ΠΑΝΕΠΙΣΤΗΜΙΟ ΜΑΚΕΔΟΝΙΑΣ

ΤΜΗΜΑ ΕΦΑΡΜΟΣΜΕΝΗΣ ΠΛΗΡΟΦΟΡΙΚΗΣ

ΔΗΜΟΚΡΙΤΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΡΑΚΗΣ

ΤΜΗΜΑ ΝΟΜΙΚΗΣ

ΔΙΪΔΡΥΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
ΔΙΚΑΙΟ ΚΑΙ ΠΛΗΡΟΦΟΡΙΚΗ

ΕΜΠΙΣΤΟΣΥΝΗ ΚΑΙ ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ ΣΤΑ ΕΥΡΩΠΑΪΚΑ ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ COVID-19

Μια παρουσίαση της εσωτερικής δομής τους

Διπλωματική Εργασία

του

Απόστολου Παπαγιαννάκη

Θεσσαλονίκη, 03/2022

ΕΜΠΙΣΤΟΣΥΝΗ ΚΑΙ ΔΙΑΛΕΙΤΟΥΡΓΙΚΟΤΗΤΑ
ΣΤΑ ΕΥΡΩΠΑΪΚΑ ΨΗΦΙΑΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ COVID-19
Μια παρουσίαση της εσωτερικής δομής τους

Απόστολος Παπαγιαννάκης

Διπλωματούχος Ηλεκτρολόγος Μηχανικός και Μηχανικός Υπολογιστών ΑΠΘ, 2003

Διπλωματική Εργασία

υποβαλλόμενη για τη μερική εκπλήρωση των απαιτήσεων του

ΜΕΤΑΠΤΥΧΙΑΚΟΥ ΤΙΤΛΟΥ ΣΠΟΥΔΩΝ ΣΤΟ ΔΙΚΑΙΟ & ΠΛΗΡΟΦΟΡΙΚΗ

Επιβλέπων Καθηγητής

Κωνσταντίνος Ψάννης

Εγκρίθηκε από την τριμελή εξεταστική επιτροπή την 3/3/2022

Κωνσταντίνος Ψάννης	Μαρία Μυλώση	Μιχαήλ Μαντάς
…….	…….	…….

Απόστολος Παπαγιαννάκης

Περίληψη

Τα Ευρωπαϊκά Ψηφιακά Πιστοποιητικά COVID-19 αποτελούν ένα από τα ισχυρά εργαλεία αντιμετώπισης των συνεπειών της πανδημίας στην Ευρώπη, αλλά και σε πλήθος χωρών ανά τον κόσμο. Οι περισσότεροι από εμάς τα χρησιμοποιούμε καθημερινά και τα εμπιστευόμαστε χωρίς δεύτερη σκέψη, παρόλο που δε γνωρίζουμε τις τεχνικές τους λεπτομέρειες. Σε αυτή την εργασία παρουσιάζουμε τα πρότυπα με τα οποία διασφαλίζεται η ευχρηστία, η Εμπιστοσύνη και η Διαλειτουργικότητά των Ευρωπαϊκών Ψηφιακών Πιστοποιητικών COVID-19 στην Ευρώπη αλλά και σε τρίτες χώρες. Ακολούθως εξετάζουμε το περιεχόμενο και την εσωτερική δομή ενός αντιπροσωπευτικού Ευρωπαϊκού Πιστοποιητικού COVID-19, χρησιμοποιώντας απλά εργαλεία γραμμής εντολών, καθώς και μια πρότυπη εφαρμογή Android για έξυπνα τηλέφωνα και tablets της ΕΕ, προερχόμενα από τα επίσημα αποθετήρια ανοιχτού κώδικα της ΕΕ. Έπειτα περιγράφουμε την Υποδομή Δημόσιου Κλειδιού και το οικοσύστημα Εμπιστοσύνης, και συγκεκριμένα τους Εθνικούς Κόμβους διανομής δημόσιων κλειδιών, αλλά και την Ευρωπαϊκή Πύλη ανταλλαγής δημόσιων κλειδιών, που είναι απαραίτητα για να λειτουργήσουν τα Πιστοποιητικά διασυνοριακά μέσα στην Ευρωπαϊκή Ένωση αλλά και σε τρίτες χώρες. Επίσης δείχνουμε πως διαφορετικές χώρες, μπορούν να χρησιμοποιούν τα Πιστοποιητικά με διαφορετικούς τρόπους και να εφαρμόζουν διαφορετικούς κανόνες, χωρίς να αλλάζει η διαδικασία και οι εφαρμογές που χρησιμοποιούνται. Αναφερόμαστε επίσης στο ρόλο των διεθνών οργανισμών και των χωρών που υποστηρίζουν την ανάπτυξη των προτύπων. Τέλος θα αναφερθούμε σε μελλοντικές δυνατότητες που ανοίγονται για παράγωγα νέα εγχειρήματα με βάση τη νεοαποκτηθείσα εμπειρία.

Λέξεις Κλειδιά: covid-19, εμπιστοσύνη, υποδομή δημόσιου κλειδιού, ψηφιακά πιστοποιητικά, πιστοποιητικά εμβολιασμού, εφαρμογές για κινητά, εφαρμογές android

Abstract

Digital Certificates for COVID-19 are one of the most powerful tools against the effects of the COVID-19 pandemic on the global economy. Most of us rely on them without second thought, despite the fact that we do not really know any technical details about them. In this paper we present the standards that ensure the usability and trust and interoperability of Digital Certificates at the European level as well as with third countries. We then examine the content and internal structure of a representative European COVID-19 Certificate, using simple command line tools as well as an Android App for smart phones and tablets from the EU Open Source repositories. Next, we describe the Public Key infrastructure as well as the Trust ecosystem, and in particular the National Public Key distribution nodes, but also the European Public Key Exchange Gateway, both of which are necessary for the Certificates to operate cross-border within the European Union and in third countries. We also show that different countries can use Certificates in different ways and apply different rules, without changing the process or the applications used. We also refer to the role of International Organizations and countries that support the development of relevant procedures and standards. Finally, we will refer to future possibilities that open up for derivative new ventures based on the newly acquired experience.

Keywords: COVID-19, trust, public key infrastructure, digital certificates, vaccination certificates, mobile applications, android applications.

Πρόλογος – Ευχαριστίες

Οφείλω ευχαριστίες στον επιβλέπων καθηγητή κ. Κωνσταντίνο Ψάννη για την εμπιστοσύνη που μου έδειξε, δίνοντάς μου την δυνατότητα να ασχοληθώ με ένα τόσο επίκαιρο θέμα, αλλά και για την υπομονή που έδειξε καθ' όλη την διάρκεια της πτυχιακής μου εργασίας. Επίσης ευχαριστώ τη σύζυγό μου Νικολέττα Κατσαβού και τα παιδιά μου Ευαγγελία και Παναγιώτη Παπαγιαννάκη για την απεριόριστη υποστήριξή τους και τους γονείς μου Μανούσο και Ελένη που συνετέλεσαν και αυτοί με τον τρόπο τους.

Περιεχόμενα

Κατάλογος Εικόνων

Κατάλογος Πινάκων

Συμβολισμοί

Πιστοποιητικό Δημόσιου Κλειδιού	Πιστοποιητικό X.509v3 (RFC5280 [1]) που περιέχει το δημόσιο κλειδί μιας οντότητας
ΠΟΥ	Παγκόσμιος Οργανισμός Υγείας
DDCC:VS	Digital Documentation for Covid Certificate: Vaccination Status
CSCA	Εθνική αρχή πιστοποίησης
DCC ή EU DCC	Ψηφιακό Πιστοποιητικό COVID-19 της ΕΕ. Υπογεγραμμένο ψηφιακό έγγραφο το οποίο περιέχει πληροφορίες εμβολιασμού, διαγνωστικού ελέγχου ή ανάρρωσης
DCCG	Πύλη Ψηφιακού Πιστοποιητικού COVID-19 της ΕΕ. Το εν λόγω σύστημα χρησιμοποιείται για την ανταλλαγή DSC μεταξύ των κρατών μελών.
GRDCC	Πιστοποιητικά της Ελληνικής Δημοκρατίας στον ιστοχώρο gov.gr, και προσπελαύνονται με QRcode
ΤΠΕ	Τεχνολογίες Πληροφορικής και Επικοινωνιών
IHR	International Health Regulations
ΠΟΥ	Διεθνής Οργανισμός Υγείας
DDCC:VS	Digital Documentation of Covid-19 Certificates: Vaccination Status
FHIR	Fast Healthcare Interoperability Resources

1 Εισαγωγή

Η πανδημία COVID-19 δεν είναι πρόβλημα μόνο της ιατρικής επιστήμης. Έχει υπερφορτώσει τα συστήματα υγείας και έχει επιφέρει το πάγωμα πλήθους επαγγελματικών και κοινωνικών δραστηριοτήτων σε όλη την υφήλιο. Οι προκλήσεις που καλούνται να αντιμετωπίσουν οι κυβερνήσεις είναι πρωτοφανείς, με προβλήματα που κανονικά συναντώνται μόνο σε πολέμους και χρονικά deadlines (σ.σ. κυριολεκτικά). Υπό τις συνθήκες αυτές κυβερνήσεις, διεθνείς οργανισμοί, επιστημονικές ενώσεις και ιδιωτικοί φορείς από όλο τον πλανήτη, αναζητούν τρόπους να αντιμετωπίσουν ή έστω να ανακουφίσουν το πρόβλημα [2]

Η παγκόσμια κινητοποίηση έφερε συνεργασίες και αποτελέσματα που υπό άλλες συνθήκες θα χρειαζόντουσαν πολλαπλάσιο χρόνο για να ολοκληρωθούν[3]. Σε λίγους μήνες ολοκληρώθηκε η ανάπτυξη και οι κλινικές δοκιμές σε αρκετά νέα εμβόλια. Δύσκολα προβλήματα παραγωγής, διακίνησης και αποθήκευσης των εμβολίων αντιμετωπίστηκαν [4]. Με την πρωτοβουλία COVAX [5] του Παγκόσμιου Οργανισμού Υγείας (ΠΟΥ) αρκετά εμβόλια έφτασαν σε χώρες του Τρίτου Κόσμου [6]. Επίσης αναπτύχθηκαν φθηνοί και εύχρηστοι διαγνωστικοί έλεγχοι, μοριακοί και αντιγόνων [7].

Από την άλλη πλευρά τα κράτη έθεσαν προσωρινά οριζόντια περιοριστικά μέτρα στις μετακινήσεις την εργασία, το εμπόριο, τη εκπαίδευση και τις κοινωνικές επαφές, ανακόπτοντας προσωρινά την εξέλιξη της πανδημίας, αλλά με τεράστιο κοινωνικό και οικονομικό κόστος [8]. Υπό τις συνθήκες αυτές, τα διεθνή ταξίδια και το εμπόριο κατέστησαν μια σχεδόν αδύνατη υπόθεση.

Καθώς τα εμβόλια άρχισαν να γίνονται διαθέσιμα σε πολλές χώρες, έγινε φανερό ότι από τα περιοριστικά μέτρα θα μπορούσαν πλέον να εξαιρεθούν μεγάλες κατηγορίες πληθυσμού οι οποίες είτε είχαν εμβολιαστεί είτε είχαν άλλες συνθήκες π.χ. είχαν ήδη νοσήσει είτε είχαν κάνει κατάλληλο διαγνωστικό έλεγχο. Αυτές οι συνθήκες όμως έπρεπε να πιστοποιηθούν ιατρικά, κι έτσι πολλές χώρες άρχισαν να εμφανίζουν λύσεις σε αυτό το πρόβλημα, βασισμένες στην πιστοποίηση της κατάστασης του εμβολιασμού και της υγείας ενός ατόμου μέσω εφαρμογών για κινητά τηλέφωνα [9].

Το πρόβλημα όμως στα διεθνή ταξίδια και το διεθνές εμπόριο παρέμενε, καθώς τα ιατρικά πιστοποιητικά μιας χώρας δεν αναγνωρίζονται αυτόματα σε άλλες χώρες. Το υπάρχον πλαίσιο πιστοποίησης ασθενειών ανάμεσα σε κράτη δεν επαρκούσε για να καλύψει τις τρέχουσες ανάγκες μιας παγκόσμιας πανδημίας.

2 Τα Πιστοποιητικά του Παγκόσμιου Οργανισμού Υγείας

2.1 Τα παραδοσιακά Πιστοποιητικά Εμβολιασμού (Carte Jeun)

Εικόνα 1 - Carte Jeun

Η προστασία της δημόσιας υγείας αλλά και ο περιορισμός των επιπτώσεων στο διεθνές εμπόριο και τα ταξίδια ήταν ήδη αντικείμενο των Διεθνών Κανονισμών Υγείας (IHR) του Παγκόσμιου Οργανισμού Υγείας ήδη από το 1951 [10]. Ακόμα και πριν την εποχή του κορονοϊού, τα Διεθνή Πιστοποιητικά Εμβολιασμού ήταν απαραίτητα για τα διεθνή ταξίδια, γιατί σε πολλά κράτη υπήρχαν και υπάρχουν μεταδιδόμενες ασθένειες που πρέπει να περιορίζονται, όπως ο Κίτρινος Πυρετός. Το παραδοσιακό Διεθνές Πιστοποιητικό εμβολιασμού ή άλλης προφύλαξης [11] του Παγκόσμιου Οργανισμού Υγείας επικράτησε να αποκαλείται Κίτρινη Κάρτα ή Yellow Card ή Carte Jeun και αποδεικνύει τον εμβολιασμό ή άλλη προφύλαξη απέναντι σε συγκεκριμένες ασθένειες. Σε αυτό καταγράφονται οι βασικές πληροφορίες μιας χορήγησης εμβολίου όπως η ημερομηνία, το χορηγημένο εμβόλιο και ο αριθμός της παρτίδας του (βλ. εικόνα). Τα έγγραφα αυτά αναγνωρίζονται και σήμερα ως αποδείξεις εμβολιασμού σε όλο τον κόσμο, και επιτρέπουν στον κάτοχο να ταξιδεύει χωρίς περιορισμούς σε μέρη που ισχύουν τακτικά ή έκτακτα μέτρα κατά ενδημικών ασθενειών, π.χ. για τον Κίτρινο Πυρετό. Όμως η χρήση τους σε καθολική κλίμακα ενέχει σοβαρά προβλήματα διαχείρισης και αξιοπιστίας καθώς παράγονται και ενημερώνονται χειρόγραφα σε τοπικό επίπεδο, δεν είναι μηχαναγνώσιμα και δεν έχουν κανένα σημαντικό χαρακτηριστικό ασφάλειας που να διευκολύνει τεχνικά τον έλεγχο ακεραιότητας και αυθεντικότητας σε πραγματικό χρόνο, όπως απαιτείται στα σημεία εισόδου μιας χώρας σε αεροδρόμια, συνοριακές διαβάσεις και λιμάνια.

2.2 Πιστοποιητικά Ψηφιακής Τεκμηρίωσης COVID-19 (DDCC:VS)

Ήδη από τις αρχές του 2021, με την διάδοση των εμβολίων κατά της COVID-19, ο ΠΟΥ εξέδωσε προτάσεις τεχνικών προδιαγραφών και ενδεικτικές οδηγίες υλοποίησης [12], [13]

για Πιστοποιητικά Ψηφιακής Τεκμηρίωσης Κατάστασης Εμβολιασμού για την COVID-19 (Digital Documentation of COVID Certificate of Vaccination Status) για χρήση από τις εθνικές αρχές, και άλλα συνεργαζόμενα μέρη που μπορεί να έχουν ενδιαφέρον, όπως επιχειρήσεις, διεθνείς οργανισμοί, Μη Κυβερνητικές Οργανώσεις, κ.α.. Ο ΠΟΥ προτείνει τρόπους αλλά θέτει και τις προϋποθέσεις για το τί πρέπει να περιέχει να πιστοποιητικό εμβολιασμού η προφύλαξης, πως μπορεί να αναπαρασταθεί με μηχαναγνώσιμο τρόπο, και πως να μπορεί να επαληθευθεί ψηφιακά ως προς την ακεραιότητα και αυθεντικότητά του, σε όλες τις χώρες μέλη του οργανισμού. Βασικό τμήμα των προδιαγραφών αποτελεί η τυποποίηση των ιατρικών δεδομένων που περιέχει, η κωδικοποίησή τους σύμφωνα με διεθνή ιατρικά πρότυπα (FHIR [15]), καθώς και η διαδικασία ψηφιακής υπογραφής τους. Επίσης περιγράφει τις απαιτούμενες υποδομές και διαδικασίες των υπηρεσιών που εκδίδουν τα Πιστοποιητικά, και προβλέπει εναλλακτικές διαδικασίες, ανάλογα τα διαθέσιμα μέσα. Ακόμη μελετά τα θέματα Εμπιστοσύνης ανάμεσα στις διάφορες εθνικές αρχές που παράγουν ή που χρησιμοποιούν τα Ψηφιακά Πιστοποιητικά. Πέρα από τα αμιγώς τεχνικά και διαδικαστικά θέματα μιδιαίτερη προσοχή δίδεται και σε ηθικά και νομικά θέματα όπως θέματα ισότιμης αντιμετώπισης πρόσβασης στα νέα Πιστοποιητικά, προστασία Προσωπικών Δεδομένων κ.α. Βέβαια όλα αυτά είναι απλά καθοδηγητικές προτάσεις με την ελπίδα ότι κάποτε θα γίνουν αποδεκτά και θα υλοποιηθούν από τα κράτη μέλη του ΠΟΥ.

Στην τελική του μορφή ο κάτοχος ενός DDCC:VS θα κατέχει ένα ψηφιακό πιστοποιητικό το οποίο θα έχει τη μορφή ενός δισδιάστατου ραβδοκώδικα QR, ο οποίος όμως μπορεί να ενσωματωθεί σε μια σελίδα χαρτί ή σε ένα αρχείο pdf ή να απεικονιστεί την οθόνη ενός έξυπνου τηλέφωνου και να αποθηκευτεί οπουδήποτε, π.χ. ή σε ένα υπολογιστή στο νέφος.

