ΕΚΤΕΛΕΣΤΙΚΗ ΑΠΟΦΑΣΗ (ΕΕ) 2021/1073 ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 28ης Ιουνίου 2021

σχετικά με τον καθορισμό τεχνικών προδιαγραφών και κανόνων για την εφαρμογή του πλαισίου εμπιστοσύνης για το Ψηφιακό Πιστοποιητικό COVID της ΕΕ που θεσπίστηκε με τον κανονισμό (ΕΕ) 2021/953 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη τον κανονισμό (ΕΕ) 2021/953 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με πλαίσιο για την έκδοση, την επαλήθευση και την αποδοχή διαλειτουργικών πιστοποιητικών εμβολιασμού κατά της COVID-19, διαγνωστικού της ελέγχου και ανάρρωσης από αυτή (Ψηφιακό Πιστοποιητικό COVID της ΕΕ) με σκοπό να διευκολυνθεί η ελεύθερη κυκλοφορία κατά τη διάρκεια της πανδημίας της COVID-19 ([1]), και ιδίως το άρθρο 9 παράγραφοι 1 και 3,

Εκτιμώντας τα ακόλουθα:

(1) Ο κανονισμός (ΕΕ) 2021/953 προβλέπει τη δημιουργία του Ψηφιακού Πιστοποιητικού COVID της ΕΕ, σκοπός του οποίου είναι να αποδεικνύει ότι ένα άτομο έχει εμβολιαστεί κατά της COVID-19, έχει υποβληθεί πρόσφατα σε έλεγχο με αρνητικό αποτέλεσμα ή έχει αναρρώσει από τη λοίμωξη.

(2) Προκειμένου η επιχειρησιακή εφαρμογή του Ψηφιακού Πιστοποιητικού COVID της ΕΕ να είναι εφικτή σε ολόκληρη την Ένωση, είναι αναγκαίο να καθοριστούν τεχνικές προδιαγραφές και κανόνες για τη συμπλήρωση, την ασφαλή έκδοση και επαλήθευση των ψηφιακών πιστοποιητικών COVID, τη διασφάλιση της προστασίας δεδομένων προσωπικού χαρακτήρα, τον καθορισμό της κοινής δομής του μοναδικού αναγνωριστικού κωδικού πιστοποιητικού, και την έκδοση έγκυρου, ασφαλούς και διαλειτουργικού ραβδοκώδικα. Το πλαίσιο εμπιστοσύνης θέτει επίσης τις βάσεις για τη διασφάλιση της διαλειτουργικότητας σύμφωνα με διεθνή πρότυπα και τεχνολογικά συστήματα, και, ως εκ τούτου, θα μπορούσε να αποτελέσει μοντέλο συνεργασίας σε παγκόσμιο επίπεδο.

(3) Για να είναι δυνατή η ανάγνωση και η ερμηνεία του Ψηφιακού Πιστοποιητικού COVID της ΕΕ, απαιτείται κοινή δομή δεδομένων και συμφωνία ως προς την αποδιδόμενη έννοια κάθε πεδίου δεδομένων του ωφέλιμου φορτίου, καθώς και ως προς τις πιθανές τιμές του. Για να διευκολυνθεί η εν λόγω διαλειτουργικότητα, είναι αναγκαίο να οριστεί κοινή, συντονισμένη δομή δεδομένων για το πλαίσιο του Ψηφιακού Πιστοποιητικού COVID της ΕΕ. Οι κατευθυντήριες γραμμές για το εν λόγω πλαίσιο εκπονήθηκαν από το δίκτυο eHealth, το οποίο συστάθηκε βάσει της οδηγίας 2011/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([2]). Οι εν λόγω κατευθυντήριες γραμμές θα πρέπει να λαμβάνονται υπόψη κατά τον καθορισμό των τεχνικών προδιαγραφών με τις οποίες προσδιορίζεται ο μορφότυπος και η διαχείριση εμπιστοσύνης για το Ψηφιακό Πιστοποιητικό COVID της ΕΕ. Θα πρέπει επίσης να προσδιοριστούν μηχανισμοί κωδικοποίησης μεταφορών, καθώς και μηχανισμός κωδικοποίησης μεταφοράς σε μηχαναγνώσιμο οπτικό μορφότυπο (QR), ο οποίος μπορεί να επιδεικνύεται από την οθόνη κινητής συσκευής ή να εκτυπώνεται σε έντυπη μορφή.

(4) Επιπλέον των τεχνικών προδιαγραφών για τον μορφότυπο και τη διαχείριση εμπιστοσύνης του Ψηφιακού Πιστοποιητικού COVID της ΕΕ, η εν λόγω απόφαση θα πρέπει να θεσπίζει γενικούς κανόνες για τη συμπλήρωση των στοιχείων στα πιστοποιητικά, οι οποίοι πρέπει να χρησιμοποιούνται για κωδικοποιημένες τιμές στο περιεχόμενο του Ψηφιακού Πιστοποιητικού COVID της ΕΕ. Τα σύνολα τιμών για την εφαρμογή αυτών των κανόνων θα πρέπει να επικαιροποιούνται ανά τακτά χρονικά διαστήματα και να δημοσιεύονται από την Επιτροπή, με βάση τις σχετικές εργασίες του δικτύου eHealth.

(5) Σύμφωνα με τον κανονισμό (ΕΕ) 2021/953, τα γνήσια πιστοποιητικά που απαρτίζουν το Ψηφιακό Πιστοποιητικό COVID της ΕΕ πρέπει να αναγνωρίζονται χωριστά μέσω ενός μοναδικού αναγνωριστικού κωδικού, δεδομένου ότι είναι δυνατή η έκδοση περισσοτέρων του ενός πιστοποιητικά για τους πολίτες, κατά το χρονικό διάστημα που ο κανονισμός (ΕΕ) 2021/953 παραμένει σε ισχύ. Ο μοναδικός αναγνωριστικός κωδικός πιστοποιητικού πρέπει να αποτελείται από σειρά αλφαριθμητικών χαρακτήρων, και τα κράτη μέλη θα πρέπει να διασφαλίζουν ότι δεν περιέχει δεδομένα που τον συνδέουν με άλλα έγγραφα ή αναγνωριστικούς κωδικούς, όπως οι αριθμοί διαβατηρίου ή δελτίου ταυτότητας, ώστε να αποτρέπεται η δυνατότητα ταυτοποίησης του κατόχου. Για να διασφαλιστεί ότι ο αναγνωριστικός κωδικός πιστοποιητικού είναι μοναδικός, θα πρέπει να καθοριστούν τεχνικές προδιαγραφές και κανόνες για την κοινή δομή του.

([1]) ΕΕ L 211 της 15.6.2021, σ. 1.

([2]) Οδηγία 2011/24/ΕΕ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 9ης Μαρτίου 2011, περί εφαρμογής των δικαιωμάτων των ασθενών στο πλαίσιο της διασυνοριακής υγειονομικής περίθαλψης (ΕΕ L 88 της 4.4.2011, σ. 45).

(6) Η ασφάλεια, η γνησιότητα, η εγκυρότητα και η ακεραιότητα των πιστοποιητικών που απαρτίζουν το Ψηφιακό Πιστοποιητικό COVID της ΕΕ, καθώς και η συμμόρφωσή τους με το ενωσιακό δίκαιο για την προστασία δεδομένων, έχουν καίρια σημασία για την αποδοχή των εν λόγω πιστοποιητικών σε όλα τα κράτη μέλη. Οι εν λόγω στόχοι επιτυγχάνονται μέσω του πλαισίου εμπιστοσύνης που καθορίζει τους κανόνες και την υποδομή για την έκδοση και επαλήθευση των Ψηφιακών Πιστοποιητικών COVID της ΕΕ με αξιόπιστο και ασφαλή τρόπο. Μεταξύ άλλων, το πλαίσιο εμπιστοσύνης θα πρέπει να βασίζεται σε υποδομή δημόσιου κλειδιού με αλυσίδα εμπιστοσύνης από τις υγειονομικές αρχές των κρατών μελών ή άλλες έμπιστες αρχές έως τις επιμέρους οντότητες που εκδίδουν τα Ψηφιακά Πιστοποιητικά COVID της ΕΕ. Ως εκ τούτου, προκειμένου να εξασφαλιστεί ένα σύστημα διαλειτουργικότητας σε ολόκληρη την ΕΕ, η Επιτροπή έχει δημιουργήσει ένα κεντρικό σύστημα —την πύλη Ψηφιακού Πιστοποιητικού COVID της ΕΕ (στο εξής: πύλη)— στο οποίο αποθηκεύονται τα δημόσια κλειδιά που χρησιμοποιούνται για την επαλήθευση. Κατά τη σάρωση του κωδικού QR, η ψηφιακή υπογραφή επαληθεύεται με τη χρήση του αντίστοιχου δημόσιου κλειδιού, το οποίο έχει αποθηκευτεί προηγουμένως στην εν λόγω κεντρική πύλη. Οι ψηφιακές υπογραφές μπορούν να χρησιμοποιούνται για τη διασφάλιση της ακεραιότητας και της γνησιότητας των δεδομένων. Οι υποδομές δημόσιων κλειδιών δημιουργούν κλίμα εμπιστοσύνης μέσω της σύνδεσης των δημόσιων κλειδιών με τους εκδότες των πιστοποιητικών. Στην πύλη χρησιμοποιούνται πολλαπλά πιστοποιητικά δημόσιου κλειδιού για λόγους γνησιότητας. Προκειμένου να διασφαλιστεί η ασφαλής ανταλλαγή δεδομένων για το υλικό δημόσιου κλειδιού μεταξύ των κρατών μελών και να εξασφαλιστεί η δυνατότητα ευρείας διαλειτουργικότητας, είναι αναγκαίο να καθοριστούν τα πιστοποιητικά δημόσιου κλειδιού που μπορούν να χρησιμοποιούνται και να προσδιοριστεί ο τρόπος με τον οποίο θα πρέπει να παράγονται.

