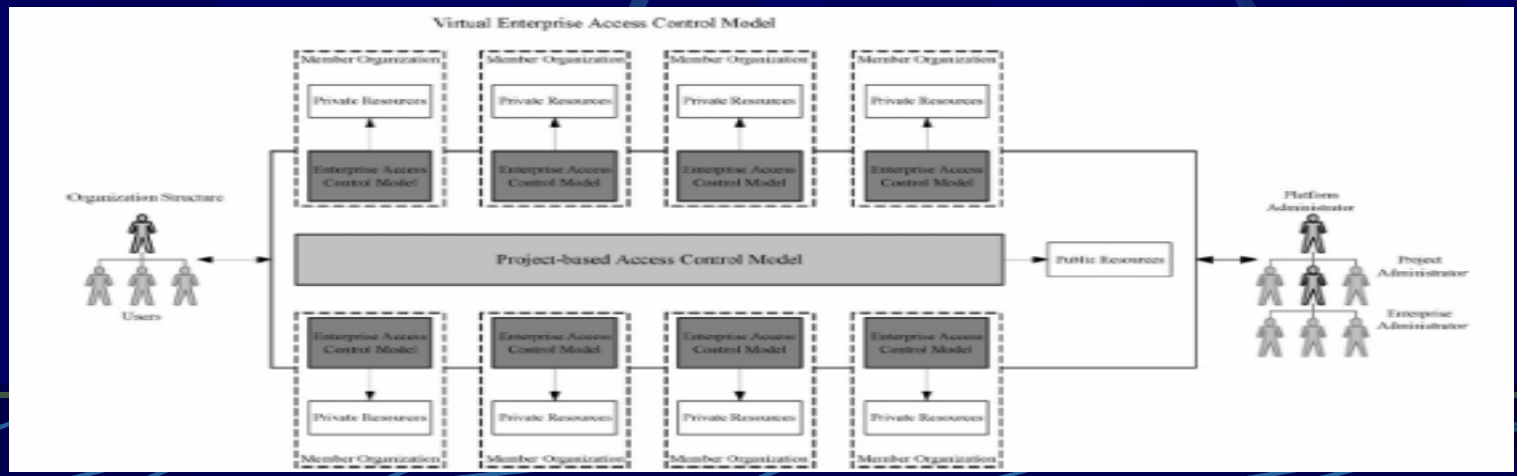
Ωθούμαστε σε μία αρχιτεκτονική πολλών επιπέδων, όπου διαχωρίζουμε την πιστοποίηση του χρήστη, από τα συστήματα αναφοράς των επιχειρηματικών διαδικασιών.

Ανάπτυξη μοντέλου ελέγχου πρόσβασης VEAC (Virtual Enterprise Access Control).

Προκειμένου να λύσουμε το πρόβλημα διαχείρισης εξουσίας και ασφάλειας μεταξύ των συνεργαζόμενων εταιριών της VE, προτείνουμε το μοντέλο **VEAC**, που αποτελείται από τα υπο-μοντέλα, **PBAC** (Project Based Access Control) που διαχειρίζεται τους δημόσιους πόρους της και **RBAC** (Role Based Access Control) που διαχειρίζεται τους ιδιωτικούς πόρους κάθε εταιρίας της VE.