Εικόνα 2 - Προτάσεις ΠΟΥ για ψηφιακό Πιστοποιητικό ([14],σελ. vii)

2.3 Προτεινόμενες χρήσεις του DDCC:VS

Τα ιατρικά δεδομένα που περιέχονται στο παραδοσιακό έγχαρτο Διεθνές Πιστοποιητικό Εμβολιασμού είναι παρόμοια με αυτά στο ψηφιακό DDCC:VS. Όμως το DDCC:VS ακολουθεί το ευρέως αποδεκτό πρότυπο διαχείρισης ιατρικών πληροφοριών FHIR [15] του μη κερδοσκοπικού οργανισμού Health Level Seven International [16]. Στις οδηγίες του ο ΠΟΥ επισημαίνει ([12], σελ. xii) ότι τα DDCC:VS μπορούν να χρησιμοποιηθούν μόνο ως απόδειξη ιατρικού γεγονότος (π.χ. έναν εμβολιασμό) και όχι ως "διαβατήριο ανοσίας". Η απόφαση για το τί επιτρέπεται να κάνει ή να μην κάνει ο κάτοχος ενός DDCC:VS στην προσωπική, κοινωνική ή επαγγελματική του ζωή είναι θέμα απόφασης των κατά τόπους κρατικών αρχών. Το DDCC:VS χρησιμοποιείται ([12], σελ. xiv) ως αποδεικτικό μέσο σε καταστάσεις όπως οι παρακάτω:

Συνέχιση Ιατρικής φροντίδας	**Απόδειξη εμβολιασμού**
• Στοιχείο πάνω στο οποίο μπορούν να βασιστεί η συνέχεια ενός εμβολιασμού ή ενός θεραπευτικού σχήματος • Παρέχει πληροφορίες στον κάτοχο για να γνωρίζει πότε	• Για τα διεθνή ταξίδια • Για την εργασία • Για την εκπαίδευση • Για τη συμμετοχή σε κοινωνικές δραστηριότητες • Επιτρέπει την παρακολούθηση του εμβολιασμού σε σχέση με

πρέπει να κάνει την επόμενη δόση και με ποιο εμβόλιο • Επιτρέπει τη διερεύνηση των παρενεργειών που ενδεχομένως προκύψουν από έναν εμβολιασμό	τυχόν μεταγενέστερη εμφάνιση θετικού τεστ COVID-19

Πίνακας 1 - Ενδεικτικές χρήσεις του DDCC:VS

3 Η υλοποίηση της Ευρωπαϊκής ένωσης: EU DCC

Η Ευρωπαϊκή Ένωση έχει πάντα ιδιαίτερο ενδιαφέρον σε οτιδήποτε περιορίζει την διασυνοριακή κινητικότητα των πολιτών. Η Ευρωπαϊκή Επιτροπή ανάθεσε στο δίκτυο εμπειρογνωμόνων eHealth [20] να μελετήσει το πρόβλημα των Ψηφιακών Πιστοποιητικών COVID-19, με τρόπο που να διασφαλίζεται η διαλειτουργικότητα σε όλες τις χώρες μέλη, και όχι μόνο. Ήδη από το Δεκέμβριο του 2020 η ΕΕ εξέδωσε κατευθυντήριες γραμμές [22] για ένα Ευρωπαϊκό Ψηφιακό Πιστοποιητικό COVID-19 (EU-DCC) που θα λειτουργούσε με τον ίδιο τρόπο σε όλες τις χώρες μέλη αλλά και σε τρίτες χώρες που θα επέλεγαν να αναγνωρίσουν τα Ευρωπαϊκά Πιστοποιητικά. Το δίκτυο βασιζόμενο και στις αντίστοιχες εργασίες του ΠΟΥ [12], [13], [14], αλλά και εργασιών πσυνέχισε να παράγει κείμενα συγκεκριμένων τεχνικών προδιαγραφών, διαδικασιών και κωδικοποιήσεων τα οποία δημοσίευσε σε επίσημο ιστοχώρο αναφοράς της ΕΕ . Επιπλέον δημιούργησε προγραμματιστικές διεπαφές (Application Programming Interfaces - APIs) και εφαρμογές αναφοράς, τις οποία ανάρτησε σε επίσημα ανοιχτά αποθετήρια κώδικα [23], [24] ώστε να μπορούν όλες οι χώρες αλλά και τα μεμονωμένα άτομα να τα αξιοποιήσουν με εύκολο τρόπο, όπως κάνουμε κι εμείς σε αυτή την εργασία. Το μεγαλύτερο μέρος των τεχνικών προδιαγραφών διαδικασιών και κωδικοποιήσεων τελικά ενσωματώθηκε στην Εκτελεστική Απόφαση (ΕΕ) 2021/1073 [25] η οποία έχει υποχρεωτική ισχύ από 1/7/2021, και η οποία συμπληρώθηκε με τις αποφάσεις 2021/2014 [26] και 2021/230 [27].

3.1 Τί είναι το Ευρωπαϊκό Πιστοποιητικό COVID-19

Το Ευρωπαϊκό Ψηφιακό Πιστοποιητικό COVID-19 (EU DCC) είναι ένα τυποποιημένο σύνολο από Ιατρικά Δεδομένα τα οποία κωδικοποιούνται σε συγκεκριμένο μορφότυπο (HCERT) που φέρει ηλεκτρονική υπογραφή. Ο φορέας του πιστοποιητικού μπορεί να είναι οποιοδήποτε καθαρό κανάλι μεταφοράς δεδομένων 8bit συμπεριλαμβανομένων των NFC και Bluetooth κ.α.., αλλά με κατάλληλη συμπίεση και κωδικοποίηση μπορεί να αποτυπωθεί και σε δισδιάστατο ραβδοκώδικα QR [28], [29].

Τα δεδομένα που έχουν επιλεγεί να περιέχονται μέσα στο Ευρωπαϊκό Ψηφιακό Πιστοποιητικό έχουν επιλεγεί να είναι παρόμοια με αυτά του ΠΟΥ DDCC:VS για την περίπτωση του Πιστοποιητικού Εμβολιασμού [30]. Όμως σε σχέση με το DDCC:VS το

Ευρωπαϊκό Ψηφιακό Πιστοποιητικό μπορεί επιπλέον να πιστοποιήσει τυχόν προηγούμενη νόσηση [31], αλλά και να πιστοποιήσει τα αποτελέσματα διαγνωστικού ελέγχου [32], έτσι ώστε τα Πιστοποιητικά να μπορούν να καλύψουν τις ανάγκες του συνόλου του πληθυσμού σε μια χώρα, και όχι μόνο των εμβολιασμένων.

Και στις τρείς περιπτώσεις τα δεδομένα που περιέχονται μέσα στα πιστοποιητικά είναι κατά το δυνατό τυποποιημένα με τιμές από πίνακες ευρέως διαδεδομένων ιατρικών προτύπων όπως LOINC FHIR, SNOMED-CT ή πρότυπα ISO/IEC ή RFCs [30], [25], [26], όπως συμβαίνει και στα DDCC:VS του ΠΟΥ ([12], σελ. xii).

3.2 Χαρακτηριστικά του Ευρωπαϊκού Πιστοποιητικού COVID-19

Τα Ευρωπαϊκά Ψηφιακά Πιστοποιητικά COVID-19 έχουν σημαντικά πλεονεκτήματα σε σχέση με τα παραδοσιακά ιατρικά Πιστοποιητικά Εμβολιασμού. Τα χάρτινα πιστοποιητικά επιδέχονται μόνο απλό οπτικό έλεγχο από άνθρωπο, και η επαλήθευσή τους κατά απαιτεί εξειδικευμένο προσωπικό ή επικοινωνία με τον εκδότη. Σημαντικά πλεονεκτήματα των ψηφιακών Πιστοποιητικών αποτελούν:

- Ακόμα κι όταν είναι απλά τυπωμένα σε χαρτί περιέχουν ραβδοκώδικα και είναι μηχαναγνώσιμα, πέρα του απλού οπτικού ελέγχου ([25], σελ. L230/35). Συνεπώς μπορούν να επαληθευθούν με απλές φορητές συσκευές, επιταχύνοντας τη διαδικασία ελέγχου και διασφαλίζοντάς την από τυχόν ανθρώπινα λάθη.
- Τα πιστοποιητικά παραμένουν το ίδιο ισχυρά είτε είναι σε ηλεκτρονική είτε σε έντυπη μορφή ([33], σελ. 5). Η χρήση της μιας μορφής δεν αποκλείει την παράλληλη χρήση της άλλης, επειδή σε όλες τις μορφές επαληθεύεται ψηφιακά και παρέχει εγγυήσεις ως προς την ακεραιότητα και αυθεντικότητα, δηλ. δεν μπορεί να παραποιηθεί και να υπάρχει αμφιβολία για το ποιος είναι αυτός που πιστοποιεί.
- Το γεγονός ότι τα Ψηφιακά Πιστοποιητικά διακινούνται μόνο από τον κάτοχό τους είτε σε χαρτί είτε σε ηλεκτρονικό αρχείο PDF με QR code, εξασφαλίζει ότι ο κάτοχος έχει ένα αρχικό έλεγχο πάνω στα προσωπικά του Δεδομένα. Επιπλέον το σύνολο των δεδομένων που περιέχονται στα πιστοποιητικά είναι ελαχιστοποιημένο ([25], σελ. L230/33) περιορίζοντας την κρισιμότητα των όποιων διαρροών.
- Είναι πολύ απλά και γρήγορα στην χρήση, ακόμα και από αυτούς που δεν έχουν ψηφιακές δεξιότητες, αλλά και από αυτούς που τα ελέγχουν. Η φυσική μορφή σε χαρτί ή

σε πλαστική κάρτα είναι ισοδύναμη με αυτήν σε ηλεκτρονική μορφή. Και στις δύο περιπτώσεις είναι εύκολα μηχαναγνώσιμη, ([25], σελ. L230/35) ώστε να είναι δυνατός ό ταχύς έλεγχος σε σημεία όπου συνωστίζονται πολλοί άνθρωποι.

- Έχει την τεχνική πρόβλεψη να μπορεί να δεχθεί επιπλέον λειτουργίες, καθώς τα δομικά του στοιχεία (JSON schema, HVCI) προβλέπουν ειδικά πεδία για αριθμούς εκδόσεων ([34], σελ. 4) και ([22], σελ.12) ώστε να μπορούν να υπάρξουν μελλοντικές εκδόσεις με νεότερα χαρακτηριστικά.
- Το οικοσύστημα ελέγχου των πιστοποιητικών συνδυάζει τα περιεχόμενα του πιστοποιητικού με κανόνες που κάθε χώρα δημοσιεύει μαζί με τα δημόσια κλειδιά των υπογραφόντων. Αυτό επιτρέπει κάθε χώρα να προσαρμόζει και να εφαρμόζει τα δικά της κριτήρια ανάλογα με τις τοπικές συνθήκες και την εξέλιξη της πανδημίας [35]. Ο κάτοχος-ταξιδιώτης κατά την είσοδο σε μια χώρα ελέγχεται με βάση τα τρέχοντα τοπικά κριτήρια ελέγχου. Αυτό συμβάλει στην αποτελεσματικότητα του πιστοποιητικού, αλλά και ο κάτοχος απαλλάσσεται από την φροντίδα να επανεκδίδει το πιστοποιητικό κάθε φορά που οι κανόνες αλλάζουν.

3.3 Χρήσεις των Ευρωπαϊκών Πιστοποιητικών COVID-19

Μια βασική στόχευση των Ευρωπαϊκών Ψηφιακών Πιστοποιητικών είναι να διευκολύνουν την ιατρική πρακτική καθιστώντας τη σχετική ιατρική γνωμάτευση αξιοποιήσιμη οπουδήποτε στην ΕΕ, άμεσα και χωρίς μετάφραση. Για παράδειγμα, αυτό διευκολύνει τον πολίτη που θα χρειαστεί να κάνει τη δεύτερη δόση του εμβολίου του σε διαφορετική χώρα από ότι στην πρώτη δόση, χωρίς να χρειάζεται να εκδώσει νέο τοπικό πιστοποιητικό, καθώς το αρχικό του Πιστοποιητικό είναι άμεσα αναγνωρίσιμο και αποδεκτό από το γιατρό της δεύτερης χώρας.

Εκτός από την αμιγώς ιατρική χρήση, το Ευρωπαϊκό Ψηφιακό Πιστοποιητικό είναι ένα πολύτιμο εργαλείο για πλήθος περιπτώσεων της προσωπικής, κοινωνικής και επαγγελματικής μας ζωής. Ιδιαίτερα χρήσιμο είναι στη διαχείριση των ταξιδιωτικών ροών, ιδιαίτερα στις χώρες που δέχονται μεγάλα πλήθη τουριστών.

Τα Πιστοποιητικά δεν καλύπτουν όλες τις δυνητικές ανάγκες τεκμηρίωσης για την COVID-19. Για παράδειγμα σε επόμενη φάση, θα μπορούσε να προστεθεί η δυνατότητα να αποτυπωθεί και η αδυναμία εμβολιασμού για ιατρικούς λόγους. Καθώς η βασική δομή

του Πιστοποιητικού είναι επεκτάσιμη, η σχετική προσαρμογή αναμένεται ότι θα είναι σχετικά εύκολη υπόθεση.

Μέχρι σήμερα έχουν οριστεί τρείς τύποι Πιστοποιητικών

- Πιστοποιητικό Εμβολιασμού
- Πιστοποιητικό Ανάρρωσης
- Πιστοποιητικό Διαγνωστικού Ελέγχου

3.4 Τα περιεχόμενα του Ευρωπαϊκού Πιστοποιητικού COVID-19

Κάθε Ευρωπαϊκό Ψηφιακό Πιστοποιητικό περιέχει ένα ελάχιστο σύνολο δεδομένων, κοινό σε όλες τις υλοποιήσεις των διαφόρων χωρών, προκειμένου να καλύπτονται οι πιστοποιούμενες ανάγκες αλλά και να μην υπάρχουν προβλήματα διαλειτουργικότητας σε τεχνικό και νομικό επίπεδο. Τα δεδομένα αυτά χωρίζονται σε τρείς κατηγορίες:

- Προσδιορισμός υποκειμένου (κατόχου)
- Ιατρικά Δεδομένα
- Μεταδεδομένα Πιστοποιητικού

Τα στοιχεία ονόματος περιέχονται οπωσδήποτε στην Αγγλική γλώσσα σε μορφότυπο κατάλληλο για διαβατήρια [37], αλλά μπορούν να υπάρχουν πληροφορίες σε άλλες γλώσσες με κατάλληλη μορφή (σύνολο χαρακτήρων Unicode 13.0 και κωδικοποίηση UTF-8, βλ. [34], σελ. 4).
Για να υπάρχει Εμπιστοσύνη στη χρήση του Ευρωπαϊκού Ψηφιακού Πιστοποιητικού, αυτό πρέπει το αντιλαμβάνονται όλοι οι αναγνώστες με τον ίδιο τρόπο. Για αυτό το λόγο τα δεδομένα στα πεδία του Πιστοποιητικού λαμβάνουν τιμές από ευρέως αποδεκτά ταξινομικά συστήματα (π.χ. FHIR [15], SNOMED-CT [38]) τα οποία έχουν μονοσήμαντη έννοια για την ιατρική κοινότητα παγκοσμίως. Ο τύπος των δεδομένων και η αντιστοίχισή τους με ταξινομικά συστήματα έχουν επιλεγεί ώστε να υπάρχει συμβατότητα με τους αντίστοιχους ορισμούς του ΠΟΥ για ένα Διεθνές Πιστοποιητικό Εμβολιασμού [12], ώστε να διευκολυνθεί η αξιοποίησή τους από ιατρούς τρίτων χωρών, αλλά και να διευκολυνθεί η διαλειτουργικότητα με τις λύσεις που αναπτύσσουν άλλες χώρες, ανά την υφήλιο.

3.5 Είδη Πιστοποιητικών:

Μέχρι σήμερα έχουν οριστεί τρείς τύποι Πιστοποιητικών

- Πιστοποιητικό Εμβολιασμού
- Πιστοποιητικό Ανάρρωσης
- Πιστοποιητικό Διαγνωστικού Ελέγχου

Κατά τη σχεδίασή τους λήφθηκε ιδιαίτερη πρόνοια για την προστασία των προσωπικών δεδομένων των κατόχων τους σύμφωνα με τον ΓΚΠΔ ([25], σελ. L230/33). Όπως θα φανεί και παρακάτω, κάθε είδος Πιστοποιητικού περιέχει τα ελάχιστα δυνατά δεδομένα σχετικά με το σκοπό που εξυπηρετεί, αν και δεν αποκλείεται να προστεθούν και άλλα δεδομένα προκειμένου αυτά να υποστηρίξουν επιπλέον λειτουργικότητες. Σε κάθε περίπτωση ο κάτοχος έχει ο ίδιος απόλυτο έλεγχο σε ποιόν τα διαθέτει και πότε τα δεδομένα του Πιστοποιητικού του.

3.6 Δεδομένα Πιστοποιητικού Εμβολιασμού

Τα ελάχιστα περιεχόμενα του Ψηφιακού Πιστοποιητικού Εμβολιασμού προδιαγράφονται αναλυτικά στο [22]. Παρακάτω αναφέρονται οι σημαντικότερες πληροφορίες οι οποίες και θα εξεταστούν παρακάτω σε ένα αντιπροσωπευτικό πραγματικό πιστοποιητικό:

Ενότητα πληροφορίας	**Στοιχείο πληροφορίας**	**Περιγραφή**
Προσωπικά στοιχεία	Ονοματεπώνυμο	Επίθετο και όνομα υποκειμένου στην τοπική γλώσσα με τη συγκεκριμένη σειρά, καθώς και οπωσδήποτε στην Αγγλική γλώσσα σε μορφότυπο κατάλληλο για διαβατήρια [37]
	Ημερομηνία γέννησης	Ημερομηνία χωρίς ώρα, κατά ISO8601 [40]

	Προσδιοριστικό προσώπου (προαιρετικό)	Τύπος και τιμή προσδιοριστικού, π.χ. Δελτίο Αστυνομικής Ταυτότητας και αριθμός αυτού ΑΔΤ AB123456
Πληροφορίες εμβολιασμού ή προφύλαξης	Ασθένεια	Προτιμώμενη τυποποίηση κατά ICD-10 [17] ή SNOMED CT [19] (GPS) μελλοντικά ICD-11 [18], π.χ. " 840539006" σημαίνει COVID-19
	Εμβόλιο ή άλλη προφύλαξη	Προτιμώμενη τυποποίηση κατά SNOMED CT και ATC (θεραπευτική υποομάδα J07) [38],[28] π.χ. • 1119349007 (COVID-19 εμβόλιο mRNA) ή • 1119305005 (COVID-19 εμβόλιο αντιγόνου)
	Ονομασία σκευάσματος	Εμπορική ονομασία π.χ. Comirnaty, ή ονομασία κατά πρότυπο ISO IDMP
	Κάτοχος άδειας διακίνησης ή κατασκευαστής εμβολίου	Όνομα σύμφωνα με την καταχώρηση του κατασκευαστή στην Ευρωπαϊκή Ιατρική Υπηρεσία (σύστημα EMA SPOR) π.χ. ORG100030215. Αν δεν υπάρχει καταχώρηση, τότε η εμπορική ονομασία προϊόντος π.χ. BioNTech Manufacturing GmbH
	Αριθμός δόσης στα πλαίσια του θεραπευτικού σχήματος	π.χ. 1 από 2 δόσεις

	Αριθμός παρτίδας (προαιρετικό)	
	Ημερομηνία εμβολιασμού	Ημερομηνία χωρίς ώρα, κατά ISO8601
	Ονομασία Κέντρου Χορήγησης	
	Προσδιοριστικό επαγγελματία υγείας (προαιρετικό)	Όνομα ή προσδιοριστικό επαγγελματία υγείας που ήταν υπεύθυνος για τη χορήγηση
	Χώρα εμβολιασμού	Διγράμματος κωδικός κατά ISO 3166 alpha2
	Ημερομηνία επόμενου εμβολιασμού	Ημερομηνία χωρίς ώρα, κατά ISO8601
Μεταδεδομένα Πιστοποιητικού	Εκδότης Πιστοποιητικού	
	Μοναδικό Προσδιοριστικό Πιστοποιητικού (UVCI)	Το προσδιοριστικό πρέπει να είναι μοναδικό, ώστε να μπορεί να αναζητηθεί στο πληροφοριακό σύστημα των εμβολιασμών
	Έναρξη ισχύος (προαιρετικό)	Ημερομηνία χωρίς ώρα, κατά ISO8601
	Λήξη ισχύος Πιστοποιητικού η οποία μπορεί να διαφέρει από τη λήξη της περιόδου ανοσοποίησης (προαιρετικό)	Ημερομηνία χωρίς ώρα, κατά ISO8601
	Αριθμός έκδοσης του σχήματος του Πιστοποιητικού	Σημασιολογία εκδόσεων κατά ISO [66]

Πίνακας 2 - Δεδομένα Πιστοποιητικού Εμβολιασμού

3.7 Δεδομένα Πιστοποιητικού Ανάρρωσης

Ο εμβολιασμός δεν ενδείκνυται για πρόσωπα που έχουν ήδη νοσήσει και αναρρώσει από την COVID-19. Αυτά τα πρόσωπα μπορεί να συνεχίζουν να παρουσιάζουν θετικά ευρήματα σε ελέγχους για αρκετό καιρό αφότου πάψουν να μεταδίδουν την ασθένεια. Έτσι πολλές χώρες έχουν ειδικές ταξιδιωτικές οδηγίες για τους πρώην νοσήσαντες και αναρρώσαντες. Το Ευρωπαϊκό Πιστοποιητικό μπορεί να παρέχει μια πιστοποίηση για το γεγονός της νόσησης παρέχοντας ένα ελάχιστο σύνολο δεδομένων [31].