(7) Η παρούσα απόφαση παρέχει τη δυνατότητα εφαρμογής των απαιτήσεων του κανονισμού (ΕΕ) 2021/953 κατά τέτοιον τρόπο ώστε να ελαχιστοποιείται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα στα αναγκαία στοιχεία που απαιτούνται για να είναι λειτουργικό το Ψηφιακό Πιστοποιητικό COVID της ΕΕ, ενώ βοηθά παράλληλα τους τελικούς υπεύθυνους επεξεργασίας να εφαρμόζουν τις εν λόγω απαιτήσεις τηρώντας την προστασία δεδομένων από το στάδιο του σχεδιασμού.

(8) Σύμφωνα με τον κανονισμό (ΕΕ) 2021/953, οι αρχές ή άλλοι εντεταλμένοι φορείς που είναι αρμόδιοι για την έκδοση των πιστοποιητικών είναι οι υπεύθυνοι επεξεργασίας για τους οποίους γίνεται μνεία στο άρθρο 4 παράγραφος 7 του κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([3]), ο ρόλος των οποίων έγκειται στην επεξεργασία δεδομένων προσωπικού χαρακτήρα κατά τη διαδικασία έκδοσης. Ενδέχεται να υπάρχουν μία ή περισσότερες αρχές ή εντεταλμένοι φορείς, για παράδειγμα περιφερειακές υγειονομικές υπηρεσίες, ανάλογα με τον τρόπο με τον οποίο τα κράτη μέλη οργανώνουν τη διαδικασία έκδοσης. Πρόκειται για επιλογή που διαθέτουν τα κράτη μέλη σύμφωνα με την αρχή της επικουρικότητας. Ως εκ τούτου, τα κράτη μέλη είναι τα πλέον κατάλληλα να διασφαλίζουν, σε περίπτωση που υπάρχουν πολλαπλές αρχές ή άλλοι εντεταλμένοι φορείς, την κατανομή των αντίστοιχων αρμοδιοτήτων τους με σαφή τρόπο, ανεξάρτητα από το αν λειτουργούν ως υπεύθυνοι επεξεργασίας χωριστά ή από κοινού (συμπεριλαμβανομένων των περιφερειακών υγειονομικών υπηρεσιών που δημιουργούν κοινή δικτυακή πύλη ασθενών για την έκδοση των πιστοποιητικών). Ομοίως, όσον αφορά την επαλήθευση πιστοποιητικών από τις αρμόδιες αρχές του κράτους μέλους προορισμού ή διέλευσης, ή από τους παρόχους διασυνοριακών υπηρεσιών επιβατικών μεταφορών που υποχρεούνται, βάσει του εθνικού δικαίου, να εφαρμόζουν ορισμένα μέτρα δημόσιας υγείας κατά τη διάρκεια της πανδημίας COVID-19, οι εν λόγω ελεγκτές οφείλουν να τηρούν τις υποχρεώσεις τους σύμφωνα με τους κανόνες προστασίας δεδομένων.

(9) Δεν πραγματοποιείται επεξεργασία δεδομένων προσωπικού χαρακτήρα μέσω της πύλης Ψηφιακού Πιστοποιητικού COVID της ΕΕ, διότι η πύλη περιέχει μόνο τα δημόσια κλειδιά των υπογραφουσών αρχών. Τα εν λόγω κλειδιά αφορούν τις υπογράφουσες αρχές και δεν παρέχουν τη δυνατότητα ούτε άμεσης ούτε έμμεσης εκ νέου ταυτοποίησης του φυσικού προσώπου για το οποίο εκδίδεται το πιστοποιητικό. Ως εκ τούτου, η Επιτροπή, ως διαχειριστής της πύλης, δεν θα πρέπει να είναι ούτε υπεύθυνος επεξεργασίας, ούτε εκτελών την επεξεργασία δεδομένων προσωπικού χαρακτήρα.

(10) Ζητήθηκε η γνώμη του Ευρωπαίου Επόπτη Προστασίας Δεδομένων σύμφωνα με το άρθρο 42 παράγραφος 1 του κανονισμού (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου ([4]), ο οποίος γνωμοδότησε στις 22 Ιουνίου 2021.

(11) Λαμβανομένων υπόψη των τεχνικών προδιαγραφών και των κανόνων που απαιτούνται για την εφαρμογή του κανονισμού (ΕΕ) 2021/953 από την 1η Ιουλίου 2021, η άμεση εφαρμογή της παρούσας απόφασης είναι αιτιολογημένη.

(12) Συνεπώς, λαμβανομένης υπόψη της ανάγκης ταχείας εφαρμογής του Ψηφιακού Πιστοποιητικού COVID της ΕΕ, η παρούσα απόφαση θα πρέπει να αρχίσει να ισχύει από την ημέρα της δημοσίευσής της.

([3]) Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων) (ΕΕ L 119 της 4.5.2016, σ. 1).

([4]) Κανονισμός (ΕΕ) 2018/1725 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Οκτωβρίου 2018, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα από τα θεσμικά και λοιπά όργανα και τους οργανισμούς της Ένωσης και την ελεύθερη κυκλοφορία των δεδομένων αυτών, και για την κατάργηση του κανονισμού (ΕΚ) αριθ. 45/2001 και της απόφασης αριθ. 1247/2002/ΕΚ (ΕΕ L 295 της 21.11.2018, σ. 39).

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

Άρθρο 1

Οι τεχνικές προδιαγραφές για το Ψηφιακό Πιστοποιητικό COVID της ΕΕ όσον αφορά τον καθορισμό της γενικής δομής δεδομένων, τους μηχανισμούς κωδικοποίησης και τον μηχανισμό κωδικοποίησης μεταφοράς σε μηχαναγνώσιμο οπτικό μορφότυπο, παρατίθενται στο παράρτημα I.

Άρθρο 2

Οι κανόνες για τη συμπλήρωση των στοιχείων στα πιστοποιητικά που αναφέρονται στο άρθρο 3 παράγραφος 1 του κανονισμού (ΕΕ) 2021/953 παρατίθενται στο παράρτημα II της παρούσας απόφασης.

Άρθρο 3

Οι απαιτήσεις με τις οποίες καθορίζεται η κοινή δομή του μοναδικού αναγνωριστικού κωδικού πιστοποιητικού, παρατίθενται στο παράρτημα III.

Άρθρο 4

Οι εφαρμοστέοι κανόνες διαχείρισης πιστοποιητικών με δημόσιο κλειδί σε σχέση με την πύλη Ψηφιακού Πιστοποιητικού COVID της ΕΕ για την υποστήριξη των πτυχών διαλειτουργικότητας του πλαισίου εμπιστοσύνης παρατίθενται στο παράρτημα IV.

Η παρούσα απόφαση αρχίζει να ισχύει την ημέρα της δημοσίευσής της στην *Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης*.

Βρυξέλλες, 28 Ιουνίου 2021.