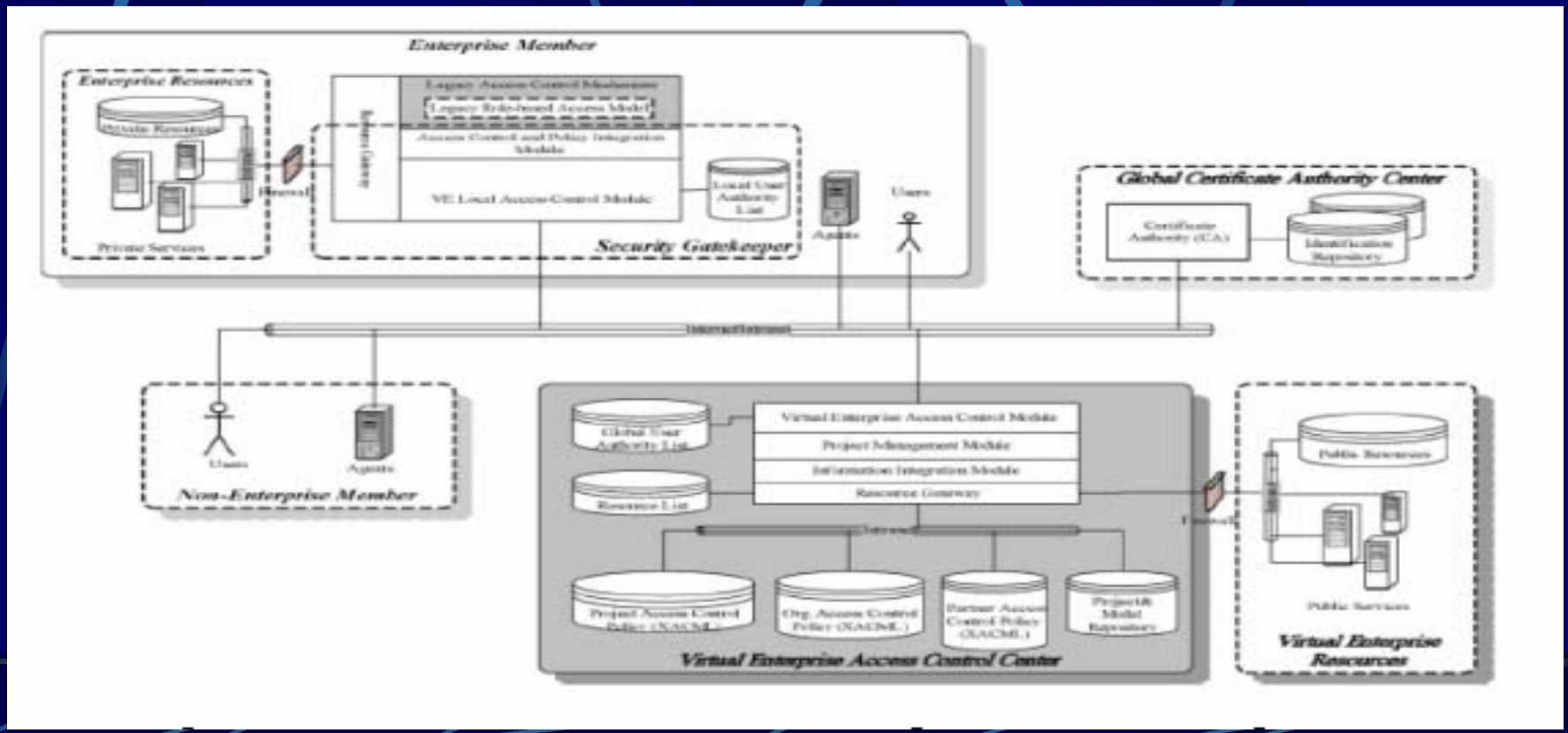
Οι ιδιότητες που το χαρακτηρίζουν είναι :

- Παρέχει διαχείριση και διαμοιρασμό πόρων μεταξύ των συνεργατών.
- Προκαλεί την αλλαγή των δικαιωμάτων πρόσβασης.
- Επεκτείνει την εξουσιοδότηση πρόσβασης και σε συνεργάτες των μελών της VE.
- Αποτρέπει την αποκάλυψη επιχειρηματικών μυστικών της VE.