Ενότητα πληροφορίας	**Στοιχείο πληροφορίας**	**Περιγραφή**
Προσωπικά στοιχεία	Όπως στο Πιστοποιητικό εμβολιασμού	
Πληροφορίες πρότερης νόσησης	Ασθένεια	Προτιμώμενη τυποποίηση κατά ICD-10 [17] ή SNOMED CT [19] (GPS) μελλοντικά ICD-11 [18], π.χ. " 840539006" σημαίνει COVID-19
	Ημερομηνία πρώτου θετικού διαγνωστικού ελέγχου	Ημερομηνία χωρίς ώρα, κατά ISO8601
	Χώρα εμβολιασμού	Διγράμματος κωδικός κατά ISO 3166 alpha2
Μεταδεδομένα Πιστοποιητικού	Όπως στο Πιστοποιητικό εμβολιασμού	

Πίνακας 3 - Δεδομένα Πιστοποιητικού Ανάρρωσης

Επειδή η επιστημονική κοινότητα διαρκώς συγκεντρώνει νέα επιστημονικά στοιχεία ως προς το επίπεδο και τη διάρκεια της επίκτητης ανοσίας, οι σχετικές οδηγίες ενδέχεται να αλλάξουν στο μέλλον, και τα κράτη μέλη πρέπει να είναι έτοιμα να προσαρμόσουν τις

διαδικασίες τους. Όπως θα φανεί και παρακάτω ο έλεγχος των Πιστοποιητικών βασίζεται πάντα σε επίκαιρους κανόνες.

3.8 Δεδομένα Πιστοποιητικού Διαγνωστικού Ελέγχου

Η Επιτροπή Υγειονομικής ασφάλειας της ΕΕ έχει εγκρίνει το ελαχιστοποιημένο σύνολο δεδομένων που πρέπει να περιέχει ένα Πιστοποιητικό σχετικά με τα αποτελέσματα διαγνωστικών ελέγχων COVID-19 [32]. Τα αποτελέσματα αυτά μπορούν να αξιοποιούνται από τα κράτη μέλη για να περιορίσουν τη μετάδοση του ιού.

Ενότητα πληροφορίας	**Στοιχείο πληροφορίας**	**Περιγραφή**
Προσωπικά στοιχεία	Όπως στο Πιστοποιητικό εμβολιασμού	
Πληροφορίες διαγνωστικών έλεγχων	Ασθένεια	Προτιμώμενη τυποποίηση κατά ICD-10 ή SNOMED CT (GPS), π.χ. " 840539006" σημαίνει COVID-19
	Τύπος ελέγχου	Περιγραφή διαγνωστικού ελέγχου με κωδικοποίηση σύμφωνα με LOINC, NPU π.χ. η τιμή "LP217198-3" σημαίνει "Rapid immunoassay" [67]
	Ονομασία ελέγχου (προαιρετικό)	
	Ονομασία κατασκευαστή (προαιρετικό)	
	Προέλευση δείγματος (προαιρετικό))	Προτιμώμενη τυποποίηση κατά SNOMED CT
	Ημερομηνία και ώρα συλλογής δείγματος	Πλήρη ημερομηνία, ώρα και ζώνη ώρας κατά ISO8601, π.χ. "2021-12-11T06:40:12Z"

	Ημερομηνία και ώρα παραγωγής αποτελεσμάτων ελέγχου	Πλήρη ημερομηνία, ώρα και ζώνη ώρας κατά ISO8601, π.χ. "2021-12-11T06:46:05Z"
	Αποτέλεσμα ελέγχου	αρνητικό, θετικό, ασαφές ή άκυρο κατά SNOMED CT [19]
	Διαγνωστικό Κέντρο (υποχρωτικό για PCR)	Ονομασία ή κωδικός διαγνωστικού κέντρου ή αρχής
	Προσδιοριστικό επαγγελματία υγείας (προαιρετικό)	Όνομα ή επαγγελματικός κωδικός υπεύθυνου για την τέλεση και επικύρωση του ελέγχου. Επίθετο και βαπτιστικό όνομα με αυτή τη σειρά.
	Χώρα εμβολιασμού	Διγράμματος κωδικός κατά ISO 3166 alpha2 [55]
Μεταδεδομένα Πιστοποιητικού	Όπως στο Πιστοποιητικό εμβολιασμού	

Πίνακας 4 - Δεδομένα Πιστοποιητικού Διαγνωστικού ελέγχου

4 Επαλήθευση και Επικύρωση Ευρωπαϊκών Πιστοποιητικών

4.1 Επαλήθευση ακεραιότητας και αυθεντικότητας

Η επαλήθευση ενός πιστοποιητικού γίνεται, ανάλογα με τον τρόπο που είναι υλοποιημένα, είτε σε χαρτί, είτε σε ψηφιακό μέσο, σε κάθε περίπτωση όμως η διαδικασία επαλήθευσης πρέπει να παραπέμπει σε κάποια αναγνωρισμένη αρχή πιστοποίησης. Κάθε διαδικασία έχει διαφορετικά επίπεδα διασφάλισης, ανάλογα τα μέσα που χρησιμοποιούνται

Μορφή Πιστοποιητικού	**Διαδικασία ελέγχου**	**Αδυναμία/Ρίσκο**
Φυσικό έγγραφο χωρίς ψηφιακά χαρακτηριστικά, π.χ. Κίτρινη Κάρτα ΠΟΥ	Οπτικός έλεγχος υπογραφών, σφραγίδων και τυχόν επισήματα ασφαλείας (αυτοκόλλητα) από εμβόλια	Συχνά είναι δύσκολη η ανίχνευση της αλλοίωσης και είναι δύσκολο να επιβεβαιωθεί ο εκδότης του Πιστοποιητικού
Φυσικό έγγραφο με μοναδικό προσδιοριστικό ή URL κωδικοποιημένο σε QR code, χωρίς άλλα ψηφιακά χαρακτηριστικά, π.χ. Ελληνικό ψηφιακό Πιστοποιητικό (αυτά με "μικρό QR")	Μπορεί να γίνει αναζήτηση του Πιστοποιητικού σε έμπιστες εθνικές αρχές της χώρας έκδοσης του Πιστοποιητικού σε εθνικές βάσεις δεδομένων της χώρας έκδοσης του Πιστοποιητικού. Το πιστοποιητικό αφότου βρεθεί μπορεί να απαιτεί επιπλέον ελέγχους για την επικύρωσή του (CRL ή OCSP checking)	Η αναζήτηση μπορεί να γίνει μόνο online, συνεπώς οι διατάξεις ελέγχου πρέπει να έχουν συνεχή σύνδεση με το διαδίκτυο.

Φυσικό ή ηλεκτρονικό έγγραφο με τα δεδομένα του Πιστοποιητικού ψηφιακά υπογεγραμμένα και κωδικοποιημένα σε κώδικα QR, π.χ. Εωρωπαϊκό Πιστοποιητικό Εμβολιασμού (αυτά με "μεγάλο QR")	Αποκωδικοποίηση QR κώδικα με φορητή συσκευή και offline έλεγχος ψηφιακών υπογραφών με βάση δημόσια κλειδιά έμπιστων αρχών πιστοποίησης που έχουν προαποθηκευθεί στη φορητή συσκευή	Η επαλήθευση μπορεί να γίνει οπουδήποτε. Απαιτούνται περιστασιακές συνδέσεις στο διαδίκτυο (π.χ. μία ανά 24 ώρες) για ενημέρωση των δημόσιων κλειδιών των αρχών πιστοποίησης.

Πίνακας 5 - Μορφή Πιστοποιητικού και δυνατότητα επαλήθευσης

Για την παραγωγή αξιόπιστων Πιστοποιητικών πρέπει κάθε χώρα να εξασφαλίζει τα παρακάτω:

- Να έχει μηχανισμούς διαπίστευσης των φορέων που εκδίδουν Πιστοποιητικά με βάση Υποδομή Δημόσιου Κλειδιού
- Να παρέχει στο κοινό απλούς μηχανισμούς επαλήθευσής των Πιστοποιητικών
- Να μπορεί να υποστηρίξει ανακλήσεις Πιστοποιητικών όπου χρειαστεί
- Οι λύσεις που θα επιλεγούν να είναι συμβατές με την προστασία των προσωπικών δεδομένων των εμβολιαζόμενων.
- Οι λύσεις που θα επιλεγούν να μπορούν να αξιοποιηθούν και από τρίτες χώρες που έχουν αναπτύξει διαφορετικές διαδικασίες και Υποδομές Εμπιστοσύνης

4.2 Έλεγχος Ακεραιότητας και Αυθεντικοποίηση Πιστοποιητικού

Ένα Πιστοποιητικό με τη μορφή δισδιάστατου ραβδοκώδικα QR μπορεί να διαβαστεί μια κατάλληλη εφαρμογή ελέγχου Πιστοποιητικών COVID-19, από οποιαδήποτε έξυπνο τηλέφωνο διαθέτει κάμερα. Οι εφαρμογές αυτές έχουν καταχωρημένο το σύνολο των δημόσιων κλειδιών των υπογραφόντων, καθώς και των κανόνων πρόσβασης σε υγειονομικά ελεγχόμενους χώρους. Όπως θα δούμε παρακάτω, οι εφαρμογές ενημερώνονται περιοδικά μέσω διαδικτύου με το τρέχον ισχύων σύνολο δημόσιων κλειδιών και κανόνων. Η εφαρμογή αναγνωρίζει τον ραβδοκώδικα QR και

αποκωδικοποιεί τα δεδομένα, καθώς και τα μεταδεδομένα υπογραφής. Στα μεταδεδομένα της υπογραφής εντοπίζει το αναγνωριστικό του δημόσιου κλειδιού, εκείνου που αντιστοιχεί στο ιδιωτικό κλειδί που που υπέγραψε το Πιστοποιητικό. Εάν η συσκευή ήδη γνωρίζει και έχει εσωτερικά καταχωρημένο το δημόσιο κλειδί που υπόγραψε το Πιστοποιητικό, τότε πρώτα παράγει το άθροισμα ελέγχου των δεδομένων, και μετά το συγκρίνει με το άθροισμα ελέγχου στα μεταδεδομένα του Πιστοποιητικού. Εάν αυτά ταυτίζονται, τότε το Πιστοποιητικό θεωρείται έγκυρο και αυθεντικό, και η συσκευή χρησιμοποιεί τους αποθηκευμένους κανόνες για να υπολογίσει αν πρέπει να επιτρέπεται η πρόσβαση σε ελεγχόμενους χώρους. Τελικά τα δεδομένα του Πιστοποιητικού παρουσιάζονται στο χρήστη σε αναγνώσιμη μορφή, μαζί με μια ρητή ένδειξη αν ισχύουν ή δεν ισχύουν υγειονομικοί περιορισμοί για τον κάτοχο.

5 Βασικά στοιχεία διαλειτουργικότητας

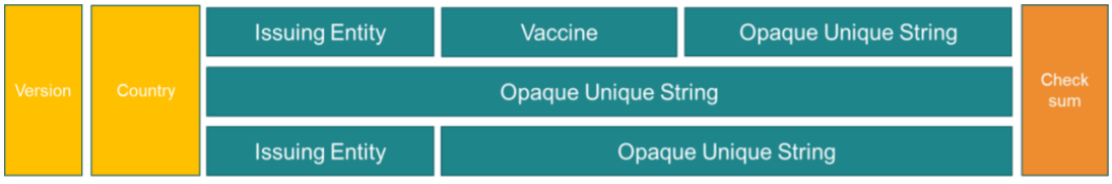
5.1 Μοναδικός αριθμός πιστοποίησης εμβολιασμού (Unique Vaccination Certificate Identifier, UVCI)

Κάθε Πιστοποιητικό για να είναι αξιόπιστο, πρέπει να μπορεί να συνδεθεί με τον διαπιστευμένο ιατρό ή ιατρικό κέντρο που το εξέδωσε αλλά και με και τη συγκεκριμένη πράξη εμβολιασμού. Συνεπώς είναι κρίσιμο να υπάρχει ένα μοναδικό προσδιοριστικό (UVCI) για κάθε ένα Πιστοποιητικό. Η μορφή του προσδιοριστικού έχει καθοριστεί στα [22] και [25].

Το UVCI ακόμα και σε χαρτί, μπορεί να χρησιμεύσει για την επαλήθευση του Πιστοποιητικού από online υπηρεσίες ή για την πλαισίωσή του από συμπληρωματικές πληροφορίες. Πέρα από μια εξωτερική κοινή δομή, επιτρέπεται στα κράτη μέλη να ενσωματώσουν επιπλέον λειτουργικότητες στη εσώτερη δομή του (π.χ. το είδος του εμβολίου), αλλά με ιδιαίτερη ευθύνη ως προς τη διαφύλαξη των προσωπικών δεδομένων και τη μοναδικότητά του. Η πιο ασφαλής προσέγγιση ως προς το ΓΚΠΔ είναι το UVCI να μην περιέχει καθόλου προσωπικά δεδομένα.

5.2 Σύνθεση μοναδικού προσδιοριστικού Πιστοποιητικού εμβολιασμού

Το μοναδικό προσδιοριστικό του Πιστοποιητικού εμβολιασμού (Unique Vaccination Certificate/assertion identifier - UVCI πρέπει να έχει συγκεκριμένα τμήματα στην εξωτερική του μορφή , να επιτρέπουν την επεξεργασία του σε όλα τα κράτη μέλη με ή χωρίς μηχανικά μέσα. Το εσωτερικό του τμήμα μπορεί να διαμορφωθεί με τρόπο διαφορετικό σε κάθε χώρα προκειμένου να επιτελέσει διαφορετικές λειτουργίες, τώρα ή στο μέλλον.



Εικόνα 3 - Εναλλακτικές μορφές UVCI

Το προσδιοριστικό θα πρέπει να είναι μοναδικό παγκοσμίως. Σε κάποιες περιπτώσεις μπορεί ήδη να περιέχει και πληροφορίες σε διακριτά πεδία, τα οποία να επιτρέπουν την προεπεξεργασία του Πιστοποιητικού ακόμα και χωρίς να είναι γνωστό το περιεχόμενό του.

Τα χαρακτηριστικά της εξωτερικής μορφής του UVCI είναι:

1. Το σύνολο χαρακτήρων είναι περιοριστικά ορισμένο σε κεφαλαία αλφαριθμητικά (‘A’ έως ‘Z’, ‘0’ έως ’9’), καθώς και τρείς χαρακτήρες που χρησιμοποιούνται για τη στίξη των επιμέρους τμημάτων του UVCI ('/', '#', ':') σύμφωνα με το συντακτικό των Universal Resource Identifiers (URIs) από το RFC3986 [68]
2. Μήκος 27-30 χαρακτήρες
3. Αριθμό έκδοσης ("01")
4. Κωδικό χώρας με δύο γράμματα (ISO 3166-1 alpha2) [55]
5. Το UVCI μπορεί να ακολουθεί άθροισμα ελέγχου όταν υπάρχει πιθανότητα λαθών κατά τη μετάδοση, π.χ. κατά την αντιγραφή από άνθρωπο. Σε αυτή την περίπτωση το προσδιοριστικό ακολουθείται από τον χαρακτήρα '#' και ακολούθως από ψηφίο ελέγχου ορισμένο κατά ISO-7812-1 Annex B

Όπως φαίνεται και στο παραπάνω σχέδιο, κάθε χώρα μπορεί να επιλέξει διαφορετική κωδικοποίηση για το UVCI, πάντα μέσα στα όρια των εξωτερικών χαρακτηριστικών του UVCI και του. Σε κάθε περίπτωση πρέπει να φροντίζει υπεύθυνα να μην κάνει επαναχρησιμοποίηση ενός UVCI σε περισσότερα του ενός Πιστοποιητικά. Επίσης οι τιμές σε τυχόν πεδία-υποδιαιρέσεις του UVCI πρέπει να γίνονται αντιληπτές με τον ίδιο τρόπο, ακόμα και σε άλλες χώρες, αλλά αυτό προϋποθέτει τη χρήση ενός κοινού λεξιλογίου, πράγμα που δεν είναι πάντα εφικτό σε διαφορετικές χώρες. Ο ασφαλέστερος τρόπος για να αποφεύγονται οι παρανοήσεις, είναι το UVCI πέρα από την κεφαλίδα αρχική έκδοσης και τον κωδικό χώρας να είναι ένας συμπαγές προσδιοριστικό αποτελούμενο αποκλειστικά από κεφαλαίους αλφαριθμητικούς χαρακτήρες.

5.3 Κωδικοποίηση δεδομένων

Οι πληροφορίες που περιέχονται στο Πιστοποιητικό λαμβάνουν κωδικοποιημένες τιμές σύμφωνα με πρότυπα από οργανισμούς που είναι παγκοσμίως αποδεκτοί (WHO [12], [14], ICAO [37], HL7 [15], [16], SNOMED [38], ISO [29]). Οι τιμές αυτές και το πρότυπα στο οποίο ορίζονται αναφέρονται αναλυτικά σε κατάλογο στον κανονισμό της 1073/2021/ΕΕ [25], και σε ενημερώσεις του που δημοσιεύονται επίσημα στον ιστοχώρο της ΕΕ [21].