Για την Επιτροπή
Η Πρόεδρος
Ursula VON DER LEYEN

ΠΑΡΑΡΤΗΜΑ Ι

ΜΟΡΦΟΤΥΠΟΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗ ΕΜΠΙΣΤΟΣΥΝΗΣ

Γενική δομή δεδομένων, μηχανισμοί κωδικοποίησης και μηχανισμός κωδικοποίησης μεταφοράς σε μηχαναγνώσιμο οπτικό μορφότυπο (στο εξής: QR)

1. **Εισαγωγή**

Οι τεχνικές προδιαγραφές που καθορίζονται στο παρόν παράρτημα περιέχουν τη γενική δομή δεδομένων, καθώς και τους μηχανισμούς κωδικοποίησης για το Ψηφιακό Πιστοποιητικό COVID της ΕΕ (στο εξής: DCC). Καθορίζουν επίσης μηχανισμό κωδικοποίησης μεταφοράς σε μηχαναγνώσιμο οπτικό μορφότυπο (QR), ο οποίος μπορεί να επιδεικνύεται από την οθόνη κινητής συσκευής ή να εκτυπώνεται. Οι μορφότυποι περιέκτη του ηλεκτρονικού πιστοποιητικού υγείας των εν λόγω προδιαγραφών είναι γενική, ωστόσο στο παρόν περιβάλλον χρησιμοποιούνται για τη μεταφορά του DCC.

2. **Ορολογία**

Για τους σκοπούς του παρόντος παραρτήματος, ως «εκδότες» νοούνται οι οργανισμοί που χρησιμοποιούν τις παρούσες προδιαγραφές για την έκδοση πιστοποιητικών υγείας και ως «ελεγκτές» νοούνται οι οργανισμοί που αποδέχονται τα πιστοποιητικά υγείας ως αποδεικτικό της κατάστασης της υγείας. Ως «συμμετέχοντες» νοούνται οι εκδότες και οι ελεγκτές. Για ορισμένες πτυχές που καθορίζονται στο παρόν παράρτημα πρέπει να εξασφαλίζεται συντονισμός μεταξύ των συμμετεχόντων, όπως για τη διαχείριση χώρου ονομάτων και τη διανομή κρυπτογραφικών κλειδιών. Τα ως άνω καθήκοντα θεωρείται ότι εκτελούνται από μια οντότητα, η οποία αναφέρεται στο εξής ως «γραμματεία».

3. **Μορφότυποι περιέκτη ηλεκτρονικού πιστοποιητικού υγείας**

Ο μορφότυπος περιέκτη ηλεκτρονικού πιστοποιητικού υγείας (Electronic Health Certificate Container Format, HCERT) έχει σχεδιαστεί με σκοπό την παροχή ενιαίου και τυποποιημένου μέσου για ηλεκτρονικά πιστοποιητικά υγείας που εκδίδονται από τους διάφορους εκδότες τους (εφεξής: «εκδότες»). Ο στόχος των παρουσών προδιαγραφών είναι η εναρμόνιση του τρόπου αναπαράστασης, κωδικοποίησης και υπογραφής των εν λόγω πιστοποιητικών υγείας, με σκοπό τη διευκόλυνση της διαλειτουργικότητας.

Για να είναι δυνατή η ανάγνωση και η ερμηνεία ενός DCC που εκδίδεται από έναν εκδότη, απαιτείται κοινή δομή δεδομένων και συμφωνία ως προς τη σημασία του ωφέλιμου φορτίου κάθε πεδίου δεδομένων. Για να διευκολυνθεί η εν λόγω διαλειτουργικότητα, ορίζεται μια κοινή συντονισμένη δομή δεδομένων μέσω της χρήσης ενός συστήματος «JSON», η οποία αποτελεί και το πλαίσιο του DCC.

3.1. *Δομή του ωφέλιμου φορτίου*

Το ωφέλιμο φορτίο δομείται και κωδικοποιείται ως μορφότυπος CBOR με ψηφιακή υπογραφή COSE. Είναι κοινώς γνωστό ως «διακριτικό Web CBOR» (CWT) και ορίζεται στο πρότυπο RFC 8392 ([1]). Το ωφέλιμο φορτίο, όπως ορίζεται στα τμήματα κατωτέρω, μεταφέρεται σε δήλωση hcert.

Η ακεραιότητα και η γνησιότητα της προέλευσης του ωφέλιμου φορτίου δεδομένων πρέπει να είναι επαληθεύσιμες από τον ελεγκτή. Για την παροχή αυτού του μηχανισμού, ο εκδότης πρέπει να υπογράφει το CWT με τη χρήση ασύμμετρου σχήματος ηλεκτρονικής υπογραφής, όπως ορίζεται στην προδιαγραφή COSE (πρότυπο RFC 8152 ([2])).

3.2. *Δηλώσεις CWT*

3.2.1. Επισκόπηση δομής CWT

Προστατευμένη κεφαλίδα

— Αλγόριθμος υπογραφής (alg, ετικέτα 1)

— Αναγνωριστικό κλειδιού (kid, ετικέτα 4)

Ωφέλιμο φορτίο

— Εκδότης (iss, δήλωση κλειδιού 1, προαιρετικά, ISO 3166-1 alpha-2 του εκδότη)

— Εκδόθηκε στις (iat, δήλωση κλειδιού 6)

— Χρόνος λήξης (exp, δήλωση κλειδιού 4)

— Πιστοποιητικό υγείας (hcert, δήλωση κλειδιού -260)

— Ψηφιακό Πιστοποιητικό COVID της ΕΕ έκδ.1 (eu_DCC_v1, δήλωση κλειδιού 1)

Υπογραφή

([1]) rfc8392 (ietf.org).
([2]) rfc8152 (ietf.org).

3.2.2. Αλγόριθμος υπογραφής

Η παράμετρος του αλγόριθμου υπογραφής (alg) δηλώνει τον αλγόριθμο που χρησιμοποιείται για τη δημιουργία της υπογραφής. Πρέπει να πληροί ή να υπερβαίνει τις υφιστάμενες κατευθυντήριες γραμμές της συμβουλευτικής επιτροπής για τα μέτρα που πρέπει να ληφθούν στον τομέα της ασφάλειας των συστημάτων πληροφοριών SOG-IS), όπως συνοψίζονται στις επόμενες παραγράφους.

Ορίζονται ένας πρωτεύων κι ένας δευτερεύων αλγόριθμος. Ο δευτερεύων αλγόριθμος θα πρέπει να χρησιμοποιείται μόνον εάν ο πρωτεύων αλγόριθμος δεν είναι αποδεκτός στο πλαίσιο των κανόνων και των κανονισμών που επιβάλλονται στον εκδότη.

Προκειμένου να διασφαλιστεί η ασφάλεια του συστήματος, ο δευτερεύων αλγόριθμος πρέπει να ενσωματώνεται σε κάθε υλοποίηση. Για τον λόγο αυτόν, πρέπει να εφαρμόζεται τόσο ο πρωτεύων όσο και ο δευτερεύων αλγόριθμος.

Τα επίπεδα του συνόλου SOG-IS για τους πρωτεύοντες και τους δευτερεύοντες αλγόριθμους είναι τα εξής:

— Πρωτεύων αλγόριθμος: Ο πρωτεύων αλγόριθμος είναι ο αλγόριθμος ελλειπτικής καμπύλης ψηφιακής υπογραφής (Elliptic Curve Digital Signature Algorithm, ECDSA), όπως ορίζεται στο τμήμα 2.3 (του προτύπου ISO/IEC 14888-3:2006), με τη χρήση των παραμέτρων P–256 που ορίζονται στο προσάρτημα D (D.1.2.3) (του πρότυπου FIPS PUB 186-4), σε συνδυασμό με τον αλγόριθμο κατακερματισμού SHA-256, όπως ορίζεται στη συνάρτηση 4 (ISO/IEC 10118-3:2004).

Η τιμή αυτή αντιστοιχεί στην παράμετρο του αλγορίθμου COSE ES256.

— Δευτερεύων αλγόριθμος: Ο δευτερεύων αλγόριθμος είναι ο RSASSA-PSS, όπως ορίζεται στο πρότυπο (RFC 8230 ([3])), με τελεστή υπολοίπου διαίρεσης 2048 bits σε συνδυασμό με τον αλγόριθμο κατακερματισμού SHA-256, όπως ορίζεται στη συνάρτηση 4 (ISO/IEC 10118-3:2004).

Η τιμή αυτή αντιστοιχεί στην παράμετρο του αλγορίθμου COSE: PS256.

3.2.3. Αναγνωριστικό κλειδιού

Η δήλωση αναγνωριστικού κλειδιού (kid) δηλώνει το πιστοποιητικό υπογραφής εγγράφου (DSC) που περιέχει το δημόσιο κλειδί που πρέπει να χρησιμοποιείται από τον ελεγκτή για τον έλεγχο της ορθότητας της ψηφιακής υπογραφής. Η διαχείριση πιστοποιητικών δημόσιου κλειδιού, συμπεριλαμβανομένων των απαιτήσεων για τα DSC, περιγράφεται στο παράρτημα IV.