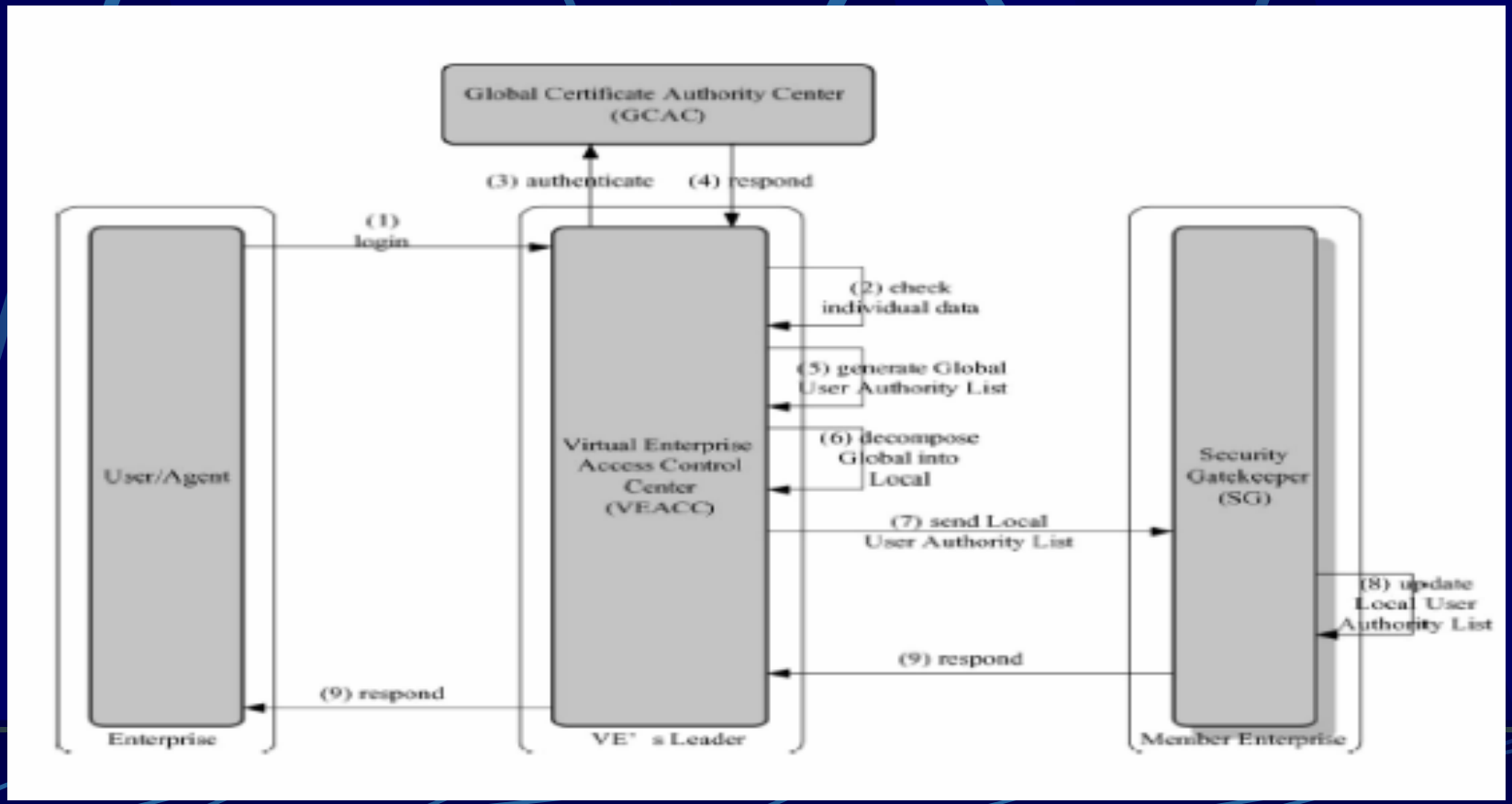
- **Η αρχιτεκτονική του συστήματος που βασίζεται στο μοντέλο VEAC.**

Περιλαμβάνει ένα κέντρο ελέγχου πρόσβασης της VE, το **VEACC** (Virtual Enterprise Access Control Center), που είναι υπεύθυνο για την διαχείριση ελέγχου ασφάλειας και αναπτύσσεται στην εταιρία οδηγό. Επιπλέον κάθε εταιρικό μέλος **EM** (Enterprise Member), έχει εγκαταστήσει ένα φύλακα ασφάλειας πύλης **SG** (Security Gatekeeper) , προκειμένου να διαφυλάξει τους πόρους του. Τέλος υπάρχει το Παγκόσμιο Κέντρο Πιστοποίησης Εξουσίας **GCAC** (Global Certificate Authority Center), στο οποίο αποστέλλει το **VEACC** την είσοδο του χρήστη, για να την πιστοποιεί.

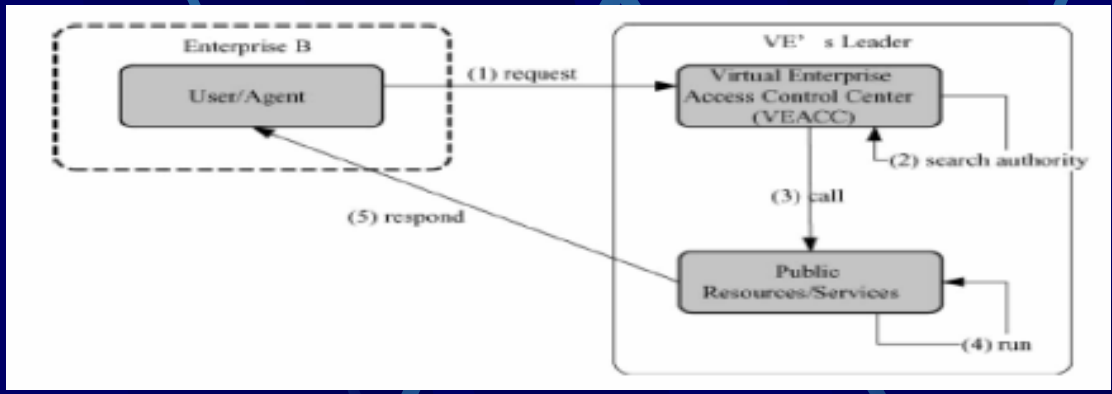


- **Προσεγγίσεις ελέγχου πρόσβασης :** Στον έλεγχο πρόσβασης της VE, η ταυτοποίηση του χρήστη, είναι ένα πολύ σημαντικό βήμα πριν την εξουσιοδότηση του σε οποιαδήποτε προστατευμένη λειτουργία.