5.4 Μορφότυπος Δήλωσης Ψηφιακού Πιστοποιητικού (HCERT)

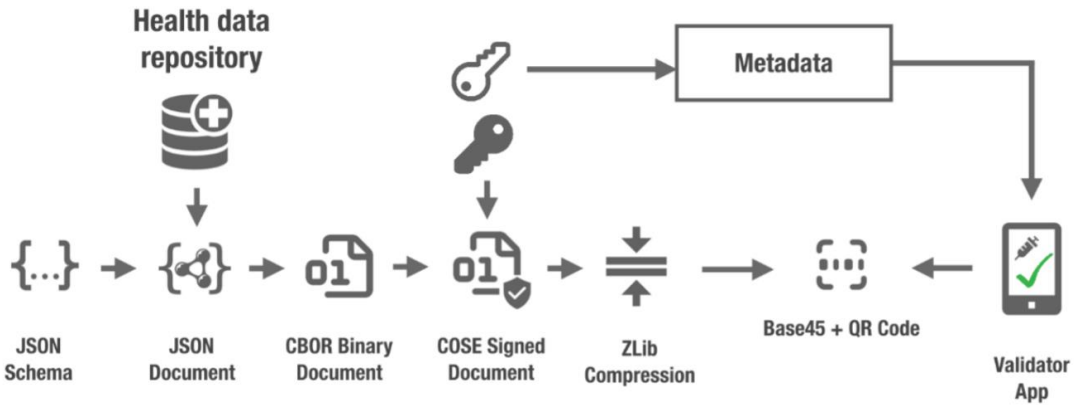
Σύμφωνα με το σχέδιο [21] που αναπτύχθηκε από το δίκτυο eHealth [20], οι παραπάνω πληροφορίες τοποθετούνται σε πεδία μιας συγκεκριμένης δομής (schema) [34] JSON [39] με συγκεκριμένα ονόματα και τιμές.

Ακολούθως γίνεται μετατροπή σε αναπαράσταση CBOR (Concise Binary Object Representation [41]). Αυτό γίνεται γιατί οι δομές JSON εκ σχεδιασμού είναι φτιαγμένες για να μπορούν να αναγνωστούν κατευθείαν και από άνθρωπο χωρίς βοηθήματα, με τη μορφή κειμένου Unicode, συνήθως κωδικοποιημένου σε UTF-8. Αυτό προσθέτει μέγεθος σε bytes και συντακτικούς κανόνες που απαιτούν πολλαπλάσιους υπολογιστικούς κύκλους επεξεργασίας και συνεπώς και πολλαπλάσια ενεργειακή κατανάλωση ενέργειας. Αντίθετα, οι σχεδιαστικοί στόχοι του CBOR περιλαμβάνουν τη δυνατότητα εξαιρετικά μικρού μεγέθους κώδικα, αρκετά μικρού μεγέθους μηνύματος και επεκτασιμότητας χωρίς αλλαγή στην έκδοση.

Το CBOR συνοδεύεται από μια ψηφιακή υπογραφή COSE [42] η οποία είναι υπεύθυνη για την ακεραιότητα του μηνύματος CBOR. Τα δύο μαζί μηνύματα αποτελούν ένα CBOR

Web Token (CWT) [43]. Έπειτα ακολουθεί συμπίεση της δομής με τη βιβλιοθήκη zlib [44]. Το αποτέλεσμα κωδικοποιείται σε κώδικα BASE45 [46].

Η παραπάνω δομή των δεδομένων φαίνεται στο παρακάτω σχέδιο



Εικόνα 4 - Κωδικοποίηση πιστοποιητικού υγείας HCERT

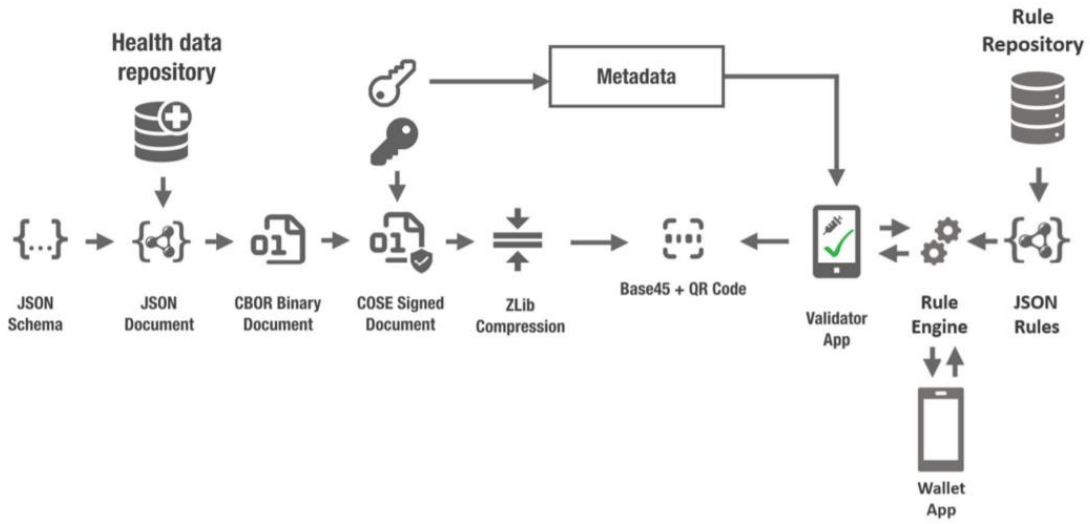
5.5 Κανόνες Επικύρωσης Ψηφιακού Πιστοποιητικού

Ανάλογα τον τόπο, τον χρόνο και τη χρήση ενός πιστοποιητικού, αυτό μπορεί να σημαίνει διαφορετική αντιμετώπιση του κατόχου. Π.χ. τα τρία αυτά πιστοποιητικά έχουν διαφορετικές διάρκειες εγκυρότητας (π.χ. τα πιστοποιητικά διαγνωστικού ελέγχου πρέπει να χρησιμοποιούνται εντός 48 ωρών). Επειδή οι κανόνες αυτοί πρέπει να μπορούν να αλλάζουν ανάλογα τις αποφάσεις των υγειονομικών, αυτοί δεν περιλαμβάνονται μέσα στο πιστοποιητικό αλλά αναρτώνται ξεχωριστά από κάθε χώρα σε κατάλληλο σημείο που ώστε να χρησιμοποιούνται από τις εφαρμογές ελέγχου στις φορητές συσκευές [46].

Κάθε χώρα αποφασίζει τους δικούς της κανόνες επικύρωσης π.χ. την απαίτηση για ύπαρξη πρόσφατου μοριακού διαγνωστικού ελέγχου έως 72 ωρών πριν την είσοδο στη χώρα ή σε ένα θέατρο. Αυτοί οι κανόνες ισοδυναμούν με απλούς περιορισμούς σε επιμέρους μεταβλητές του πιστοποιητικού. Τέτοιοι περιορισμοί μπορούν να εκφράζονται σε γλώσσα JsonLogic [47], η οποία περιγράφει με απλό και μηχαναγνώσιμο τρόπο τα κριτήρια και τους συνδυασμούς τιμών που πρέπει να ικανοποιεί ένα πιστοποιητικό για να θεωρηθεί

έγκυρο. Η JsonLogic είναι εκ σχεδιασμού κατάλληλη για την δυναμική διαχείριση κανόνων που μεταβάλλονται ανεξάρτητα από το πρόγραμμα που τους εφαρμόζει.

Οι κανόνες αυτοί με τη μορφή JsonLogic υπογράφονται ψηφιακά από τις χώρες μέλη και αναρτώνται στην Κεντρική Ευρωπαϊκή Πύλη για γνωστοποίηση στις υπόλοιπες χώρες, μαζί με τα πιστοποιητικά των Αρσχών που υπογράφουν EU DCCs. Από εκεί οι χώρες μέλη ενημερώνουν τα εθνικά τους αποθετήρια, από τα οποία με τη σειρά τους ενημερώνονται περιοδικά και οι τελικές εφαρμογές που τα χρησιμοποιούν, τουλάχιστον μία φορά κάθε ημέρα. Οι κανόνες και τα πιστοποιητικά οφείλουν να αναρτώνται τουλάχιστον 48 ώρες πριν την έναρξη της ενεργοποίησής τους. Εφόσον μια συσκευή έχει ενημερώσει πρόσφατα τους κανόνες και τα αποδεκτά πιστοποιητικά ο έλεγχος των κανόνων και των EU DCCs γίνεται offline, χωρίς σύνδεση με το διαδίκτυο. Η λογική περιγράφεται στο κεφάλαιο Διαχείρισης Εμπιστοσύνης.



Εικόνα 5 - Επικύρωση με κανόνες από αποθετήριο κανόνων

6 Αποσυμπίληση ενός πραγματικού Πιστοποιητικού

Για τους σκοπούς του παρόντος θα εφαρμόσουμε τα εργαλεία ανοιχτού κώδικα της ΕΕ για να ανοίξουμε ένα πραγματικό δείγμα ευρωπαϊκού Πιστοποιητικού και να εξετάσουμε τα περιεχόμενά του αφαιρώντας τα διάφορα στρώματα κωδικοποίησης που τα καλύπτουν. Επίσης θα αναδείξουμε την προτυποποίηση για κάθε ένα στοιχείο που αυτά περιέχουν. Αφετηρία θα αποτελεί το παρακάτω έντυπο ψηφιακό Πιστοποιητικό.

Εικόνα 6 - Έντυπη μορφή ψηφιακού Πιστοποιητικού

Το τυπωμένο Πιστοποιητικό χρησιμοποιεί το υπόδειγμα που προτείνεται από την πηγή της ΕΕ [48]. Όπως αναγράφει και πάνω του, το Πιστοποιητικό δεν αποτελεί ταξιδιωτικό έγγραφο, συνεπώς χρειάζεται να συνοδεύεται από κάποιο άλλο έγγραφο ταυτοποίησης. Η χρήση δισδιάστατου ραβδοκώδικα QR [29] καθιστά δυνατό τον έλεγχο με ένα έξυπνο τηλέφωνο, των αναγραφόμενων σε σχέση με την ψηφιακή υπογραφή που περιέχει. Στα επόμενα στάδια θα επεξεργαστούμε ένα σαρωμένο αντίγραφο του Πιστοποιητικού που θα το αποθηκεύσουμε σε ένα απλό αρχείο εικόνας τύπου PNG ("certificate-of-vaccination.png").

6.1 Αφαίρεση εξωτερικών στρωμάτων κωδικοποίησης

6.1.1 Αφαίρεση ραβδοκώδικα QR

Ο ραβδοκώδικας ορίζεται ότι θα κωδικοποιεί μόνο αλφαριθμητικά δεδομένα (QR Mode 2) για να μην υπάρχουν προβλήματα συμβατότητας με παλαιότερο εξοπλισμό QR. Αυτό το σύνολο χαρακτήρων με τη βοήθεια της κωδικοποίησης σε ASCII base45 [46] κωδικοποιεί τα περιεχόμενα που βρίσκονται στα εσώτερα στρώματα του Πιστοποιητικού.

Παρακάτω χρησιμοποιούμε την εφαρμογή αναφοράς [49] της ΕΕ για έξυπνα τηλέφωνα η οποία μπορεί να διαβάσει το συγκεκριμένο δισδιάστατο ραβδοκώδικα με την κάμερα της συσκευής, και να ελέγξει την εγκυρότητά του. Όμως σε αυτό το στάδιο θα χρησιμοποιήσουμε εργαλεία γραμμής εντολών, και συγκεκριμένα το zbarimg [51] σε περιβάλλον Ubuntu Linux 21.10 [51] το οποίο μπορεί να εξάγει και να αποκωδικοποιήσει τον κώδικα QR από ένα αρχείο εικόνας. Στο ίδιο περιβάλλον θα συνεχίσουμε την ανάλυσή του εξαγόμενου κώδικα με απλά εργαλεία Linux και τα απλά εργαλεία αναφοράς [50] που έχει δημοσιεύσει το δίκτυο eHealth της ΕΕ, για να αποφλοιώσουμε τα διάφορα επίπεδα κωδικοποίησης μέχρι να φτάσουμε στο ωφέλιμο περιεχόμενο του Πιστοποιητικού.

Εικόνα 7 - Δισδιάστατος ραβδοκώδικας QR

```
Linux $ zbarimg --raw certificate-of-vaccination.png > decode-stage1-
QR-removed

scanned 1 barcode symbols from 1 images in 0.03 seconds

Linux$ cat decode-stage1-QR-removed

HC1:NCFOXNEG2NBJ5*H:QO-.O%9S ILECSM$9:5BZKP09N:X91EE5TLSRHMJ9Z-
P92P*AVAN9I6T5XH4PIQJAZGA+1V2:U:PI/E2$4JY/K7ZA8+JR9E/D4
0AE/6899YW0NJHY/CQTJD/DOKEH-BS/D2QCKVKU8L38KGVKK3D9JA6+B3BB7-
VGUH1V5POIRD8M.SY$NZV9U50UES83GTFWG+SB.V
Q5AO96J0TM8%YBWYQ1RM8ZAUZ4+FJE 4Y3LL/II
0OC9SX0+*B85T%6213PPHN6D7LLK*2HG%89UVM:K35TMKN4NN3F85QNCY0O%0D0H0
29B9+HFUE9ZC59B9LW4G%89-85QNG.8N680OPZ48XW44$2JDL
PNGKF4J56P5H0D3ZCL4JMYAZ+SFC5QWCD4D-
T4T6599TP*FI7JM7JHOJKYJPGK:H3J1D1I3-*TW CXBD+$3T*C3CU3 3%2T1KT
TD8O2MJSA+2.VS+TD*B2.GC6DLAC30DMUNENYQZL2YK7S0EBPBEZKTFA1QM06MILDBRLT
9KR.F-B39LE30E:YR0/SSSN3DBL:P3NPK+URH7O05
/53$7TWIK$VDCKO+F50I3H0KM5/1K

Linux $ wc -c decode-stage1-QR-removed

617 decode-stage1-QR-removed
```

Πίνακας 6 - Αφαίρεση HCERT header, base45 και συμπίεσης zlib

6.1.2 Αφαίρεση κεφαλίδας, κωδικοποίησης Base45 και συμπίεσης ZLIB

Από τη μετατροπή προέκυψε ένα μεγάλο αλφαριθμητικό μήκους 617 χαρακτήρων που ξεκινά με τους χαρακτήρες "HC1:" και το οποίο φυλάχθηκε στο αρχείο decode-stage1-QRremoved. Σύμφωνα με τα §5.2.2 και §5.2.1 της 1073/2021/ΕΕ [25], ακολουθεί ωφέλιμο φορτίο κωδικοποιημένο σε base45, και το οποίο με τη σειρά του περιέχει ένα CBOR Web Token (CWT, [43]) το οποίο έχει συμπιεστεί με χρήση της βιβλιοθήκης ZLIB (RFC1950, [44]) βιβλιοθήκης Deflate (RFC1951, [45]). Θα τοποθετήσουμε το παραπάνω αλφαριθμητικό σε ένα αρχείο "decode-stage2-HC1header-removed" αφού αφαιρέσουμε πρώτα την κεφαλίδα 'HC1:', με το utility "sed" [53] οπότε και έχουμε:

```
Linux$ sed 's/^HC1://' decode-stage1-QR-removed >decode-stage2-
HC1header-removed

Linux$ cat decode-stage2-HC1header-removed

NCFOXNEG2NBJ5*H:QO-.O%9S ILECSM$9:5BZKP09N:X91EE5TLSRHMJ9Z-
P92P*AVAN9I6T5XH4PIQJAZGA+1V2:U:PI/E2$4JY/K7ZA8+JR9E/D4
0AE/6899YW0NJHY/CQTJD/DOKEH-BS/D2QCKVKU8L38KGVKK3D9JA6+B3BB7-
VGUH1V5POIRD8M.SY$NZV9U50UES83GTFWG+SB.V
Q5AO96J0TM8%YBWYQ1RM8ZAUZ4+FJE 4Y3LL/II
0OC9SX0+*B85T%6213PPHN6D7LLK*2HG%89UVM:K35TMKN4NN3F85QNCY0O%0D0H0
29B9+HFUE9ZC59B9LW4G%89-85QNG.8N680OPZ48XW44$2JDL
PNGKF4J56P5H0D3ZCL4JMYAZ+SFC5QWCD4D-
T4T6599TP*FI7JM7JHOJKYJPGK:H3J1D1I3-*TW CXBD+$3T*C3CU3 3%2T1KT
TD8O2MJSA+2.VS+TD*B2.GC6DLAC30DMUNENYQZL2YK7S0EBPBEZKTFA1QM06MILDBRLT
9KR.F-B39LE30E:YR0/SSSN3DBL:P3NPK+URH7O05
/53$7TWIK$VDCKO+F50I3H0KM5/1K
```

Πίνακας 7 - Αφαίρεση Header "HC1:"

Έπειτα αφαιρούμε την κωδικοποίηση κατά base45.

```
Linux$ base45 --decode < decode-stage2-HC1header-removed > decode-
stage3-removed-base45
Linux$ file decode-stage3-removed-base45

decode-stage3-removed-base45: zlib compressed data
```

Πίνακας 8 - Αφαίρεση κωδικοποίησης base45

Παρατηρούμε ότι μετά από αυτό το στάδιο μένει ένα αρχείο decode-stage3-removed-base45 που είναι συμπιεσμένο με τη βιβλιοθήκη ZLIB. Θα δοκιμάσουμε να το αποσυμπιέσουμε με το utility pigz (parallel gzip [54]), το οποίο τυχαίνει να βασίζεται στη βιβλιοθήκη ZLIB.

```
$ pigz --decompress <decode-stage3-removed-base45 >decode-stage4-uncompressed
```

Πίνακας 9 – Αποσυμπίεση δεδομένων

Μετά την αποσυμπίεση απομένει ένα αρχείο δυαδικού χαρακτήρα που δεν περιέχει μέσα μόνο κείμενο. Εξετάζοντάς το με το utility "strings" [69] ξεχωρίζουμε ανάμεσα σε διάφορους χαρακτήρες εμφανίζονται τα στοιχεία του Πιστοποιητικού!

```
$ strings decode-stage4-uncompressed

Y αvbGR9

cvere1.3.0cnam

bfnx

cfntmPAPAGIANNAKISbgnr

cgntiAPOSTOLOScdobj1970-11-25av

btgi840539006bvpgJ07BX03bmplEU/1/20/1507bmamORG-100031184bdn

bdtj2021-12-03bcobGRbisx&IDIKA / Ministry of Digital
Governancebcix+URN:UVCI:01:GR:2OK7TZJAEC4RTPIFRLIS6XQH6A#9X@
```

Πίνακας 10 – Προβολή περιεχόμενων συμβολοσειρών

6.2 Έλεγχος ακεραιότητας και αυθεντικότητας υπογραφής

Σύμφωνα με τα προαναφερθέντα το αρχείο decode-stage4-uncompressed είναι ένα δυαδικό αρχείο που περιέχει μια δομή CWT (CBOR Web Token). Το αρχείο αυτό είναι ο μορφότυπος HCERT που περιγράφεται στο πρότυπο των EU DCCs, και το οποίο περιέχει μια δομή COSE (Cbor Object Signing and Encryption) η οποία με τη σειρά της υπογράφει

ψηφιακά μια δομή CBOR (Consise Binary Object Representation). Η τελευταία αυτή δομή αποτελεί το ωφέλιμο φορτίο όλων των ανωτέρω στρωμάτων, και περιέχει το αντικείμενο JSON σε μια δυαδική μορφή η οποία ελαχιστοποιεί την επεξεργασία που χρειάζεται για την ανάγνωσή της, καθιστώντας την κατάλληλη για συσκευές που έχουν περιορισμένη ενέργεια στη διάθεσή τους.