Η δήλωση αναγνωριστικού κλειδιού (kid) χρησιμοποιείται από τους ελεγκτές για την επιλογή του ορθού δημόσιου κλειδιού από έναν κατάλογο κλειδιών που παραπέμπουν στον εκδότη που αναφέρεται στη δήλωση εκδότη (iss). Ο εκδότης μπορεί, για διοικητικούς λόγους, να χρησιμοποιεί παράλληλα διάφορα κλειδιά, καθώς και όταν πραγματοποιεί επαναφορές κλειδιών. Το αναγνωριστικό κλειδιού δεν συνιστά τομέα δεδομένων κρίσιμης σημασίας για την ασφάλεια. Για τον λόγο αυτόν, μπορεί να τοποθετείται επίσης σε μη προστατευμένη κεφαλίδα, εάν αυτό απαιτείται. Οι ελεγκτές πρέπει να κάνουν δεκτές και τις δύο επιλογές. Εάν υπάρχουν και οι δύο επιλογές, το αναγνωριστικό κλειδιού πρέπει να χρησιμοποιείται στην προστατευόμενη κεφαλίδα.

Λόγω της συντόμευσης του αναγνωριστικού (για λόγους περιορισμού του μεγέθους), υπάρχει μικρή, αλλά όχι μηδενική, πιθανότητα ο συνολικός κατάλογος των πιστοποιητικών υπογραφής εγγράφων (DSC) που γίνονται δεκτά από τον ελεγκτή να περιέχει DSC με διπλότυπα αναγνωριστικά κλειδιού (kid). Για τον λόγο αυτόν, ο ελεγκτής πρέπει να ελέγχει όλα τα DSC με τα εν λόγω kid.

3.2.4. Εκδότης

Η δήλωση εκδότη (iss) είναι η τιμή συμβολοσειράς που μπορεί να φέρει προαιρετικά τον κωδικό χώρας ISO 3166-1 alpha-2 της οντότητας που εκδίδει το πιστοποιητικό υγείας. Ο ελεγκτής μπορεί να χρησιμοποιεί την εν λόγω δήλωση για τον προσδιορισμό του συνόλου των DSC που πρέπει να χρησιμοποιούνται για τους σκοπούς της επαλήθευσης. Η δήλωση κλειδιού 1 χρησιμοποιείται για τον προσδιορισμό αυτής της δήλωσης.

3.2.5. Χρόνος λήξης

Η δήλωση του χρόνου λήξης (exp) φέρει χρονοσφραγίδα σε ακέραιο αριθμητικό μορφότυπο ημερομηνίας (όπως ορίζεται στο πρότυπο RFC 8392 ([4]) τμήμα 2), με την οποία δηλώνεται το χρονικό διάστημα κατά το οποίο η συγκεκριμένη υπογραφή για το ωφέλιμο φορτίο θεωρείται έγκυρη, μετά την παρέλευση του οποίου ο ελεγκτής απορρίπτει το ωφέλιμο φορτίο διότι έχει λήξει. Σκοπός της παραμέτρου λήξης είναι η επιβολή περιορισμού στην περίοδο εγκυρότητας του πιστοποιητικού υγείας. Η δήλωση κλειδιού 4 χρησιμοποιείται για τον προσδιορισμό αυτής της δήλωσης.

Ο χρόνος λήξης δεν πρέπει να υπερβαίνει την περίοδο ισχύος του DSC.

([3]) rfc8230 (ietf.org).
([4]) rfc8392 (ietf.org).

3.2.6. Εκδόθηκε στις

Η δήλωση «Εκδόθηκε στις» (iat) φέρει χρονοσφραγίδα σε ακέραιο αριθμητικό μορφότυπο ημερομηνίας (όπως ορίζεται στο πρότυπο RFC 8392 ([5]) τμήμα 2), με την οποία δηλώνεται ο χρόνος δημιουργίας του πιστοποιητικού υγείας.

Η τιμή στο πεδίο «Εκδόθηκε στις» δεν πρέπει να είναι προγενέστερη της περιόδου ισχύος του DSC.

Οι ελεγκτές δύνανται να εφαρμόζουν συμπληρωματικές πολιτικές για τον περιορισμό της εγκυρότητας του πιστοποιητικού υγείας με βάση τον χρόνο έκδοσης. Η δήλωση κλειδιού 6 χρησιμοποιείται για τον προσδιορισμό αυτής της δήλωσης.

3.2.7. Δήλωση πιστοποιητικού υγείας

Η δήλωση πιστοποιητικού υγείας (hcert) αποτελεί αντικείμενο JSON (πρότυπο RFC 7159 ([6])), το οποίο περιέχει τις πληροφορίες σχετικά με την κατάσταση της υγείας. Η ίδια δήλωση μπορεί να περιλαμβάνει πολλούς διαφορετικούς τύπους πιστοποιητικού υγείας, μεταξύ των οποίων και το DCC.

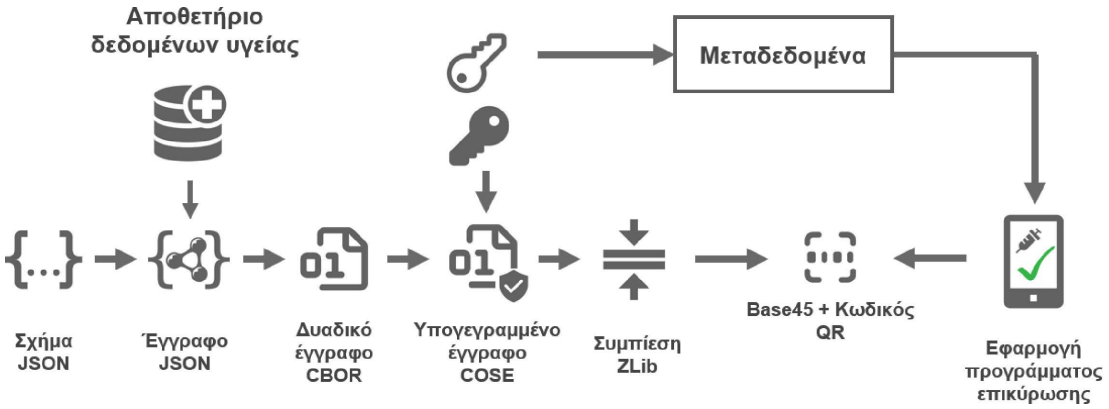
Ο μορφότυπος JSON χρησιμοποιείται αποκλειστικά και μόνο για τους σκοπούς του σχήματος. ο μορφότυπος αναπαράστασης είναι ο CBOR, όπως ορίζεται στο πρότυπο (RFC 7049 ([7])). Οι προγραμματιστές εφαρμογών ενδέχεται στην πράξη να μην προβαίνουν σε αποκωδικοποίηση ή κωδικοποίηση από και προς τον μορφότυπο JSON, αλλά να χρησιμοποιούν τη δομή εντός μνήμης.

Η δήλωση κλειδιού που πρέπει να χρησιμοποιείται για τον προσδιορισμό αυτής της δήλωσης είναι το -260.

Οι συμβολοσειρές στο αντικείμενο του JSON θα πρέπει να είναι κανονικοποιημένες κατά τη Μορφή κανονικοποίησης κανονικής σύνθεσης/Normalization Form Canonical Composition (NFC), που ορίζεται στο πρότυπο Unicode. Ωστόσο, οι εφαρμογές αποκωδικοποίησης στις πτυχές αυτές θα πρέπει να μην είναι περιοριστικές και να είναι αξιόπιστες, ενώ ενθαρρύνεται ιδιαιτέρως να γίνεται αποδεκτός κάθε εύλογος τύπος μετατροπής. Εάν, κατά τη διάρκεια της αποκωδικοποίησης, ή σε μεταγενέστερες συναρτήσεις σύγκρισης, διαπιστωθούν δεδομένα που δεν είναι κανονικοποιημένα, οι εφαρμογές θα πρέπει να εκτελεστούν με τον ίδιο τρόπο που θα λειτουργούσαν εάν τα δεδομένα εισόδου ήταν κανονικοποιημένα κατά NFC.

4. Σειριοποίηση και δημιουργία του ωφέλιμου φορτίου DCC

Το σχήμα που ακολουθεί χρησιμοποιείται ως μοτίβο σειριοποίησης:



Η διαδικασία ξεκινά με την εξαγωγή δεδομένων, για παράδειγμα, από αποθετήριο δεδομένων υγείας (ή από κάποια εξωτερική πηγή δεδομένων), που διαρθρώνει τα εξαγόμενα δεδομένα σύμφωνα με τα καθορισμένα συστήματα DCC. Κατά τη διαδικασία αυτή, η μετατροπή στον καθορισμένο μορφότυπο δεδομένων και ο μετασχηματισμός, ώστε τα δεδομένα να είναι πιο ευανάγνωστα για τους χρήστες, μπορούν να πραγματοποιηθούν πριν από την έναρξη της σειριοποίησης σε μορφότυπο CBOR. Σε κάθε περίπτωση, τα ακρωνύμια των δηλώσεων αντιστοιχούν στα εμφανιζόμενα ονόματα πριν από τη σειριοποίηση και μετά την απο-σειριοποίηση.