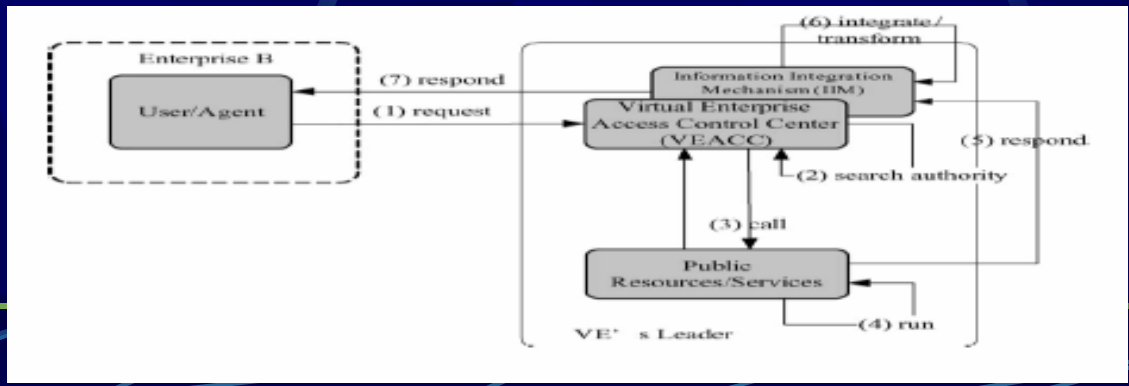
  - **Προσέγγιση για ενημέρωση λίστας δικαιοδοσίας χρηστών :** Όταν ο χρήστης εισέρχεται στο σύστημα του VEAC, αυτό θα πρέπει να δημιουργεί μία λίστα δικαιοδοσιών χρήστη, που θα ενημερώνει τόσο την τοπική λίστα του κάθε SG, όσο και την παγκόσμια του VEACC.



- **Προσέγγιση για πρόσβαση στους δημόσιους πόρους :** Το VEACC παρέχει δύο τρόπους για πρόσβαση στους δημόσιους πόρους, με ή χωρίς συγχώνευση της πληροφορίας.
  - **Χωρίς συγχώνευση :**



  - **Με συγχώνευση :**



Τελικά Συμπεράσματα

Συνοψίζοντας καταλήγουμε στα ακόλουθα :

- Από το πρώτο μέρος της εργασίας μας, έχοντας αναπτύξει διεξοδικά τους λόγους που υπάρχει ανασφάλεια στο Διαδίκτυο, τους κινδύνους που ελλοχεύουν, καθώς και τις λύσεις που διασφαλίζουν τις ηλεκτρονικές μας συναλλαγές, συμπεραίνουμε ότι δεν υπάρχει απόλυτη ασφάλεια. Ακόμη και τα πλέον εξελιγμένα συστήματα ασφάλειας δεν μπορούν να μας εγγυηθούν απόλυτη ασφάλεια. Όσα περισσότερα χρήματα επενδύσει κάποιος, τόσο περισσότερο είναι προστατευμένος από τις σύγχρονες απειλές.

- Από το δεύτερο μέρος της εργασίας μας, παρατηρώντας τα πλεονεκτήματα που αποκτά μία εταιρία, από την συμμετοχή της σε μία VE, αντιλαμβανόμαστε ότι αντλεί πολύ σημαντικά πράγματα, που είναι δύσκολο να τα αποκτήσει αν λειτουργεί από μόνη της στην αγορά. Το γεγονός αυτό, σε συνδυασμό με την σωστή εφαρμογή των λύσεων, όσον αφορά τα προβλήματα που αντιμετωπίζουν οι VEs, μας ωθεί στο συμπέρασμα, ότι μία εταιρία μάλλον επωφελείται από την σύμπραξή της σε κάποια VE. Κερδίζει πολλά χαρακτηριστικά, που την τροποποιούν, την εξοπλίζουν και την εξελίσσουν σαν εταιρία.

Σας Ευχαριστώ…