Μέχρι αυτό το στάδιο ήταν εφικτό να αφαιρέσουμε τα υπερκείμενα στρώματα κωδικοποίησης με ανεξάρτητα off-the-shelf εργαλεία. Τα επόμενα στάδια είναι επίσης τυποποιημένα, αλλά η ανάγνωσή τους χρειάζεται να γίνει με τη χρήση του απλού εργαλείου αναφοράς hc1_verify.py [50], σε περιβάλλον γραμμής εντολών. Το εργαλείο αυτό το χρησιμοποιούμε με επιλογή να παραλείψει τα στάδια αποκωδικοποίησης που εκτελέσαμε παραπάνω με ανεξάρτητα εργαλεία.

```
01 Linux$ $ python3 hc1_verify.py --skip-base45 --skip-zlib --use-verifier --noanon --prettyprint-json --verbose <decode-stage4-uncompressed
02 Correct signature againt known key (kid=vvYa1vaWkGg=)

03 Signature      : vvYa1vaWkGg= @ ES256

04 Issued At      : 1638597959

05 Experation time   : 1684946124

06 Issuer       : GR

07 Health payload   : {

08   "dob": "1970-11-25",

09   "nam": {

10     "fn": "ΠΑΠΑΓΙΑΝΝΑΚΗΣ",

11     "fnt": "PAPAGIANNAKIS",

12     "gn": "ΑΠΟΣΤΟΛΟΣ",

13     "gnt": "APOSTOLOS"
```

```
14   },
15   "v": [
16     {
17       "ci": "URN:UVCI:01:GR:2OK7TZJAEC4RTPIFRLIS6XQH6A#9",
18       "co": "GR",
19       "dn": 3,
20       "dt": "2021-12-03",
21       "is": "IDIKA / Ministry of Digital Governance",
22       "ma": "ORG-100031184",
23       "mp": "EU/1/20/1507",
24       "sd": 3,
25       "tg": "840539006",
26       "vp": "J07BX03"
27     }
28   ],
29   "ver": "1.3.0"
30 }
```


Πίνακας 11 - Απόπειρα ανοίγματος του αρχείου

Ακολούθως κάνουμε τις αναφορές των πεδίων που βρέθηκαν προς την απόφαση 1073/2021/ΕΕ [25] για να δείξουμε και να επιβεβαιώσουμε κι εμείς ότι όλες έχουν νομική ισχύ.

Line	COSE key	COSE value	Comment	reference
02	kid	vvYa1vaWkGg=	Key Identifier	§3.2.3/1073/2021/EE [25]
03	alg	ES256	Elliptic Curve Digital Signature Algorithm, ECDSA	§3.2.2/1073/2021/EE [25]
04	iat	1638597959	Σαβ, 4 Δεκεμβρίου 2021 8:05:59 ΠΜ GMT+02:00	RFC8392 [43]
05	exp	1684946124	Τετ, 24 Μαΐου 2023 7:35:24 ΜΜ GMT+03:00 DST	RFC8392 [43]
06	iss	GR	Κωδικός υπογράφουσας χώρας	ISO 3166-1 alpha-2 set [55]

Πίνακας 12 - Πεδία (claims) υπογραφής COSE μέσα στο CWT

Αρχικά στις γραμμές 02-06 φαίνονται οι πληροφορίες που περιέχονται μέσα στην δομή COSE στο Cbor Web Token. Η υπογραφή είχε τεθεί από κλειδί με αναγνωριστικό κλειδιού "vvYa1vaWkGg=". Μαζί με τον αλγόριθμο υπογραφής COSE "alg", παρέχουν hints στην συσκευή ανάγνωσης για να αποφύγει να ελέγξει περισσότερες από μία υπογραφές. Τα πεδία με το χρόνο έκδοσης ("iat" κατά §3.2.6) και λήξης ("exp" κατά §3.2.5) αφορούν την εγκυρότητα της υπογραφής και όχι το περιεχόμενο του Πιστοποιητικού και ερμηνεύονται σύμφωνα με το RFC8392 [43] ως αριθμός δευτερολέπτων από την αρχή του 1/1/1970, 00:00 GMT. Επίσης στη δήλωση εκδότη ("iss" κατά §3.2.4) [55] περιέχεται ο κωδικός "GR" της Ελλάδας σύμφωνα με το πρότυπο διγράμματων διεθνών συντομεύσεων ISO 3166-1 alpha-2. Έπειτα ακολουθεί το ωφέλιμο φορτίο:

Line	COSE key	COSE value	Comment	reference
08	dob	1970-22-25	Ημερομηνία γέννησης	§3.2.3/1073/2021/EE [25]
10	nam/fn	ΠΑΠΑΓΙΑΝΝΑΚΗΣ	Επώνυμο σε UTF-8	Σχήμα JSON [34]

11	nam/fnt	PAPAGIANNAKIS	Επώνυμο όπως στα ταξιδιωτικά έγγραφα	Σχήμα JSON [34], ICAO Doc 9303 Part 3 [37]
12	nam/gn	ΑΠΟΣΤΟΛΟΣ	Όνομα σε UTF-8	Σχήμα JSON [34]
13	nam/gnt	APOSTOLOS	Όνομα όπως στα ταξιδωτικά έγγραφα	Σχήμα JSON [34], ICAO Doc 9303 Part 3 [37]
17	ci	URN:UVCI:01:GR:2OK7TZJAEC4RTPIFRLIS6XQH6A#9	Μοναδικό προσδιοριστικό Δήλωσης Πιστοποιητικού υγείας	Παράρτημα III 1073/2021/ΕΕ [25]
18	co	GR	Κωδικός χώρας από την οποία γίνεται η δήλωση	ISO 3166-1 alpha-2 set [55]
19	dn	3	Αριθμός σε σειρά δόσεων	
20	dt	2021-12-03	Ημερομηνία εμβολιασμού	
21	is	IDIKA / Ministry of Digital Governance	Εκδότης Πιστοποιητικού μέσα στη χώρα	Παράρτημα III 1073/2021/ΕΕ [25]
22	ma	ORG-100031184	Κατασκευαστής εμβολίου (Spikevax, Previously COVID-19 Vaccine Moderna)	Σύνολα τιμών [30]
23	mp	EU/1/20/1507	Ιατρικό προϊόν αναφερόμενο με τον αριθμό έγκρισής του	Σύνολα τιμών [30]
24	sd	3	Συνολικό ποσό απαιτούμενων δόσεων	Σύνολα τιμών [30]

25	tg	840539006	Κωδικός στοχευόμενης νόσου, κωδικός σύμφωνα με το κλινικό πρότυπο SNOMED-CT (COVID-19),	Παράρτημα II 1073/2021/ΕΕ [25]
26	vp	J07BX03	Εμβόλιο κατά της νόσου COVID-19, κωδικός σύμφωνα με το κλινικό πρότυπο SNOMED-CT (COVID-19)	Παράρτημα II 1073/2021/ΕΕ [25]
27	ver	1.3.0	Έκδοση Σχήματος JSON	Σύνολα τιμών [30]

Πίνακας 13 - Ωφέλιμο φορτίο HCERT

Αποκωδικοποιώντας τη δυαδική δομή CBOR και μετατρέποντάς τη σε ένα JSON αντικείμενο (βλ. ορισμό σχήματος [30]) βρίσκουμε τη μορφή κειμένου του Πιστοποιητικού Εμβολιασμού. Όπως περιγράφεται και στο §3.2.7 [25] η αποκωδικοποίηση μέχρι το επίπεδο JSON κατά την ανάγνωση του Πιστοποιητικού δεν είναι απαραίτητη, καθώς τα στοιχεία της υπάρχουν ήδη από το προηγούμενο στάδιο (CBOR). Αυτό είναι ιδιαίτερα σημαντικό για τις συσκευές που έχουν ενεργειακούς περιορισμούς, και για την κατά το δυνατό γρήγορη απόκριση των συσκευών ελέγχου.

Το πεδίο "ci" είναι το παγκοσμίως μοναδικό προσδιοριστικό της δήλωσης (UCI, Universal Certificate Identifier). Η μορφή του και η κωδικοποίησή του σε χαρακτήρες είναι καθορισμένα στο Παράρτημα III [25]. Περιέχει κεφαλίδα URN (rfc8141 [56]) με ιδιαίτερο χώρο ονομάτων ("UVCI"), έκδοση ("01") και κωδικό χώρας ("GR") κατά ISO 3166-1 [55], η οποία αποδίδει το εκάστοτε UCI. Το αλφαριθμητικό UCI όταν μεταδίδεται με ηλεκτρονικά μέσα, επακολουθεί υποχρεωτικά ένα διαχωριστικό ψηφίο "#" και ένα μονοψήφιο άθροισμα ελέγχου σύμφωνα με το πρότυπο ISO-7812-1 (LUHN-10, [57]). Το άθροισμα ελέγχου χωρίζεται από το υπόλοιπο UCI με τον χαρακτήρα "#". Οι δύο αυτοί χαρακτήρες τεχνικά δεν αποτελούν μέρος του Πιστοποιητικού.

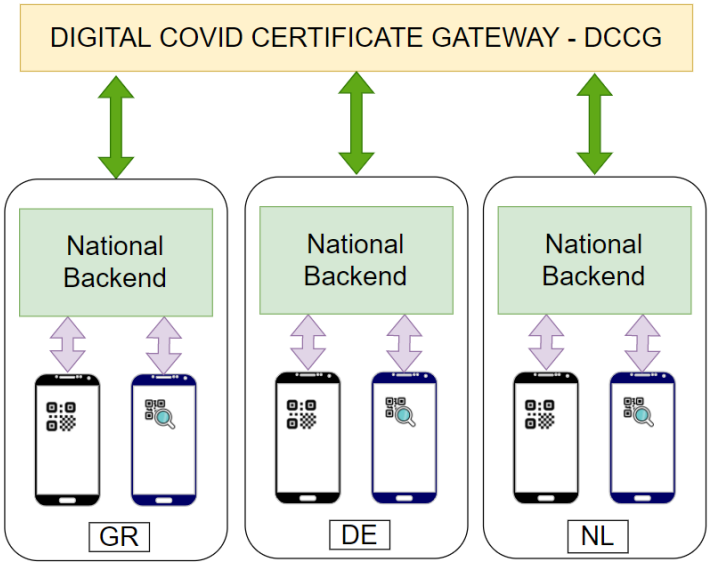
Παρατηρούμε ότι και τα υπόλοιπα claims αποτελούνται από διγράμματους κωδικούς χάριν ελάττωσης του μεγέθους της δομής: "co", "dn", "dt", "is" κλπ.

7 Εθνικοί κόμβοι και Ευρωπαϊκή Πύλη διαχείρισης Εμπιστοσύνης

Κάθε Πιστοποιητικό έχει αξία όταν εκδίδεται από αξιόπιστους εκδότες, και μπορεί να επαληθευθεί χωρίς σημαντική προσπάθεια. Για αυτό το σκοπό κάθε Πιστοποιητικό φέρει ψηφιακή υπογραφή με δημόσιο κλειδί το οποία καθιστά ανιχνεύσιμη οποιεσδήποτε παρέμβαση στο περιεχόμενό του, και συνδέει μονοσήμαντα το περιεχόμενο με τον εκδότη του Πιστοποιητικού.

Η διαδικασία ελέγχου των Ψηφιακών Πιστοποιητικών είναι σχεδιασμένη ώστε να γίνεται offline, δηλ. να μην απαιτεί συνεχή πρόσβαση στο διαδίκτυο. Τα πιστοποιητικά COVID-19 ελέγχονται αν είναι υπογεγραμμένα με το δημόσιο κλειδί από κάποια γνωστή Αρχή Έκδοσης. Τα δημόσια αυτά κλειδιά πρέπει να είναι γνωστά εκ των προτέρων στη συσκευή με την οποία γίνεται ο έλεγχος. Όμως τα κλειδιά από τις Αρχές Έκδοσης ενδέχεται να αντικαθίστανται καθώς μια Αρχή Έκδοσης μπορεί να αλλάξει τα κλειδιά της π.χ. σε περιπτώσεις ανάκλησης ή και στην περίπτωση που προστίθεται ή αφαιρούνται οντότητες που υπογράφουν Πιστοποιητικά. Για αυτό το λόγο όλες οι συσκευές ελέγχου συνδέονται κατά την πρώτη τους σύνδεση αλλά και περιοδικά σε αραιά διαστήματα (π.χ. άπαξ ανά 24ωρο) με τον αρμόδιο εθνικό κόμβο. Οι περισσότερες χώρες που συμμετέχουν στο σχήμα των Ευρωπαϊκών Πιστοποιητικών διατηρούν ένα κόμβο ο οποίος μοιράζει τα κλειδιά αυτά στις εφαρμογές πελάτες που τα ζητούν.

Για να μπορούν να ελέγξουν Πιστοποιητικά που έχουν δημιουργηθεί σε άλλες χώρες, οι εθνικοί κόμβοι ανταλλάσσουν και διαπιστεύουν εθνικά κλειδιά μεταξύ τους. Αυτό δεν το κάνουν με απευθείας επικοινωνία, αλλά μέσω ενός κόμβου Ευρωπαϊκής Πύλης Digital COVID-19 Certificate Gateway (EU DCCG) στον οποίο όλες οι χώρες αναρτούν τα κλειδιά από τις δικές τους Αρχές Έκδοσης Πιστοποιητικών αλλά και τους κανόνες Επικύρωσής τους. Το σημαντικό είναι ότι όλα τα στάδια επικοινωνίας προστατεύονται με αμοιβαία ταυτοποίηση και εξουσιοδότηση με χρήση TLS πρωτόκολλων. Όλες οι λίστες κλειδιών και κανόνων που ανταλλάσσονται είναι υπογεγραμμένες με τα κλειδιά των χωρών. Τα κλειδιά των χωρών διακινούνται μέσω ειδικής γραμματείας της ΕΕ. Στο σχήμα που ακολουθεί φαίνεται πως οι έξυπνες συσκευές που προβάλουν και ελέγχουν τα πιστοποιητικά επικοινωνούν περιοδικά με τους εθνικούς κόμβους (National Backends). Με τη σειρά τους οι εθνικοί κόμβοι επικοινωνούν με την Ευρωπαϊκή Πύλη DCCG.



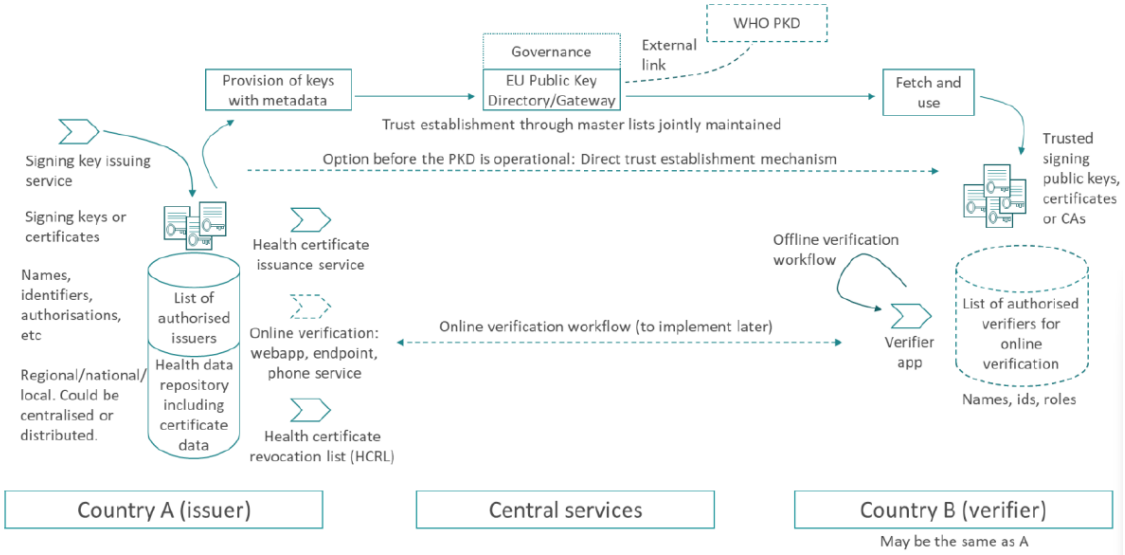
Εικόνα 8 Κόμβοι Εμπιστοσύνης

7.1 Ιεραρχία Εμπιστοσύνης

Αυτός που κάνει τον έλεγχο των Πιστοποιητικών, θα πρέπει να γνωρίζει τα δημόσια κλειδιά όλων των φορέων που εκδίδουν Πιστοποιητικά, σε όλα τα κράτη μέλη αλλά και σε όσες χώρες έχουν προσχωρήσει σε συμφωνίες αλληλοαναγνώρισης με την ΕΕ [64]. Κάθε χώρα είναι υπεύθυνη να διατηρεί μια ιεραρχία πιστοποιητικών υπογραφής με δύο μόνο επίπεδα. Η διαδικασία έχει περιγραφεί αναλυτικά στη νομοθεσία στο παράρτημα IV της Εκτελεστικής Απόφασης (ΕΕ) 2021/1073 [25]. Στο ανώτερο επίπεδο υπάρχουν μία ή περισσότερες αρχές πιστοποίησης επιπέδου χώρας (Certificate Signer Certificate Authorities, CSCAs) που με τη σειρά τους υπογράφουν τα πιστοποιητικά (Document Signing Certificates, DSCs) των οντοτήτων που υπογράφουν τα πιστοποιητικά COVID-19, συνήθως από κρατικές υγειονομικές αρχές. Η λίστα παράγεται με τον ίδιο τρόπο όπως και αυτή που χρησιμοποιείται από τον ICAO για τα μηχαναγνώσιμα έγγραφα eMRTD (Machine Readable Travel Documents) [37]. Τα CSCAs κατά κανόνα είναι αυθυπόγραφα, αλλά είναι δυνατό να είναι τα ίδια που χρησιμοποιούνται και στην ιεραρχική δομή του ICAO/eMRTD. Επίσης είναι δυνατό να υπάγονται σε ιεραρχία εμπορικών αρχών πιστοποίησης, ή και εγκεκριμένων αρχών πιστοποίησης αναγνωρισμένων κατά eIDAS [59] αλλά για τους σκοπούς του Ευρωπαϊκού Πιστοποιητικού τα CSCAs θεωρούνται η ανώτερη άγκυρα εμπιστοσύνης.

Κάθε χώρα δημοσιεύει προς στην ΕυρωπαΙκή Πύλη Ψηφιακών Πιστοποιητικών (DCCG) τα πιστοποιητικά CSCAs και DSCs αλλά και τους κανόνες επικύρωσης πιστοποιητικών. Εκεί διατηρείται κεντρικό αποθετήριο από όλα τα κλειδιά και τους κανόνες επικύρωσης της ένωσης αλλά και από τρίτες χώρες που έχουν προσχωρήσει στο ίδιο σχήμα εμπιστοσύνης.