Δεν επιτρέπεται προαιρετικό περιεχόμενο εθνικών δεδομένων σε πιστοποιητικά που εκδίδονται σύμφωνα με τον κανονισμό (ΕΕ) 2021/953 ([8]). Το περιεχόμενο δεδομένων περιορίζεται στα καθορισμένα στοιχεία δεδομένων που περιλαμβάνονται στο ελάχιστο σύνολο δεδομένων, το οποίο καθορίζεται στο παράρτημα του κανονισμού (ΕΕ) 2021/953.

([5]) rfc8392 (ietf.org).
([6]) rfc7159 (ietf.org).
([7]) rfc7049 (ietf.org).
([8]) Κανονισμός (ΕΕ) 2021/953 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 14ης Ιουνίου 2021, σχετικά με πλαίσιο για την έκδοση, την επαλήθευση και την αποδοχή διαλειτουργικών πιστοποιητικών εμβολιασμού κατά της COVID-19, διαγνωστικού της ελέγχου και ανάρρωσης από αυτή (Ψηφιακό Πιστοποιητικό COVID της ΕΕ) με σκοπό να διευκολυνθεί η ελεύθερη κυκλοφορία κατά τη διάρκεια της πανδημίας της COVID-19 (ΕΕ L 211 της 15.6.2021, σ. 1).

5. **Κωδικοποιήσεις μεταφοράς**

5.1. *Χωρίς επεξεργασία*

Για αυθαίρετες διεπαφές δεδομένων, ο περιέκτης HCERT και τα ωφέλιμα φορτία του μπορούν να διαβιβάζονται ως έχουν, με τη χρήση οποιασδήποτε υποκείμενης, ασφαλούς κατά 8 bit, αξιόπιστης μεταφοράς δεδομένων. Οι εν λόγω διεπαφές δύνανται να περιλαμβάνουν τεχνολογία που περιλαμβάνει τη λειτουργία επικοινωνίας κοντινού πεδίου (Near-Field Communication - NFC), Bluetooth ή διαβίβαση από πρωτόκολλο επιπέδου εφαρμογών, για παράδειγμα διαβίβαση ενός HCERT από τον εκδότη προς την κινητή συσκευή του κατόχου.

Εάν η διαβίβαση του HCERT από τον εκδότη στον κάτοχο βασίζεται σε διεπαφή που περιέχει μόνο επίδειξη (π.χ. SMS, e-mail), προφανώς δεν μπορεί να εφαρμοστεί η κωδικοποίηση μεταφοράς χωρίς επεξεργασία.

5.2. *Ραβδοκώδικας*

5.2.1. Συμπίεση ωφέλιμου φορτίου (CWT)

Για τη μείωση του μεγέθους και τη βελτίωση της ταχύτητας και της αξιοπιστίας στη διαδικασία ανάγνωσης του HCERT, το CWT θα πρέπει να συμπιεστεί με τη χρήση του ZLIB (πρότυπο RFC 1950 ([9])) και του συστήματος συμπίεσης «Deflate», στον μορφότυπο που ορίζεται στο πρότυπο RFC 1951 ([10]).

5.2.2. Δισδιάστατος ραβδοκώδικας QR

Για τον καλύτερο χειρισμό του εξοπλισμού παλαιού τύπου που είναι σχεδιασμένος να λειτουργεί σε ωφέλιμα φορτία ASCII, το συμπιεσμένο CWT κωδικοποιείται ως ASCII με τη χρήση της Base45 πριν από την κωδικοποίησή του σε δισδιάστατο ραβδοκώδικα.

Ο μορφότυπος QR, όπως ορίζεται στο (ISO/IEC 18004:2015), χρησιμοποιείται για τη δημιουργία του δισδιάστατου ραβδοκώδικα. Συνιστάται ποσοστό διόρθωσης σφάλματος «Q» (περίπου 25 %). Επειδή χρησιμοποιείται η Base45, ο κωδικός QR πρέπει να χρησιμοποιεί αλφαριθμητική κωδικοποίηση (λειτουργία 2, που υποδεικνύεται από τα σύμβολα 0010).

Προκειμένου οι ελεγκτές να είναι σε θέση να εντοπίζουν τον τύπο των κωδικοποιημένων δεδομένων και να επιλέγουν το κατάλληλο σχήμα αποκωδικοποίησης και επεξεργασίας, τα δεδομένα που έχουν κωδικοποιηθεί με Base45 (σύμφωνα με τις παρούσες προδιαγραφές) φέρουν πρόθεμα με τη συμβολοσειρά αναγνωριστικού περιβάλλοντος «HC1». Σε μελλοντικές εκδόσεις των παρουσών προδιαγραφών με αντίκτυπο στην οπισθόδρομη συμβατότητα θα πρέπει να ορίζεται νέο αναγνωριστικό περιβάλλοντος, ενώ ο χαρακτήρας μετά το «HC» θα πρέπει να απαλείφεται από το σύνολο χαρακτήρων [1-9A-Z]. Η σειρά προσαυξήσεων ορίζεται να έχει αυτή τη σειρά, δηλαδή πρώτα [1-9] και μετά [A-Z].

Συνιστάται ο οπτικός κώδικας να παρέχεται σε μέσα προβολής με διαγώνιο μέγεθος μεταξύ 35 mm και 60 mm, ώστε να διευκολύνεται η χρήση συσκευών ανάγνωσης σταθερής οπτικής, σε περίπτωση που τα μέσα προβολής πρέπει να τίθενται στην επιφάνεια της συσκευής ανάγνωσης.

Εάν ο οπτικός κώδικας εκτυπώνεται σε χαρτί με τη χρήση εκτυπωτών χαμηλής ανάλυσης (< 300 dpi), εφιστάται ιδιαιτέρως η προσοχή ώστε κάθε σύμβολο (τελεία) του κωδικού QR να αναπαρίσταται ακριβώς ως τετράγωνο. Η μη αναλογική προσαρμογή θα έχει ως αποτέλεσμα ορισμένες γραμμές ή στήλες στον κωδικό QR να περιλαμβάνουν παραλληλόγραμμα σύμβολα, λόγω των οποίων ο κωδικός σε πολλές περιπτώσεις δεν θα είναι ευανάγνωστος.

6. **Μορφότυπος καταλόγων εμπιστοσύνης (κατάλογος CSCA και DSC)**

Κάθε κράτος μέλος οφείλει να παρέχει κατάλογο μίας ή περισσοτέρων εθνικών αρχών πιστοποίησης (CSCA), κατάλογο πιστοποιητικών του υπογράφοντος το έγγραφο (DSC), και να διατηρεί τους εν λόγω καταλόγους ενημερωμένους.

6.1. *Απλουστευμένα πιστοποιητικά CSCA/DSC*

Από την παρούσα έκδοση των προδιαγραφών, τα κράτη μέλη δεν θεωρούν ότι χρησιμοποιούνται πληροφορίες από καταστάσεις ανάκλησης πιστοποιητικών (Certificate Revocation List, CRL)· ή ότι η περίοδος χρήσης ιδιωτικού κλειδιού επαληθεύεται από τους φορείς υλοποίησης.

Αντιθέτως, ο κύριος μηχανισμός εγκυρότητας είναι η εμφάνιση του πιστοποιητικού στην πλέον πρόσφατη έκδοση του εν λόγω καταλόγου πιστοποιητικών.

([9]) rfc1950 (ietf.org).
([10]) rfc1951 (ietf.org).

6.2. *Υποδομή δημόσιου κλειδιού (PKI) για ηλεκτρονικό μηχανικώς αναγνώσιμο ταξιδιωτικό έγγραφο (eMRTD) του ΔΟΠΑ και Κέντρα Εμπιστοσύνης*

Τα κράτη μέλη μπορούν να χρησιμοποιούν χωριστή CSCA, αλλά μπορούν επίσης να χρησιμοποιούν και να υποβάλλουν τα υφιστάμενα πιστοποιητικά CSCA και/ή DSC για ηλεκτρονικά μηχανικώς αναγνώσιμα ταξιδιωτικά έγγραφα (eMRTD)· μπορούν ακόμη και να επιλέγουν να προμηθεύονται τα εν λόγω πιστοποιητικά από (εμπορικά) κέντρα εμπιστοσύνης, και να υποβάλλουν τα εν λόγω πιστοποιητικά. Ωστόσο, κάθε DSC πρέπει πάντα να υπογράφεται από τη CSCA, την οποία υποβάλλει το εν λόγω κράτος μέλος.

7. **Παράμετροι ασφάλειας**

Κατά τον σχεδιασμό σχήματος με τη χρήση των παρουσών προδιαγραφών, τα κράτη μέλη προσδιορίζουν, αναλύουν και παρακολουθούν ορισμένες πτυχές ασφαλείας.

Θα πρέπει να λαμβάνονται υπόψη, κατ' ελάχιστον, οι ακόλουθες πτυχές:

7.1. *Χρόνος ισχύος υπογραφής του HCERT*

Ο εκδότης HCERT οφείλει να περιορίζει τη χρονική περίοδο ισχύος της υπογραφής καθορίζοντας τον χρόνο λήξης της υπογραφής. Με αυτόν τον τρόπο, ο κάτοχος πιστοποιητικού υγείας υποχρεούται να το ανανεώνει ανά τακτά χρονικά διαστήματα.

Η αποδεκτή χρονική περίοδος ισχύος μπορεί να καθορίζεται βάσει πρακτικών περιορισμών. Για παράδειγμα, έναν ταξιδιώτης ενδέχεται να μην έχει τη δυνατότητα να ανανεώνει το πιστοποιητικό υγείας ενώ βρίσκεται σε ταξίδι στο εξωτερικό. Ωστόσο, αυτό μπορεί να συμβεί επίσης σε περίπτωση που ο εκδότης εξετάζει την πιθανότητα κινδύνου ασφάλειας, περίπτωση στην οποία ο εκδότης οφείλει να αποσύρει ένα DSC (με ακύρωση όλων των πιστοποιητικών υγείας που έχουν εκδοθεί με τη χρήση του εν λόγω κλειδιού, το οποίο εξακολουθεί να βρίσκεται εντός της περιόδου ισχύος των εν λόγω πιστοποιητικών). Οι συνέπειες αυτής της περίπτωσης μπορούν να περιοριστούν με την κυλιόμενη χρήση των κλειδιών του εκδότη και με απαίτηση ανανέωσης όλων των πιστοποιητικών υγείας, μετά την παρέλευση εύλογου χρονικού διαστήματος.

7.2. *Διαχείριση κλειδιών*

Η εν λόγω προδιαγραφή βασίζεται σε μεγάλο βαθμό σε ισχυρούς μηχανισμούς κρυπτογράφησης για τη διασφάλιση της ακεραιότητας των δεδομένων και τον έλεγχο προέλευσης των δεδομένων. Ως εκ τούτου, είναι απαραίτητη η διατήρηση της εμπιστευτικότητας των ιδιωτικών κλειδιών.

Η εμπιστευτικότητα των κλειδιών κρυπτογράφησης μπορεί να εκτεθεί σε κίνδυνο με πολλούς διαφορετικούς τρόπους, π.χ.:

— Η διαδικασία δημιουργίας κλειδιού μπορεί να είναι ελαττωματική, με αποτέλεσμα τη δημιουργία αδύναμων κλειδιών.

— Τα κλειδιά μπορούν να αποκαλυφθούν από ανθρώπινο λάθος.

— Τα κλειδιά μπορούν να κλαπούν από εξωτερικούς ή εσωτερικούς παραβάτες.

— Οι αλγόριθμοι των κλειδιών μπορούν να υπολογιστούν με τη μέθοδο της κρυπτανάλυσης.

Προκειμένου να μετριαστούν οι κίνδυνοι σε περίπτωση που διαπιστωθεί ότι ο αλγόριθμος υπογραφής είναι αδύναμος, και υπάρχει πιθανότητα έκθεσης των ιδιωτικών κλειδιών σε κίνδυνο μέσω κρυπτανάλυσης, με την παρούσα προδιαγραφή συνιστάται σε όλους τους συμμετέχοντες να εφαρμόζουν δευτερεύοντα αλγόριθμο εναλλακτικής υπογραφής βάσει διαφορετικών παραμέτρων ή να εφαρμόζουν διαφορετικό μαθηματικό τύπο σε σχέση με τον πρωτεύοντα αλγόριθμο.

Όσον αφορά τους κινδύνους που αναφέρονται και συνδέονται με το περιβάλλον λειτουργίας των εκδοτών, εφαρμόζονται μέτρα μετριασμού του κινδύνου για τη διασφάλιση αποτελεσματικού ελέγχου, όπως, π.χ., δημιουργία, αποθήκευση και χρήση των ιδιωτικών κλειδιών σε ασφαλείς κρυπτογραφικές μονάδες (Hardware Security Modules, HSM). Συνιστάται ιδιαιτέρως η χρήση HSM για την υπογραφή των πιστοποιητικών υγείας.

Ανεξάρτητα από το αν ο εκδότης αποφασίσει να χρησιμοποιήσει τις HSM ή όχι, θα πρέπει να καταρτίζεται σχέδιο επαναφοράς κλειδιού, σύμφωνα με το οποίο η συχνότητα επαναφοράς των κλειδιών είναι ανάλογη προς την έκθεση των κλειδιών σε εξωτερικά δίκτυα, σε άλλα συστήματα και σε εργαζομένους. Ένα ορθά επιλεγμένο σχέδιο επαναφοράς περιορίζει επίσης τους κινδύνους που συνδέονται με πιστοποιητικά υγείας που έχουν εκδοθεί εσφαλμένα, παρέχοντας στον εκδότη τη δυνατότητα ανάκλησης των εν λόγω πιστοποιητικών σε δέσμες, με απόσυρση του κλειδιού, εάν αυτό απαιτείται.

7.3. *Επικύρωση δεδομένων εισόδου*

Οι εν λόγω προδιαγραφές μπορούν να χρησιμοποιούνται κατά τέτοιον τρόπο ώστε να αφήνεται να εννοηθεί η λήψη δεδομένων από μη έμπιστες πηγές σε συστήματα που ενδέχεται να είναι κρίσιμης σημασίας. Για τον μετριασμό των κινδύνων που συνδέονται με αυτό το εφαλτήριο επίθεσης, όλα τα πεδία εισόδου πρέπει να επικυρώνονται δεόντως μέσω του τύπου, του μήκους και του περιεχομένου των δεδομένων. Η υπογραφή του εκδότη επαληθεύεται επίσης πριν από την επεξεργασία του περιεχομένου του HCERT. Ωστόσο, η επικύρωση της υπογραφής του εκδότη συνεπάγεται πρώτα την ανάλυση της κεφαλίδας προστατευμένου εκδότη, στην οποία ο εισβολέας μπορεί να προσπαθήσει να εισαγάγει επιμελώς δημιουργημένες πληροφορίες που έχουν ως στόχο να θέσουν σε κίνδυνο την ασφάλεια του συστήματος.

8. **Διαχείριση εμπιστοσύνης**

Για την επαλήθευση της υπογραφής του HCERT απαιτείται δημόσιο κλειδί. Δημόσια κλειδιά αυτού του είδους καθίστανται διαθέσιμα από τα κράτη μέλη. Εντέλει, κάθε ελεγκτής πρέπει να έχει στη διάθεσή του έναν κατάλογο με όλα τα δημόσια κλειδιά που προτίθεται να εμπιστευτεί (δεδομένου ότι το δημόσιο κλειδί δεν αποτελεί μέρος του HCERT).

Το σύστημα αποτελείται (μόνο) από δύο επίπεδα· για κάθε κράτος μέλος, ένα ή περισσότερα πιστοποιητικά σε επίπεδο χώρας που το καθένα υπογράφει ένα ή περισσότερα πιστοποιητικά του υπογράφοντος το έγγραφο που χρησιμοποιούνται για καθημερινές λειτουργίες.

Τα πιστοποιητικά των κρατών μελών ονομάζονται πιστοποιητικά των «εθνικών αρχών πιστοποίησης» (CSCA) και αποτελούν (κατά κανόνα) αυθυπόγραφα πιστοποιητικά. Τα κράτη μέλη ενδέχεται να έχουν περισσότερες από μία αρχές (για παράδειγμα, σε περίπτωση διοικητικής αποκέντρωσης σε επίπεδο περιφερειών). Τα εν λόγω πιστοποιητικά CSCA υπογράφουν, ανά τακτά χρονικά διαστήματα, τα πιστοποιητικά του υπογράφοντος το έγγραφο (DSC) που χρησιμοποιούνται για την υπογραφή των HCERT.

Η «γραμματεία» επιτελεί λειτουργικό ρόλο. Ανά τακτά χρονικά διαστήματα συγκεντρώνει και δημοσιεύει τα DSC των κρατών μελών, αφού τα έχει επαληθεύσει βάσει του καταλόγου πιστοποιητικών CSCA (τα οποία έχουν διαβιβαστεί και επαληθευτεί με άλλα μέσα).