Για λόγους απλότητας των διατάξεων επαλήθευσης, κατά τον έλεγχο ενός πιστοποιητικού δεν γίνεται έλεγχος ανακλήσεων των πιστοποιητικών (CRL ή OCSP checking). Τα πιστοποιητικά και οι κανόνες επικύρωσης που ανακαλούνται ή λήγουν πρέπει να αφαιρούνται από τη λίστα που δημοσιεύει κάθε χώρα προς την Ευρωπαϊκή Πύλη.



Εικόνα 9 Σχέσεις εμπιστοσύνης στα Ευρωπαϊκά Πιστοποιητικά [33]

Τα πιστοποιητικά CSCA έχουν σχετικά μεγάλη διάρκεια, η οποία υπερκαλύπτει τη διάρκεια των DSCs. Η διάρκεια των DSCs είναι σχετικά μικρή ώστε στην περίπτωση που για οποιοδήποτε λόγο ανακαλείται ένα πιστοποιητικό DSC να επηρεάζονται κατά το δυνατό μικρότερος αριθμός Πιστοποιητικών COVID-19. Για τον ίδιο λόγο είναι δυνατό σε μία χώρα, να χρησιμοποιούνται ταυτόχρονα περισσότερα του ενός CSCAs.

Επίσης σε κάθε χώρα λειτουργεί κόμβος από όπου οι τοπικές εφαρμογές στις τερματικές συσκευές μπορούν να αναδιανέμουν την εθνική λίστα DCSs αλλά και τις λίστες DCSs που έχουν δημοσιευτεί στο αποθετήριο DCCG. Επίσης στον εθνικό κόμβο μπορούν να δημοσιεύουν αποδεκτά πιστοποιητικά και κανόνες, με βάση απευθείας διμερείς

συμφωνίες με τρίτες χώρες, ανεξάρτητα από την ΕΕ. Το ίδιο συμβαίνει και με τους κανόνες επικύρωσης. Εκτιμάται ότι για πλήθος 30 χωρών που αλλάζουν το κλειδί τους κάθε 1 μήνα, σε ένα διάστημα 5 ετών θα απαιτηθούν 1800 κλειδιά ή περίπου 1Mbyte δεδομένα ([60], σελ. 20), στην πραγματικότητα πολύ λιγότερα, καθώς τα Πιστοποιητικά αλλάζουν ή ανακαλούνται σχετικά σπάνια. Αναμένεται ότι όλες οι τερματικές συσκευές κατεβάζουν την λίστα κατά αραιά περιοδικά διαστήματα, π.χ. άπαξ ημερησίως με ρυθμό πολύ λίγα πιστοποιητικά χωρών κάθε φορά με μέγεθος της τάξης των ελαχίστων Kbytes. Σημειώνεται ότι οι τερματικές συσκευές επικοινωνούν μόνο με τους εθνικούς κόμβους, και σε καμία περίπτωση δεν επικοινωνούν απευθείας με την Κεντρική Ευρωπαϊκή Πύλη.

7.2 Κατανεμημένη Εμπιστοσύνη και τρίτες χώρες

Το σχέδιο πάνω στο οποίο βασίζεται το οικοσύστημα των Ευρωπαϊκών Πιστοποιητικών ακολουθεί τις ίδιες αρχές κατανεμημένης εμπιστοσύνης που προβλέπονται στις προτάσεις του ΠΟΥ και του ICAO. Αντί για μία μοναδική κεντρική αρχή εμπιστοσύνης σε παγκόσμιο επίπεδο, προβλέπει εγκαθίδρυση διμερών σχέσεων εμπιστοσύνης ανάμεσα στα κράτη. Σε τεχνικό επίπεδο κάθε κράτος δημοσιεύει σε ένα κεντρικό σημείο τα δημόσια κλειδιά από τις δικές του Αρχές Πιστοποίησης, και επαφίεται στα υπόλοιπα κράτη να υιοθετήσουν ή όχι την εμπιστοσύνη στη βάση συμφωνιών.

Η ΕΕ έχει δημοσιεύσει κείμενο οδηγιών προς όσα κράτη ενδιαφέρονται να κάνουν αμοιβαία αναγνώριση των αντίστοιχων Πιστοποιητικών των χωρών τους [63] και αυτά να συμπεριληφθούν στον κατάλογο έμπιστων Αρχών Έκδοσης Πιστοποιητικών που δημοσιεύεται στην Ευρωπαϊκή Πύλη DCCG. Μέχρι σήμερα (27/2/2022) 35 χώρες εκτός ΕΕ έχουν συνάψει με την ΕΕ συμφωνία αμοιβαίας αναγνώρισης των δικών τους Ψηφιακών Πιστοποιητικών [64].

8 Εφαρμογή αναφοράς για φορητές συσκευές Android

Το δίκτυο eHealth έχει δημοσιεύσει στο επίσημο αποθετήριο κώδικα της ΕΕ https://github.com/eu-digital-green-certificates [23], τις εφαρμογές αναφοράς και τα Application data που υλοποιούν τις λειτουργίες που προαναφέρθηκαν. Από αυτές επιλέχθηκε το project "dgca-verifier-app-android" για να δείξει πως ο ανοιχτός κώδικας δίνει τη δυνατότητα σε οποιαδήποτε χώρα να υλοποιήσει τις απαραίτητες υποδομές ελέγχου. Μαζί με αυτό έμμεσα χρησιμοποιήθηκαν και ως άμεσα dependencies τα " dgca-app-core-android" και "dgc-certlogic-android"

- https://github.com/eu-digital-green-certificates/dgca-verifier-app-android
- https://github.com/eu-digital-green-certificates/dgca-app-core-android
- https://github.com/eu-digital-green-certificates/dgc-certlogic-android

Το περιβάλλον μεταγλώττισης ήταν Android Studio 3.20.31. Εκτός από κάποιες επουσιώδεις αλλαγές στο περιβάλλον μεταγλώττισης χρειάστηκε να ρυθμιστεί η διασύνδεση με τους εθνικούς κόμβους διανομής πιστοποιητικών (DSG). Η εφαρμογή μεταγλωττίστηκε και μεταφορτώθηκε στο Google Play Store για τους σκοπούς αυτής της εργασίας με το όνομα "**mli18017**" [61] και να το εγκαταστήσει σε οποιαδήποτε σύγχρονη συσκευή Android. Έχουν τεθεί οι κατάλληλες σημάνσεις για τον εκπαιδευτικό σκοπό της ανάρτησης και γίνεται αναφορά στον πηγαίο κώδικα της ΕΕ. Η εφαρμογή έχει τις κατάλληλες προειδοποιήσεις προκειμένου να μη γίνει χρήση για ιατρικούς σκοπούς. Σημειωτέο ότι για τη δημόσια ανάρτηση εφαρμογής ελέγχου COVID-19 η πάροχος Google έχει ειδικούς όρους που προβλέπουν γραπτή έγκριση από κυβέρνηση ή κεντρική υπηρεσία κράτους και για συγκεκριμένο υγειονομικό σκοπό [62].

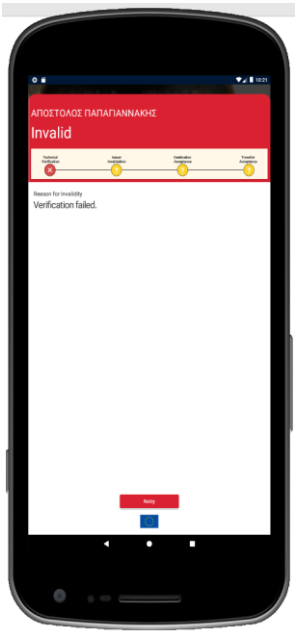
Εικόνα 10 - Εικονίδιο Εφαρμογής

8.1 Επιβεβαίωση εφαρμογής σε πραγματικά πιστοποιητικά

Η εφαρμογή ρυθμίστηκε να αναγνωρίζει μόνο επίσημα πιστοποιητικά της Ευρωπαϊκής Ένωσης, προκειμένου τα αποτελέσματα να μπορούν να συγκριθούν με αυτά από οποιαδήποτε επίσημη εφαρμογή Covid-19. Για να αποφευχθούν θέματα προσωπικών δεδομένων, οι έλεγχοι έγιναν με τα προσωπικά Ευρωπαϊκά πιστοποιητικά του γράφοντος

8.1.1 Παράδειγμα Μη έγκυρης Ηλεκτρονικής Υπογραφής

Στον παρακάτω πίνακα, η εφαρμογή αποκωδικοποιεί τα δεδομένα από το QR code και. απεικονίζει το Ονοματεπώνυμο, αλλά αδυνατεί να αναγνωρίσει την ηλεκτρονική υπογραφή του Πιστοποιητικού. Αυτό μπορεί να συμβαίνει είτε γιατί αυτός/ή που υπέγραψε το πιστοποιητικό δεν έχει διαπιστευμένο ηλεκτρονικό πιστοποιητικό υπογραφής είτε γιατί η εφαρμογή δεν έχει ενημερωθεί προσφάτως με την τρέχουσα λίστα των έγκυρων πιστοποιητικών υπογραφής. Η εφαρμογή χρειάζεται να επικοινωνεί με τους κόμβους διανομής πιστοποιητικών DSC κατά αραιές περιόδους π.χ. ανα 24 ώρες για να ενημερώνεται για την εγκυρότητα των ηλεκτρονικών υπογραφών των ατόμων ή φορέων υπογραφόντων.

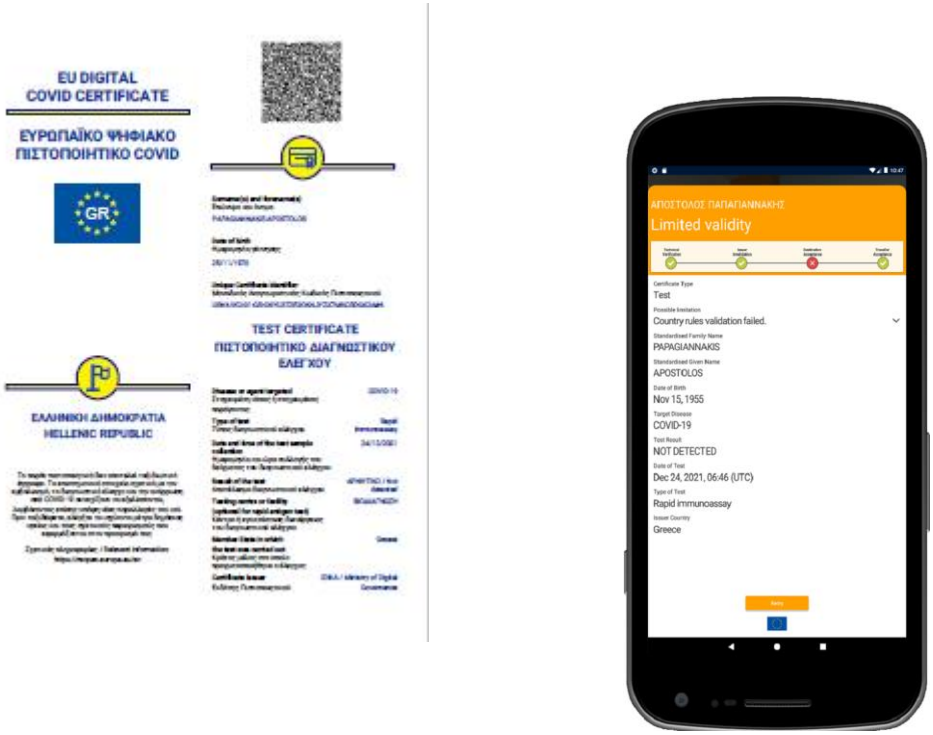


Εικόνα 11 – Μη αναγνώριση ηλεκτρονικής Υπογραφής

8.1.2 Παράδειγμα Μη έγκυρου πιστοποιητικού λόγω κανόνων χώρας

1. Στην επόμενη εικόνα ελέγχουμε ένα πιστοποιητικό Διαγνωστικού Ελέγχου (Rapid Immunoassay) το οποίο έχει τελεστεί σε παλαιότερο χρόνο, με βάση τους κανόνες

που ίσχυαν κατά το χρόνο ελέγχου (20 Ιαν 2022) για την είσοδο στη Γερμανία. Στην οθόνη φαίνεται ότι η εφαρμογή αναγνωρίζει την ηλεκτρονική υπογραφή του υπογράφοντος στο πιστοποιητικό, ως διαπιστευμένη αλλά η χώρα στην οποία ασκείται ο έλεγχος έχει κανόνες που δεν επιτρέπουν την αναγνώριση του συγκεκριμένου Πιστοποιητικού.



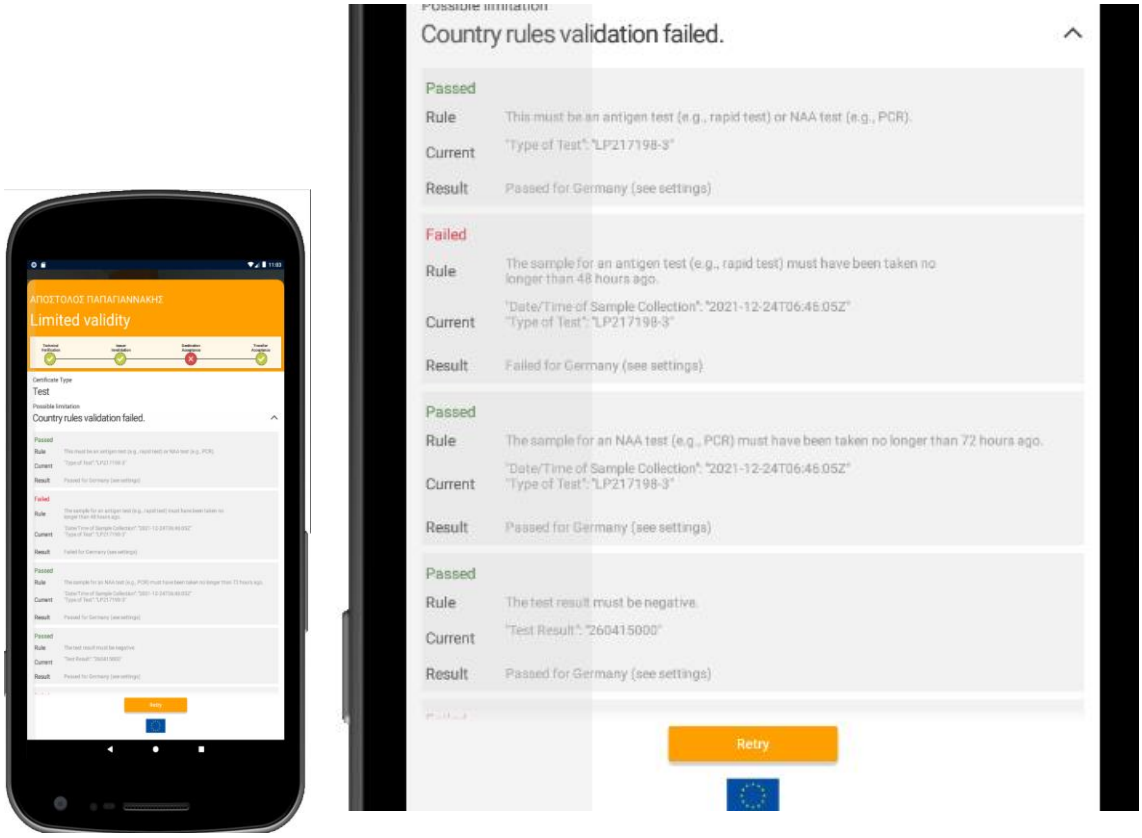
Εικόνα 12 – Πιστοποιητικό με περιορισμένη εγκυρότητα

Οι επιμέρους έλεγχοι όπως έχουν οριστεί για την χώρα της Γερμανίας είναι οι ακόλουθοι:

1. This must be an antigen test (e.g., rapid test) or NAA test (e.g., PCR).
2. The sample for an antigen test (e.g., rapid test) must have been taken no longer than 48 hours ago.
3. The sample for an NAA test (e.g., PCR) must have been taken no longer than 72 hours ago.
4. The test result must be negative

Στην επόμενη εικόνα φαίνονται φαίνεται η ακολουθία των κανόνων που πρέπει να ικανοποιούνται όλοι ταυτόχρονα, και με κόκκινο χρώμα επισημαίνεται ο έλεγχος που αποτυγχάνει και είναι ο "The sample for an antigen test (e.g., rapid test) must have been

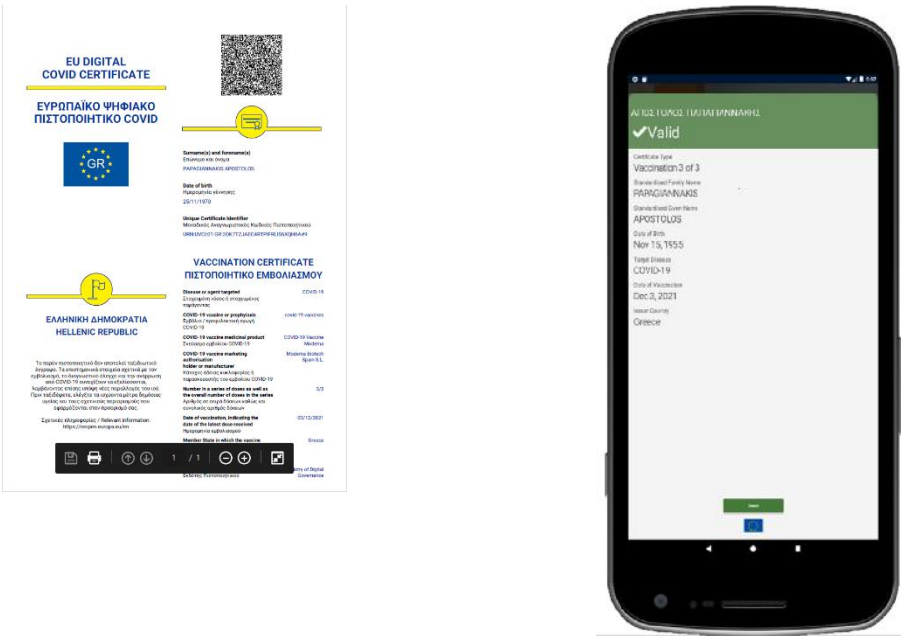
taken no longer than 48 hours ago". Οι κανόνες δημοσιεύονται ανά χώρα από τις αντίστοιχες υπηρεσίες CSCA, και όλες μαζί αναδημοσιεύονται στην Κεντρική Ευρωπαϊκή Πύλη DCCG. Ενδεικτικό σύνολο κανόνων είναι δημοσιευμένο από το δίκτυο eHealth [65] και παρατίθεται δείγμα στο Παράρτημα D.



Εικόνα 13 –Αναγνώριση ηλεκτρονικής Υπογραφής

8.1.3 Παράδειγμα Έγκυρου πιστοποιητικού

Παρακάτω φαίνεται το αποτέλεσμα που δίνει η εφαρμογή για ένα πιστοποιητικό που είναι έγκυρο και δεν έχει πρόβλημα με τους κανόνες επικύρωσης.