Ο κατάλογος των DSC που προκύπτει παρέχει στη συνέχεια το σύνολο των αποδεκτών δημόσιων κλειδιών (και τα αντίστοιχα αναγνωριστικά κλειδιών), τα οποία μπορούν να χρησιμοποιούν οι ελεγκτές για την επικύρωση των υπογραφών στα HCERT. Οι ελεγκτές πρέπει να λαμβάνουν και να ενημερώνουν τον εν λόγω κατάλογο ανά τακτά χρονικά διαστήματα.

Αυτοί οι ειδικοί για κάθε κράτος μέλος κατάλογοι μπορούν να προσαρμόζονται στον μορφότυπο που χρησιμοποιείται για τις εθνικές ρυθμίσεις τους. Στην περίπτωση αυτή, ο μορφότυπος αρχείου του συγκεκριμένου καταλόγου εμπιστοσύνης μπορεί να παρουσιάζει διαφοροποιήσεις, για παράδειγμα, μπορεί να αποτελεί υπογεγραμμένο JWKS (μορφότυπος συνόλου JWK σύμφωνα με το πρότυπο RFC 7517 ([11]) τμήμα 5) ή οποιονδήποτε άλλο, ειδικό για την τεχνολογία που χρησιμοποιείται στο συγκεκριμένο κράτος μέλος μορφότυπο.

Για λόγους απλούστευσης, τα κράτη μέλη μπορούν είτε να υποβάλλουν τα υφιστάμενα πιστοποιητικά CSCA από τα οικεία συστήματα που περιλαμβάνουν τα eMRTD του ΔΟΠΑ, σύμφωνα με τις συστάσεις του ΠΟΕ, είτε να δημιουργήσουν ένα πιστοποιητικό ειδικά για τον τομέα της υγείας.

8.1. *Το αναγνωριστικό κλειδιού (kid)*

Το αναγνωριστικό κλειδιού (key identifier, kid) υπολογίζεται κατά την κατάρτιση του καταλόγου έμπιστων δημόσιων κλειδιών από DSC και αποτελείται από περικομμένο (πρώτα 8 bytes) αποτύπωμα SHA-256 του DSC που έχει κωδικοποιηθεί σε μορφότυπο DER (χωρίς επεξεργασία).

Οι ελεγκτές δεν χρειάζεται να υπολογίσουν το αναγνωριστικό κλειδιού βάσει του DSC και μπορούν να αντιστοιχίσουν άμεσα το αναγνωριστικό κλειδιού με πιστοποιητικό υγείας που έχει εκδοθεί με το αναγνωριστικό κλειδιού στον κατάλογο εμπιστοσύνης.

8.2. *Διαφορές με το μοντέλο εμπιστοσύνης της υποδομής δημόσιου κλειδιού για το eMRTD του ΔΟΠΑ*

Παρόλο που ο σχεδιασμός βασίστηκε στις βέλτιστες πρακτικές του μοντέλου εμπιστοσύνης της υποδομής δημόσιου κλειδιού για τα eMRTD του ΔΟΠΑ, απαιτούνται ορισμένες απλουστεύσεις για λόγους ταχύτητας:

— Ένα κράτος μέλος μπορεί να υποβάλει πολλαπλά πιστοποιητικά CSCA.

— Η περίοδος ισχύος του DSC (χρήση κλειδιού) μπορεί να ορίζεται με οποιαδήποτε διάρκεια που δεν υπερβαίνει τη διάρκεια ισχύος του πιστοποιητικού CSCA και μπορεί να μην υπάρχει και καθόλου.

— Το DSC δύναται να περιέχει αναγνωριστικούς κωδικούς πολιτικής (εκτεταμένη χρήση κλειδιού), που αφορούν ειδικά τα πιστοποιητικά υγείας.

— Τα κράτη μέλη μπορούν να επιλέξουν να μην προβούν ποτέ σε επαλήθευση δημοσιοποιημένων ανακλήσεων· αντ' αυτού, μπορεί να βασίζονται αποκλειστικά και μόνο στους καταλόγους DSC που λαμβάνουν καθημερινά από τη γραμματεία ή τους οποίους καταρτίζουν οι ίδιοι.

([11]) rfc7517 (ietf.org).

ΠΑΡΑΡΤΗΜΑ II

ΚΑΝΟΝΕΣ ΓΙΑ ΤΗ ΣΥΜΠΛΗΡΩΣΗ ΤΩΝ ΣΤΟΙΧΕΙΩΝ ΣΤΟ ΨΗΦΙΑΚΟ ΠΙΣΤΟΠΟΙΗΤΙΚΟ COVID ΤΗΣ ΕΕ

Οι γενικοί κανόνες όσον αφορά τα σύνολα τιμών που καθορίζονται στο παρόν παράρτημα αποσκοπούν στη διασφάλιση της διαλειτουργικότητας σε σημασιολογικό επίπεδο και παρέχουν τη δυνατότητα ενιαίων τεχνικών εφαρμογών για το DCC. Τα στοιχεία που περιλαμβάνονται στο παρόν παράρτημα μπορούν να χρησιμοποιούνται για τις τρεις διαφορετικές ρυθμίσεις (εμβολιασμός/διαγνωστικός έλεγχος/ανάρρωση) που προβλέπονται στον κανονισμό (ΕΕ) 2021/953. Στο παρόν παράρτημα αναφέρονται μόνο στοιχεία που είναι αναγκαία για λόγους σημασιολογικής τυποποίησης μέσω κωδικοποιημένων συνόλων τιμών.

Τα κράτη μέλη είναι αρμόδια για τη μετάφραση των κωδικοποιημένων στοιχείων στην εθνική γλώσσα.

Για κάθε πεδίο δεδομένων που δεν αναφέρεται στις περιγραφές του συνόλου τιμών που παρατίθενται κατωτέρω, συνιστάται η κωδικοποίηση UTF-8 (ονοματεπώνυμο, κέντρο διαγνωστικού ελέγχου εξέτασης, εκδότης πιστοποιητικού). Συνιστάται η κωδικοποίηση των πεδίων δεδομένων που περιέχουν ημερολογιακές ημερομηνίες (ημερομηνία γέννησης, ημερομηνία εμβολιασμού, ημερομηνία συλλογής δείγματος διαγνωστικού ελέγχου, ημερομηνία πρώτου θετικού αποτελέσματος διαγνωστικού ελέγχου, ημερομηνίες ισχύος πιστοποιητικού) σύμφωνα με το πρότυπο ISO 8601.

Εάν, για οποιονδήποτε λόγο, δεν μπορούν να χρησιμοποιηθούν τα προτιμώμενα κωδικά συστήματα που αναφέρονται κατωτέρω, παρέχεται η δυνατότητα χρήσης άλλων διεθνών κωδικών συστημάτων και θα πρέπει να παρέχονται συμβουλές σχετικά με τον τρόπο αντιστοίχισης των κωδικών του άλλου κωδικού συστήματος με το προτιμώμενο κωδικό σύστημα. Σε εξαιρετικές περιπτώσεις είναι δυνατή η χρήση κειμένου (εμφάνιση ονομάτων) ως μηχανισμού δημιουργίας αντιγράφων ασφαλείας όταν δεν υπάρχει κατάλληλος κωδικός στα καθορισμένα σύνολα τιμών.

Τα κράτη μέλη που χρησιμοποιούν άλλη κωδικοποίηση στα συστήματά τους θα πρέπει να προβαίνουν σε αντιστοίχιση των εν λόγω κωδικών με τα περιγραφόμενα σύνολα τιμών. Τα κράτη μέλη είναι αρμόδια για τις εν λόγω αντιστοιχίσεις.

Η Επιτροπή ενημερώνει τα σύνολα τιμών ανά τακτά χρονικά διαστήματα με την υποστήριξη του δικτύου eHealth και της Επιτροπής Υγειονομικής Ασφάλειας. Τα ενημερωμένα σύνολα τιμών δημοσιεύονται στον αντίστοιχο ιστότοπο της Επιτροπής, καθώς και στην ιστοσελίδα του δικτύου eHealth. Θα πρέπει να παρέχεται ιστορικό των αλλαγών.

1. **Στοχευόμενη νόσος ή στοχευόμενος παράγοντας/νόσος ή νοσογόνος παράγοντας από τον οποίο έχει αναρρώσει ο κάτοχος: COVID-19 (SARS-CoV-2 ή μία από τις παραλλαγές του)**

   Προτιμώμενο κωδικό σύστημα: SNOMED CT.