Εικόνα 14 –Έγκυρο Πιστοποιητικό σε Ισχύ

9 Επίλογος

9.1 Σύνοψη και συμπεράσματα

Συνήθως οι νόμοι έρχονται να ρυθμίσουν τις τεχνολογικές εξελίξεις εκ των υστέρων. Όμως στην περίπτωση των Ευρωπαϊκών Ψηφιακών Πιστοποιητικών COVID-19, οι κυβερνήσεις και οι νομοθέτες της ΕΕ κινητοποιήθηκαν με ταχύτητα και έφτιαξαν μαζί με την τεχνική κοινότητα ένα πολύ αποτελεσματικό εργαλείο περιορισμού των συνεπειών της πανδημίας. Διαβάζοντας το επίσημο νομικό κείμενο της Εκτελεστικής Απόφασης (ΕΕ) 2021/1073 [25] της Ευρωπαϊκής Επιτροπής, είδαμε ότι περιγράφει με σαφήνεια και απλότητα τις τεχνικές διαδικασίες και προδιαγραφές των Ψηφιακών Πιστοποιητικών, όπως αυτές δόθηκαν από το δίκτυο εμπειρογνωμόνων eHealth [21]. Αντίστροφα είδαμε τις τελευταίες εκδόσεις των τεχνικών κειμένων του δικτύου eHealth να παραπέμπουν πίσω στα νομικά κείμενα, αποδεικνύοντας ότι νόμοι και τεχνικά κείμενα και διαδικασίες αποτελούν ένα στενά συνδεδεμένο σύνολο [58]. Επίσης προσέξαμε ότι έχει καταβληθεί μεγάλη προσπάθεια για την ελαχιστοποίηση των δεδομένων και την συμμόρφωση με τον Γενικό Κανονισμό Προσωπικών Δεδομένων. Επίσης παρατηρήσαμε ότι χρησιμοποιήθηκαν παλαιές αλλά και νέες τεχνολογίες, οι οποίες όμως έχουν ήδη δοκιμαστεί επιτυχώς στο διαδίκτυο και το διαδίκτυο των πραγμάτων, και σχεδόν σε όλες τις περιπτώσεις έχουν αναχθεί σε διεθνή πρότυπα από αναγνωρισμένους φορείς προτυποποίησης και οργανισμούς(ISO , IETF, HL7, SNOMED κ.α.). Άξιο προσοχής είναι ότι οι επιμέρους κανόνες σχετικά με την εγκυρότητα των πιστοποιητικών, δεν είναι ενσωματωμένοι στα πιστοποιητικά, αλλά έχει προβλεφθεί η δυνατότητα κάθε χώρα να ορίζει και να δημοσιεύει τους δικούς της εκάστοτε επιθυμητούς κανόνες επικύρωσης των πιστοποιητικών. Αυτό γίνεται μέσα από τα ίδια έμπιστα κανάλια από τα οποία διανέμονται τα πιστοποιητικά των αρχών που εκδίδουν πιστοποιητικά, ανάλογα με τις εκάστοτε συνθήκες κι επιλογές των χωρών. Αυτό περιορίζει τις ανάγκες για ανακλήσεις πιστοποιητικών, και καθιστά δυνατές τις αλλαγές των εφαρμοζόμενων πολιτικών επικύρωσης ανάλογα με την εξέλιξη της πανδημίας.

Μέχρι τον Δεκέμβριο του 2021 είχαν εκδοθεί 807 εκατομμύρια πιστοποιητικά και χρησιμοποιούνταν σε 60 χώρες [36]. Πριν την εμφάνιση των ψηφιακών πιστοποιητικών η διακίνηση και ο έλεγχος τόσων εγγράφων θα θεωρούνταν αδύνατη. Μπορεί κανείς να πει ότι η νομοθετική διαδικασία πλέον αντιμετωπίζει με εμπιστοσύνη τα ηλεκτρονικά

έγγραφα, και πλέον σύνθετοι κανόνες και διαδικασίες που εφαρμόζονται με τεχνικά μέσα μπορούν να αποκτούν νομικό έρεισμα.

Το τελικό συμπέρασμα για τα Πιστοποιητικά COVID-19 είναι ότι η ταυτόχρονη προσέγγισή τους από τεχνολογική αλλά και από νομική σκοπιά, μεγιστοποίησε την αποδοχή τους από τους πολίτες των χωρών. Χάρις σε αυτή την αποδοχή περιορίστηκε σημαντικά η έκταση της ασθένειας και αποφεύχθηκε η πλήρης καθήλωση της Ευρωπαϊκής και της Παγκόσμιας Οικονομίας.

9.2 Όρια και περιορισμοί της έρευνας

Η εργασία αυτή εξετάζει σε περιορισμένο βάθος μόνο τα περιεχόμενα και το μορφότυπο του Ευρωπαϊκού Πιστοποιητικού με κάποιες εφαρμογές αναφοράς. Το σύνολο του οικοσυστήματος του Ευρωπαϊκού Πιστοποιητικού είναι πολύ ευρύτερο και περιλαμβάνει πλήθος οντοτήτων και λειτουργιών, όπως Ευρωπαϊκή Πύλη, Εθνικούς Κόμβους διανομής πιστοποιητικών, διεπαφές διασύνδεσης με τοπικά Ιατρικά πληροφοριακά συστήματα, κρυπτογραφική επικοινωνία με ταυτοποίηση και δεν είναι δυνατό να αναπαραχθούν στα πλαίσια μια εργασίας ειδίκευσης όπως η παρούσα. Πρέπει επίσης να αναφερθεί επίσης ότι οι δοκιμαστικές εφαρμογές που παρουσιάστηκαν δεν επικοινωνούν με τους παραγωγικούς εθνικούς κόμβους, αλλά με άλλους που περιέχουν αντίγραφα των δεδομένων τους. Συνεπώς δεν είναι δεδομένο το επίπεδο ενημέρωσής τους με τρέχουσες τιμές.

9.3 Μελλοντικές Επεκτάσεις

Μέχρι σήμερα οι άνθρωποι χρησιμοποιούσαν "χαρτιά", για να πιστοποιήσουν οποιοδήποτε γεγονός, π.χ. το όνομά τους, τις σπουδές τους, αλλά και κάθε συναλλαγή τους. Σε βάθος χρόνου πιστεύουμε ότι όλα αυτά θα αντικατασταθούν από ηλεκτρονικά έγγραφα-αρχεία. Καθώς όμως δεν έχουν όλοι οι άνθρωποι την ίδια πρόσβαση ή εξοικείωση με τα ψηφιακά εργαλεία, φαίνεται εύλογο κι αναμενόμενο ότι πολλά από αυτά τα "χαρτιά" θα συνεχίσουν να διακινούνται σε φυσικό χαρτί, αλλά πλέον θα αρχίσουν θα φέρουν το περιεχόμενό τους και τις ηλεκτρονικές υπογραφές τους και σε ραβδοκώδικα QR ή ισοδύναμο. Η τεχνολογία υπάρχει (signed QR codes), το πλαίσιο εμπιστοσύνης έχει ήδη σχηματιστεί (π.χ. νομοθεσία eIDAS), αυτό που μένει είναι να δούμε περισσότερη τυποποίηση στις συναλλαγές από τα κράτη και τον κόσμο του εμπορίου.

10 Βιβλιογραφία

[1] “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile” https://datatracker.ietf.org/doc/html/rfc5280 (accessed Feb. 06, 2022).

[2] Kövér, Ágnes. "The Relationship between Government and Civil Society in the Era of COVID-19" Nonprofit Policy Forum, vol. 12, no. 1, 2021, pp. 1-24. https://doi.org/10.1515/npf-2021-0007

[3] “J. J. Lee and J. P. Haupt, “Scientific globalism during a global crisis: research collaboration and open access publications on COVID-19” High Educ, vol. 81, no. 5, pp. 949–966, May 2021, doi: 10.1007/s10734-020-00589-0.

[4] L. Fransen, J. Nkengason, S. Srinivas, and S. Vella, “Boosting equitable access and production of diagnostics, therapeutics and vaccines to confront covid-19 on a global footing,” p. 17.

[5] “COVAX.” https://www.who.int/initiatives/act-accelerator/covax (accessed Feb. 06, 2022).

[6] “COVID-19 Vaccine Market Dashboard | UNICEF Supply Division.” https://www.unicef.org/supply/covid-19-vaccine-market-dashboard (accessed Feb. 06, 2022).

[7] “Rapid, point-of-care antigen and molecular-based tests for diagnosis of SARS-CoV-2 infection - Dinnes, J - 2021 | Cochrane Library.” https://www.cochranelibrary.com/cdsr/doi/10.1002/14651858.CD013705.pub2/full (accessed Feb. 06, 2022).

[8] S. Hsiang et al., “The effect of large-scale anti-contagion policies on the COVID-19 pandemic,” Nature, vol. 584, no. 7820, pp. 262–267, Aug. 2020, doi: 10.1038/s41586-020-2404-8.

[9] G. Karopoulos, J. L. Hernandez-Ramos, V. Kouliaridis, and G. Kambourakis, “A Survey on Digital Certificates Approaches for the COVID-19 Pandemic,” IEEE Access, vol. 9, pp. 138003–138025, 2021, doi: 10.1109/ACCESS.2021.3117781.

[10] Fourth World Health Assembly, 1952, International Sanitary Regulations (1951). Geneva: World Health Organization

[11] Sixty-Seventh World Health Assembly, 2014, International health regulations (2005), Geneva: World Health Organization, Annex VI

[12] Digital Documentation of COVID-19 Certificates: Vaccination Status — Technical Specifications and Implementation Guidance, 27 August 2021. Geneva: World Health Organization; 2021 (WHO/2019-nCoV/Digital_certificates/vaccination/2021.1).

[13] N. Ratanaprayul, “Digital Documentation of COVID-19 Certificates: Vaccination Status,” p. 11.

[14] “Interim guidance for developing a Smart Vaccination Certificate.” https://www.who.int/publications/m/item/interim-guidance-for-developing-a-smart-vaccination-certificate (accessed Feb. 06, 2022).

[15] “FHIR v4.0.1.” http://hl7.org/fhir/ (accessed Feb. 06, 2022).

[16] “Health Level Seven International - Homepage | HL7 International.” http://www.hl7.org/ (accessed Feb. 06, 2022).

[17] “ICD-10 International Classification of Diseases 10th Revision”, https://icd.who.int/browse10/2010/en (accessed Feb. 06, 2022).

[18] “ICD-11 International Classification of Diseases 11th Revision”, https://icd.who.int/en (accessed Feb. 06, 2022).

[19] “SNOMED-CT”, https://www.snomed.org/snomed-ct/five-step-briefing (accessed Feb. 06, 2022).

[20] “eHealth : Digital health and care.” https://ec.europa.eu/health/ehealth-digital-health-and-care_en (accessed Feb. 06, 2022).

[21] “eHealth and COVID-19.” https://ec.europa.eu/health/ehealth-digital-health-and-care/ehealth-and-covid-19_en (accessed Feb. 26, 2022).

[22] “eHealth Network, Guidelines on verifiable vaccination certificates - basic interoperability elements, Release 2, 2021-03-12”, (accessed Feb. 06, 2022).

[23] “eu-digital-green-certificates · GitHub.” https://github.com/eu-digital-green-certificates (accessed Feb. 06, 2022).

[24] “European eHealth network - Digital Covid Certificate · GitHub.” https://github.com/ehn-dcc-development (accessed Feb. 06, 2022).

[25] “ΕΚΤΕΛΕΣΤΙΚΗ ΑΠΟΦΑΣΗ (ΕΕ) 2021/1073 ΤΗΣ ΕΠΙΤΡΟΠΗΣ της 28ης Ιουνίου 2021”, https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32021D1073&from=EL(accessed Feb. 06, 2022).

[26] “ΕΚΤΕΛΕΣΤΙΚΗ ΑΠΟΦΑΣΗ (ΕΕ) 2021/2014 ΤΗΣ ΕΠΙΤΡΟΠΗΣ της 17ης Νοεμβρίου 2021”, https://eur-lex.europa.eu/legal-content/EL/TXT/PDF/?uri=CELEX:32021D2014&from=EN (accessed Feb. 06, 2022).

[27] “ΕΚΤΕΛΕΣΤΙΚΗ ΑΠΟΦΑΣΗ (ΕΕ) 2021/2301 ΤΗΣ ΕΠΙΤΡΟΠΗΣ της της 21ης Δεκεμβρίου 2021”, https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32021D2301&from=EL (accessed Feb. 07, 2022).

[28] “eHealth Network, Guidelines on Technical Specifications for Digital Green Certificates, Volume 1, V1.0.5, 2021-04-21”, (accessed Feb. 06, 2022).

[29] “Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification”, ISO/IEC 18004:2015(en)

[30] “eHealth Network, Guidelines on Value Sets for EU Digital COVID-19, Version 1.8, 2022-01-26" https://ec.europa.eu/health/system/files/2022-01/EU DCC-value-sets_en_0.pdf, (accessed Feb. 06, 2022).

[31] “eHealth Network, Guidelines on COVID-19 citizen recovery interoperable certificates - minimum dataset, Release 1, 2021-03-15”, (accessed Feb. 06, 2022).

[32] “EU health preparedness: A common list of COVID-19 rapid antigen tests; A common standardised set of data to be included in COVID-19 test result certificates; and a common list of COVID-19 laboratory based antigenic assays”, Health Security Committee, 2022-01-22 (accessed Feb. 06, 2022).

[33] “eHealth Network, OUTLINE, Interoperability of health certificates Trust framework, V.1.0,, 2021-03-12”, (accessed Feb. 07, 2022).

[34] “eHealth Network, Guidelines on Technical Specifications for EU Digital COVID-19 Certificates, JSON Schema Specification, Schema version: 1.3.0, 2021-06-09”, https://ec.europa.eu/health/system/files/2021-06/covid-certificate_json_specification_en_0.pdf, (accessed Feb. 07, 2022).

[35] “eHealth Network, EU DCC Validation Rules, V1.00, 2021-06-09”, (accessed Feb. 07, 2022).

[36] “Press corner | European Commission.” https://ec.europa.eu/commission/presscorner/detail/en/ip_21_6837 (accessed Feb. 09, 2022).

[37] “Doc 9303” https://www.icao.int/publications/pages/publication.aspx?docnum=9303 (accessed Feb. 10, 2022).

[38] “SNOMED - 5-Step Briefing.” https://www.snomed.org/snomed-ct/five-step-briefing (accessed Feb. 14, 2022).

[39] “RFC 7159 - The JavaScript Object Notation (JSON) Data Interchange Format.” https://datatracker.ietf.org/doc/html/rfc7159 (accessed Feb. 15, 2022).

[40] “ISO - ISO 8601 — Date and time format.” https://www.iso.org/iso-8601-date-and-time-format.html (accessed Feb. 20, 2022).

[41] “RFC 7049 - Concise Binary Object Representation (CBOR).” https://datatracker.ietf.org/doc/html/rfc7049 (accessed Feb. 27, 2022).

[42] “RFC 8152 - CBOR Object Signing and Encryption (COSE).” https://datatracker.ietf.org/doc/html/rfc8152 (accessed Feb. 27, 2022).

[43] “RFC 8392 - CBOR Web Token (CWT).” https://datatracker.ietf.org/doc/html/rfc8392 (accessed Feb. 27, 2022).

[44] “RFC 1950 - ZLIB Compressed Data Format Specification version 3.3.” https://datatracker.ietf.org/doc/html/rfc1950 (accessed Feb. 27, 2022).

[45] “RFC 1951 - DEFLATE Compressed Data Format Specification version 1.3.” https://datatracker.ietf.org/doc/html/rfc1951 (accessed Feb. 27, 2022).

[46] “draft-faltstrom-base45-04.” https://datatracker.ietf.org/doc/html/draft-faltstrom-base45-04 (accessed Feb. 27, 2022).

[47] “JsonLogic.” https://jsonlogic.com/ (accessed Feb. 27, 2022).

[48] “eHealth Network Guidelines on Paper version of the EU Digital COVID Certificate V1.0.2 2021-05-26” https://ec.europa.eu/health/system/files/2021-05/covid-certificate_paper_guidelines_en_0.pdf (accessed Feb. 27, 2022).

[49] “GitHub - eu-digital-green-certificates/dgca-verifier-app-android: Repository for the dgca verifier android app.” https://github.com/eu-digital-green-certificates/dgca-verifier-app-android (accessed Feb. 27, 2022).

[50] “GitHub - ehn-dcc-development/ehn-sign-verify-python-trivial: Extremely minimal python implementation of the eHN-S protocol.” https://github.com/ehn-dcc-development/ehn-sign-verify-python-trivial (accessed Feb. 27, 2022).

[51] “ZBar bar code reader.” http://zbar.sourceforge.net/ (accessed Feb. 27, 2022).

[52] “Ubuntu 21.10 | Ubuntu.” https://ubuntu.com/blog/tag/ubuntu-21-10 (accessed Feb. 27, 2022).

[53] “sed(1) - Linux man page.” https://linux.die.net/man/1/sed (accessed Feb. 27, 2022).

[54] “pigz - Parallel gzip.” https://zlib.net/pigz/ (accessed Feb. 27, 2022).

[55] “ISO - ISO 3166 — Country Codes.” https://www.iso.org/iso-3166-country-codes.html (accessed Feb. 27, 2022).

[56] “RFC 8141 - Uniform Resource Names (URNs).” https://datatracker.ietf.org/doc/html/rfc8141 (accessed Feb. 27, 2022).

[57] ISO/IEC 7812-1:2017(en) Identification cards — Identification of issuers — Part 1: Numbering system, https://www.iso.org/obp/ui/ (Accessed Feb. 27, 2022).

[58] “eHealth Network, Guidelines on Technical Specifications for EU Digital COVID Certificates, Volume 1, V1.1.1, 2022-02-23” https://ec.europa.eu/health/system/files/2022-02/digital-covid-certificates_v1_en.pdf (accessed Feb. 27, 2022).

[59] “ΚΑΝΟΝΙΣΜΌΣ (ΕΕ) αριθ. 910/2014 ΤΟΥ ΕΥΡΩΠΑΪΚΟΎ ΚΟΙΝΟΒΟΥΛΊΟΥ ΚΑΙ ΤΟΥ ΣΥΜΒΟΥΛΊΟΥ της 23ης Ιουλίου 2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ” https://eur-lex.europa.eu/legal-content/EL/TXT/HTML/?uri=CELEX:32014R0910&from=EN (accessed Feb. 27, 2022).

[60] “eHealth Network, Guidelines on Technical Specifications for EU Digital COVID Certificates, Volume 4, EU Digital COVID Certificate Applications, Version 1.4, 2022-02-23” https://ec.europa.eu/health/system/files/2022-02/digital-covid-certificates_v4_en_0.pdf (accessed Feb. 27, 2022).

[61] “mli18017 - Apps on Google Play.” https://play.google.com/store/apps/details?id=gr.uom.mli18017 (accessed Feb. 27, 2022).

[62] “Απαιτήσεις για εφαρμογές που σχετίζονται με τον κορονοϊό 2019 (COVID-19)” https://support.google.com/googleplay/android-developer/answer/9889712?hl=el#app_requirements (accessed Feb. 27, 2022).

[63] “Third Country EU Digital COVID certificate Equivalence Decision procedure, Version 1.0”, https://ec.europa.eu/health/system/files/2021-07/covid-certificate_equivalence-decision_en_0.pdf (accessed Feb. 27, 2022).

[64] “Commission Implementing Decisions (EU) on the equivalence of COVID-19 certificates issued by non-EU countries”, https://ec.europa.eu/info/publications/commission-implementing-decisions-eu-equivalence-covid-19-certificates-issued-non-eu-countries_el (accessed Feb. 27, 2022).

[65] “Digital COVID Certificates: Business Rules testdata”, https://github.com/eu-digital-green-certificates/dgc-business-rules-testdata (accessed Feb. 27, 2022).

[66] “Semantic Versioning 2.0.0”, https://semver.org/ (accessed Feb. 27, 2022).

[67] “Digital Covid Certificate Schema", https://github.com/ehn-dcc-development/ehn-dcc-schema/blob/release/1.3.0/valuesets/test-type.json (accessed Feb. 27, 2022).

[68] “Uniform Resource Identifier (URI): Generic Syntax”, https://datatracker.ietf.org/doc/html/rfc3986 (accessed Feb. 27, 2022).

[69] “strings(1) — Linux manual page”, https://man7.org/linux/man-pages/man1/strings.1.html (accessed Feb. 27, 2022).

Παράρτημα Α - Δείγματα πιστοποιητικών

Α.1 Προηγούμενη νόσηση


```
{
  "ver": "1.2.1",
  "nam": {
    "fn": "Παπαγιαννάκης",
    "gn": "Απόστολος-Μανούσος",
    "fnt": "PAPAGIANNAKIS",
    "gnt": "APOSTOLOS<MANOUSOS"
  },
  "dob": "1995-10-28",
  "r": [
    {
      "tg": "840539006",
      "fr": "2021-03-10",
      "co": "GR",
      "is": "IDIKA / Ministry of Digital Governance",
      "df": "2021-06-16",
      "du": "2021-12-16",
      "ci": "URN:UVCI:01:GR:URN:UVCI:01:GR:12345678901234567890123456789:/#6"
    }
  ]
}
```

A.2 **Εμβολιασμός**


```
{
  "ver": "1.2.1",
  "nam": {
    "fn": "Παπαγιαννάκης",
    "gn": "Απόστολος-Μανούσος",
    "fnt": "PAPAGIANNAKIS",
    "gnt": "APOSTOLOS<MANOUSOS"
  },
  "dob": "1940-10-28",
  "v": [
    {
      "tg": "840539006",
      "vp": "1119349007",
      "mp": "EU\/1\/20\/1528",
      "ma": "ORG-100030215",
      "dn": 1,
      "sd": 2,
      "dt": "2021-02-18",
      "co": "GR",
      "is": "IDIKA / Ministry of Digital Governance",
      "ci": "URN:UVCI:01:GR:URN:UVCI:01:GR:123456789012345678901234567 89:/#6"
    }
  ]
}
```

A.3 Διαγνωστικός έλεγχος αντιγόνου


```
{
  "ver": "1.2.1",
  "nam": {
    "fn": "Παπαγιαννάκης",
    "gn": "Απόστολος-Μανούσος",
    "fnt": "PAPAGIANNAKIS",
    "gnt": "APOSTOLOS<MANOUSOS"
  },
  "dob": "1995-10-28",
  "t": [
    {
      "tg": "840539006",
      "tt": "LP217198-3",
      "ma": "1232",
      "sc": "2021-03-10T12:34:56+00:00",
      "tr": "260415000",
      "tc": "Testing center Vienna 1",
      "co": "GR",
      "is": "IDIKA / Ministry of Digital Governance",
      "ci": "URN:UVCI:01:GR:URN:UVCI:01:GR:12345678901234567890123456789:/#6"
    }
  ]
}
```

A.4 Μοριακός Διαγνωστικός Έλεγχος


```
{
  "ver": "1.2.1",
  "nam": {
    "fn": "Παπαγιαννάκης",
    "gn": "Απόστολος-Μανούσος",
    "fnt": "PAPAGIANNAKIS",
    "gnt": "APOSTOLOS<MANOUSOS"
  },
  "dob": "1995-10-28",
  "t": [
    {
      "tg": "840539006",
      "tt": "LP6464-4",
      "nm": "Roche LightCycler qPCR",
      "sc": "2021-03-10T12:34:56+00:00",
      "tr": "260415000",
      "tc": "Testing center Vienna 1",
      "co": "GR",
      "is": "IDIKA / Ministry of Digital Governance",
      "ci": "URN:UVCI:01:GR:URN:UVCI:01:GR:12345678901234567890123456789:/#6"
    }
  ]
}
```

Παράρτημα Β - Δυαδική Κωδικοποίηση Πιστοποιητικού

Τα παρακάτω έχουν συντεθεί με τη βοήθεια της υπηρεσίας https://github.com/ehn-dcc-development/hcert-service-kotlin (https://dgc.a-sit.at/ehn/)

B.1 **Input**


```
{ "ver": "1.2.1", "nam": { "fn": "Παπαγιαννάκης", "gn": "Απόστολος-Μανούσος", "fnt": "PAPAGIANNAKIS", "gnt": "APOSTOLOS<MANOUSOS" }, "dob": "1995-10-28", "r": [ { "tg": "840539006", "fr": "2021-03-10", "co": "GR", "is": "IDIKA / Ministry of Digital Governance", "df": "2021-06-16", "du": "2021-12-16", "ci": "URN:UVCI:01:GR:1234567890123456789012345678 90#6" } ] }
```


B.2 **CBOR (Hex) (614 chars):**


```
bf6376657265312e322e31636e616dbf62666e781acea0ceb1cf80ceb1ceb3ceb9ceb1c
ebdcebdceaccebaceb7cf8263666e746d504150414749414e4e414b495362676e7823ce
91cf80cf8ccf83cf84cebfcebbcebfcf822dce9cceb1cebdcebfcf8dcf83cebfcf82636
76e747241504f53544f4c4f533c4d414e4f55534f53ff63646f626a313939352d31302d
323861729fbf6274676938343035333930303662667 26a323032312d30332d313062636
f624752626973782649444 94b41202f204d696e6973747279206f66204469676974616c
20476f7665726e616e63656264666a323032312d30362d31366264756a323032312d313
22d3136626369782f55524e3a555643493a30313a47523a313233343536373839303132
333435363738393031323334353637383930233 6ffffff
```


B.3 **CWT (Hex) (650 chars):**


```
a401624154041a63e58390061a62045010390103a101a4617281a7626369782f55524e3
a555643493a30313a47523a313233343536373839303132333435363738393031323334
353637383930233662636f6247526264666a323032312d30362d31366264756a3230323
12d31322d31366266726a323032312d30332d313062697378264944494b41202f204d69
6e6973747279206f66204469676974616c20476f7665726e616e6365627467693834303
533393030366364 6f626a313939352d31302d3238636e616da462666e781acea0ceb1cf
80ceb1ceb3ceb9ceb1cebdcebdceaccebaceb7cf8262676e7823ce91cf80cf8ccf83cf8
4cebfcebbcebfcf822dce9cceb1cebdcebfcf8dcf83cebfcf8263666e746d5041504147
49414e4e414b495363676e747241504f53544f4c4f533c4d414e4f55534f53637665726
5312e322e31
```

B.4 **COSE (Hex) (822 chars):**

```
d2844da201260448d919375fc1e7b6b2a0590145a401624154041a63e58390061a62045
010390103a101a4617281a7626369782f55524e3a555643493a30313a47523a31323334
353637383930313233343536373839303132333435363738393023662636f624752626
4666a323032312d30362d31366264756a323032312d31322d31366266726a323032312d
30332d313062697378264944494b41202f204d696e6973747279206f662044696769746
16c20476f7665726e616e6365627467693834303533393030366364 6f626a313939352d
31302d3238636e616da462666e781acea0ceb1cf80ceb1ceb3ceb9ceb1cebdcebdceacc
ebaceb7cf8262676e7823ce91cf80cf8ccf83cf84cebfcebbcebfcf822dce9cceb1cebd
cebfcf8dcf83cebfcf8263666e746d504150414749414e4e414b495363676e747241504
f53544f4c4f533c4d414e4f55534f536376657265312e322e315840134aade6477cca99
ee24cf2ce69c73ea3991c7fe08715d398432bcfe16167c9486524499fe1f45a327c9af2
750dee556ece9d8bdecdb145232e821155f072d47
```

B.5 **Compressed COSE (Base45) (584 chars):**

```
NCFOXN%TSMAHN-H3ZSUZK+.V0ET9%6-AH:VE1ROR$SIOOB/IV
M$E0CSANO909GNO4*J8OX4UZ85XPWLI2P53O8J.V
J8$XJK*L5R1L*RYXLB+HXY9Y0Q:V5*W1AKML:P:PI7VIMSG7LAXPMHQ1*P1MX19UEL:P6IA
394.L8322G*LAG5*ZL%9D.XI/VBS8T*US02U5EKYHSYIJGDBGIASJLA8KPHS-
IJPEBFDJ$HSZ3CDKBI7JM7J/MJ4OIMEDTJCJKDLEDL9CWZJ$7K+
CUED2D1.P8ODPEA7IB65C94JBF-GPHNFATE1KT77-
PU06TNN77*S444UQEACRI3U1UJ3UQAH5E9QDV7HBE+BT.$U+0JN$VT:TXBNVXF38UIB78-
E4DQE1KFY0NS431T9$SW37W771QFYWV:B7*OFQ05KCT2P2T*0$.0JLV0GVH
RNK7OOVW*0V+06J0V0J1DLCZKO63D7470N6IJ::PWKJKWAAXTSSJ4/VPNE%NUBR3CKMPW5H
UFJHHJ/QQCD.LEDNVO5SMMM-NPAQTUDVN1H2GFNSCTVJ*E4C*8EP29 SN+E770FRDF0
```

B.6 **Prefixed Compressed COSE (Base45) (588 chars):**

```
HC1:NCFOXN%TSMAHN-H3ZSUZK+.V0ET9%6-AH:VE1ROR$SIOOB/IV
M$E0CSANO909GNO4*J8OX4UZ85XPWLI2P53O8J.V
J8$XJK*L5R1L*RYXLB+HXY9Y0Q:V5*W1AKML:P:PI7VIMSG7LAXPMHQ1*P1MX19UEL:P6IA
394.L8322G*LAG5*ZL%9D.XI/VBS8T*US02U5EKYHSYIJGDBGIASJLA8KPHS-
IJPEBFDJ$HSZ3CDKBI7JM7J/MJ4OIMEDTJCJKDLEDL9CWZJ$7K+
CUED2D1.P8ODPEA7IB65C94JBF-GPHNFATE1KT77-
PU06TNN77*S444UQEACRI3U1UJ3UQAH5E9QDV7HBE+BT.$U+0JN$VT:TXBNVXF38UIB78-
E4DQE1KFY0NS431T9$SW37W771QFYWV:B7*OFQ05KCT2P2T*0$.0JLV0GVH
RNK7OOVW*0V+06J0V0J1DLCZKO63D7470N6IJ::PWKJKWAAXTSSJ4/VPNE%NUBR3CKMPW5H
UFJHHJ/QQCD.LEDNVO5SMMM-NPAQTUDVN1H2GFNSCTVJ*E4C*8EP29 SN+E770FRDF0
```

B.7 **QR Code**

Παράρτημα C - Δείγματα πιστοποιητικών X.509

C.1 Πιστοποιητικό υπογράφοντος:

```
Data:
    Version: 3 (0x2)
    Serial Number:
        01:79:3c:8b:cf:0e:95:e2:ec:b9
    Signature Algorithm: ecdsa-with-SHA256
    Issuer: CN = AT DGC CSCA 1, C = AT, O = BMSGPK
    Validity
        Not Before: May  5 12:41:06 2021 GMT
        Not After : May  5 12:41:06 2023 GMT
    Subject: CN = AT DSC 1, C = AT, O = BMSGPK, serialNumber = 1
    Subject Public Key Info:
        Public Key Algorithm: id-ecPublicKey
            Public-Key: (256 bit)
            pub:
                04:ad:d5:5c:f5:ad:1b:96:d4:7a:8e:6d:41:3d:30:
                37:bb:47:32:24:d6:0a:b8:5d:6e:46:4f:21:ee:1d:
                38:f9:70:51:27:d9:18:1e:df:bf:a1:20:d7:c2:65:
                97:28:ce:9c:10:29:dc:9a:a6:8a:cf:50:fd:53:13:
                b5:16:97:41:77
            ASN1 OID: prime256v1
```

```
                NIST CURVE: P-256

        X509v3 extensions:

            X509v3 Key Usage: critical

                Digital Signature

            X509v3 Subject Key Identifier:

EE:3D:CB:52:12:6F:A7:2F:5E:C8:4B:72:9F:14:52:9F:55:A0:62:D0

            X509v3 Authority Key Identifier:

keyid:FE:C9:28:43:9F:94:61:2F:79:FD:A2:31:DB:68:A6:C7:AD:C0:61:9E


    Signature Algorithm: ecdsa-with-SHA256

         30:45:02:21:00:c6:da:8a:68:b5:61:bc:b4:95:cd:f3:86:59:

         a9:3e:b0:50:1c:fd:28:5f:03:fb:3f:4d:ba:46:2f:9d:41:10:

         dd:02:20:74:12:c5:49:34:a2:0e:dd:14:25:a0:c5:e9:2b:76:

         6e:45:10:b9:51:d6:e9:f4:1b:38:d7:7b:df:5f:cc:e2:77

-----BEGIN CERTIFICATE-----

MIIBvTCCAWOgAwIBAgIKAXk8i88OleLsuTAKBggqhkjOPQQDAjA2MRYwFAYDVQQD

DA1BVCBER0MgQ1NDQSAxMQswCQYDVQQGEwJBVDEPMA0GA1UECgwGQk1TR1BLMB4X

DTIxMDUwNTEyNDEwNloXDTIzMDUwNTEyNDEwNlowPTERMA8GA1UEAwwIQVQgRFND

IDExCzAJBgNVBAYTAkFUMQ8wDQYDVQQKDAZCTVNHUEsxCjAIBgNVBAUTATEwWTAT

BgcqhkjOPQIBBggqhkjOPQMBBwNCAASt1Vz1rRuW1HqObUE9MDe7RzIk1gq4XW5G

TyHuHTj5cFEn2Rge37+hINfCZZcozpwQKdyaporPUP1TE7UWl0F3o1IwUDAOBgNV
```

```
HQ8BAf8EBAMCB4AwHQYDVR0OBBYEFO49y1ISb6cvXshLcp8UUp9VoGLQMB8GA1Ud

IwQYMBaAFP7JKEOflGEvef2iMdtopsetwGGeMAoGCCqGSM49BAMCA0gAMEUCIQDG

2opotWG8tJXN84ZZqT6wUBz9KF8D+z9NukYvnUEQ3QIgdBLFSTSiDt0UJaDF6St2

bkUQuVHW6fQbONd731/M4nc=

-----END CERTIFICATE-----
```

C.2 Πιστοποιητικό Εθνικού κόμβου

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 3270579603 (0xc2f11593)
        Signature Algorithm: ecdsa-with-SHA256
        Issuer: CN = EC-Me
        Validity
            Not Before: Apr 23 11:27:48 2021 GMT
            Not After : May 23 11:27:48 2021 GMT
        Subject: CN = EC-Me
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:fc:e5:79:51:f6:2b:b4:4d:78:d3:3b:45:f6:33:
                    a0:9e:ec:75:a3:23:4e:f0:1b:2c:e3:7e:fb:13:f9:
                    03:86:9f:44:cc:56:5d:b2:06:b3:b5:f4:fe:c2:f0:
                    36:f5:be:eb:49:bd:84:b0:72:6b:af:c6:90:76:7d:
                    ff:d7:29:ed:7b
                ASN1 OID: prime256v1
                NIST CURVE: P-256
```

```
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
    Signature Algorithm: ecdsa-with-SHA256
         30:46:02:21:00:b9:d5:7c:2c:b6:32:01:1f:5d:12:37:bd:35:
         12:7c:56:18:ad:e0:22:03:da:52:00:4d:fa:58:d9:02:ce:fa:
         cd:02:21:00:e0:ea:e1:32:76:a8:03:e9:15:cd:45:21:43:af:
         be:5c:9c:18:9e:90:57:13:57:12:48:51:72:07:65:55:f5:1b
-----BEGIN CERTIFICATE-----
MIIBJTCBy6ADAgECAgUAwvEVkzAKBggqhkjOPQQDAjAQMQ4wDAYDVQQDDAVFQy1N
ZTAeFw0yMTA0MjMxMTI3NDhaFw0yMTA1MjMxMTI3NDhaMBAxDjAMBgNVBAMMBUVD
LU1lMFkwEwYHKoZIzj0CAQYIKoZIzj0DAQcDQgAE/OV5UfYrtE140ztF9jOgnux1
oyNO8Bss4377E/kDhp9EzFZdsgaztfT+wvA29b7rSb2EsHJrr8aQdn3/1ynte6MS
MBAwDgYDVR0PAQH/BAQDAgWgMAoGCCqGSM49BAMCA0kAMEYCIQC51XwstjIBH10S
N701EnxWGK3gIgPaUgBN+ljZAs76zQIhAODq4TJ2qAPpFc1FIUOvvlycGJ6QVxNX
EkhRcgdlVfUb
-----END CERTIFICATE-----
```

Παράρτημα D - Δείγμα Γερμανικού κανόνα επικύρωσης Διαγνωστικού ελέγχου Αντιγόνου (rapid test)


```
{
  "Identifier": "TR-DE-0002",
  "Type": "Acceptance",
  "Country": "DE",
  "Version": "1.0.0",
  "SchemaVersion": "1.0.0",
  "Engine": "CERTLOGIC",
  "EngineVersion": "0.7.5",
  "CertificateType": "Test",
  "Description": [
    {
      "lang": "en",
      "desc": "The sample for an antigen test (e.g., rapid test) must have been taken no longer than 48 hours ago."
    },
    {
      "lang": "de",
      "desc": "Die Probenahme für einen Antigen-Test (z.B. Schnelltest) darf maximal 48 Stunden zurückliegen."
    },
    {
      "lang": "fr",
      "desc": "Le prélèvement pour un test antigénique (p. ex. test rapide) ne doit pas dater de plus de 48 heures."
    },
    {
```

```
            "lang": "es",

            "desc": "Deben haber transcurrido 48 horas como máximo
desde la extracción para una prueba de antígenos (por ejemplo, un
autotest rápido)."

          },

          {

            "lang": "it",

            "desc": "Il campione per il test antigenico (test rapido)
deve essere stato rilevato nelle ultime 48 ore."

          }

        ],

        "ValidFrom": "2021-07-03T00:00:00Z",

        "ValidTo": "2030-06-01T00:00:00Z",

        "AffectedFields": [

          "t.0",

          "t.0.sc",

          "t.0.tt"

        ],

        "Logic": {

          "if": [

            {

              "var": "payload.t.0"

            },

            {

              "if": [

                {

                  "===": [

                    {

                      "var": "payload.t.0.tt"
```

```
    },
    "LP217198-3"
  ]
},
{
  "not-after": [
    {
      "plusTime": [
        {
          "var": "external.validationClock"
        },
        0,
        "day"
      ]
    },
    {
      "plusTime": [
        {
          "var": "payload.t.0.sc"
        },
        48,
        "hour"
      ]
    }
  ]
},
true
```

```
                ]
            },
            true
        ]
    }
}
```