   Πρέπει να χρησιμοποιείται στα πιστοποιητικά 1, 2 και 3.

   Οι επιλεγμένοι κωδικοί παραπέμπουν στη νόσο COVID-19 ή, εάν απαιτούνται λεπτομερέστερες πληροφορίες για τη γενετική παραλλαγή του SARS-CoV-2, στις εν λόγω παραλλαγές, σε περίπτωση που οι συγκεκριμένες λεπτομερείς πληροφορίες είναι αναγκαίες για επιδημιολογικούς λόγους.

   Παράδειγμα κωδικού που θα πρέπει να χρησιμοποιείται αποτελεί ο κωδικός SNOMED CT 840539006 (COVID-19).

2. **Εμβόλιο ή προφυλακτική αγωγή κατά της COVID-19**

   Προτιμώμενο κωδικό σύστημα: SNOMED CT ή ταξινόμηση ATC.

   Πρέπει να χρησιμοποιείται στο πιστοποιητικό 1.

   Παραδείγματα κωδικών που θα πρέπει να χρησιμοποιούνται από τα προτιμώμενα κωδικά συστήματα αποτελούν οι εξής κωδικοί: SNOMED CT 1119305005 (εμβόλιο αντιγόνου κατά του ιού SARS-CoV-2), 1119349007 (εμβόλιο mRNA κατά του ιού SARS-CoV-2) ή J07BX03 (εμβόλια κατά της νόσου COVID-19). Το σύνολο τιμών θα πρέπει να επεκτείνεται όταν αναπτύσσονται και χρησιμοποιούνται νέοι τύποι εμβολίων.

3. **Σκεύασμα εμβολίου κατά της COVID-19**

   Προτιμώμενα κωδικά συστήματα (κατά σειρά προτίμησης):

   — Ενωσιακό μητρώο σκευασμάτων εμβολίου με άδεια κυκλοφορίας σε όλη την ΕΕ (αριθμοί άδειας)

   — Παγκόσμιο μητρώο εμβολίων, όπως το μητρώο που θα μπορούσε να δημιουργήσει ο Παγκόσμιος Οργανισμός Υγείας

   — Ονομασία του σκευάσματος εμβολίου σε άλλες περιπτώσεις. Εάν η ονομασία περιλαμβάνει κενά διαστήματα, θα πρέπει να αντικαθίστανται με ενωτικό (-).

Ονομασία του συνόλου τιμών: Εμβόλιο.

Πρέπει να χρησιμοποιείται στο πιστοποιητικό 1.

Παράδειγμα κωδικού που θα πρέπει να χρησιμοποιείται από τα προτιμώμενα κωδικά συστήματα αποτελεί ο κωδικός EU/1/20/1528 (Comirnaty). Παράδειγμα με την ονομασία του εμβολίου που πρέπει να χρησιμοποιείται ως κωδικός: Sputnik-V (αντιστοιχεί στο εμβόλιο Sputnik V).

4. **Κάτοχος άδειας κυκλοφορίας ή κατασκευαστής του εμβολίου κατά της COVID-19**

Προτιμώμενο κωδικό σύστημα:

— Κωδικός οργανισμού από τον EMA (σύστημα SPOR για το πρότυπο ISO IDMP)

— Παγκόσμιο μητρώο κατόχων άδειας κυκλοφορίας ή κατασκευαστών του εμβολίου, όπως το μητρώο που θα μπορούσε να δημιουργήσει ο Παγκόσμιος Οργανισμός Υγείας

— Ονομασία οργανισμού σε άλλες περιπτώσεις. Εάν η ονομασία περιλαμβάνει κενά διαστήματα, θα πρέπει να αντικαθίστανται με ενωτικό (-).

Πρέπει να χρησιμοποιείται στο πιστοποιητικό 1.

Παράδειγμα κωδικού που θα πρέπει να χρησιμοποιείται από το προτιμώμενο κωδικό σύστημα αποτελεί ο κωδικός ORG-100001699 (AstraZeneca AB). Παράδειγμα με την ονομασία του οργανισμού που πρέπει να χρησιμοποιείται ως κωδικός: Sinovac-Biotech (αντιστοιχεί στο εμβόλιο Sinovac Biotech).

5. **Αριθμός σε σειρά δόσεων, καθώς και συνολικός αριθμός δόσεων της σειράς**

Πρέπει να χρησιμοποιείται στο πιστοποιητικό 1.

Δύο πεδία:

(1) Αριθμός χορηγούμενων δόσεων σε έναν κύκλο

(2) Αριθμός αναμενόμενων δόσεων για έναν πλήρη κύκλο (συγκεκριμένος για ένα άτομο κατά τον χρόνο χορήγησης)

Για παράδειγμα, 1/1, 2/2 θα παρουσιάζονται ως ολοκληρωμένες· συμπεριλαμβανομένης της επιλογής 1/1 για εμβόλια που περιλαμβάνουν δύο δόσεις, για τα οποία όμως το πρωτόκολλο που εφαρμόζουν τα κράτη μέλη αναφέρει ότι πρέπει να χορηγείται μία δόση σε πολίτες που είχαν διαγνωστεί με την COVID-19 πριν από τον εμβολιασμό. Ο συνολικός αριθμός δόσεων της σειράς θα πρέπει να αναφέρεται σύμφωνα με τις πληροφορίες που παρέχονται κατά τον χρόνο χορήγησης της δόσης. Για παράδειγμα, εάν για ένα συγκεκριμένο εμβόλιο απαιτείται τρίτη δόση (ενισχυτική) κατά τον χρόνο χορήγησης της τελευταίας δόσης, ο αριθμός στο δεύτερο πεδίο αντιστοιχεί στην περίπτωση αυτή (π.χ. 2/3, 3/3 κ.λπ.).

6. **Κράτος μέλος ή τρίτη χώρα όπου χορηγήθηκε το εμβόλιο/διενεργήθηκε ο διαγνωστικός έλεγχος**

Προτιμώμενο κωδικό σύστημα: Κωδικοί χωρών ISO 3166.

Πρέπει να χρησιμοποιείται στα πιστοποιητικά 1, 2 και 3

Περιεχόμενο συνόλου τιμών: ο πλήρης κατάλογος κωδικών 2 γραμμάτων που είναι διαθέσιμος ως σύνολο τιμών το οποίο ορίζεται στο πρότυπο FHIR (http://hl7.org/fhir/ValueSet/iso3166-1-2

7. **Τύπος διαγνωστικού ελέγχου**

Προτιμώμενο κωδικό σύστημα: LOINC.

Πρέπει να χρησιμοποιείται στο πιστοποιητικό 2 και στο πιστοποιητικό 3, εάν η στήριξη για την έκδοση πιστοποιητικών ανάκτησης με βάση άλλους τύπους διαγνωστικού ελέγχου εκτός του διαγνωστικού ελέγχου NAAT θεσπίζεται μέσω κατ' εξουσιοδότηση πράξης.

Οι κωδικοί που περιλαμβάνονται σε αυτό το σύνολο τιμών παραπέμπουν στη μέθοδο του διαγνωστικού ελέγχου και επιλέγονται τουλάχιστον για τον διαχωρισμό των διαγνωστικών ελέγχων NAAT από τους διαγνωστικούς ελέγχους RAT όπως αναφέρεται στον κανονισμό (ΕΕ) 2021/953.

Παράδειγμα κωδικού που θα πρέπει να χρησιμοποιείται από το προτιμώμενο κωδικό σύστημα αποτελεί ο κωδικός LP217198-3 (ταχεία ανοσολογική δοκιμασία).

8. **Κατασκευαστής και εμπορική ονομασία του διαγνωστικού ελέγχου που χρησιμοποιήθηκε (προαιρετικά για τον διαγνωστικό έλεγχο NAAT)**

Προτιμώμενο κωδικό σύστημα: Κατάλογος ταχειών δοκιμασιών αντιγόνων της Επιτροπής Υγειονομικής Ασφάλειας (HSC), όπως τηρείται από το JRC (βάση δεδομένων για τις in vitro διαγνωστικές συσκευές και τις μεθόδους δοκιμών για τη νόσο COVID-19).

Πρέπει να χρησιμοποιείται στο πιστοποιητικό 2.

Στο περιεχόμενο του συνόλου τιμών περιλαμβάνεται η επιλογή των ταχειών δοκιμασιών αντιγόνων, όπως αναφέρονται στον κοινό και ενημερωμένο κατάλογο ταχειών δοκιμασιών αντιγόνων για τη νόσο COVID-19, που θεσπίστηκε βάσει της σύστασης 2021/C 24/01 του Συμβουλίου και συμφωνήθηκε στο πλαίσιο της Επιτροπής Υγειονομικής Ασφάλειας. Ο κατάλογος τηρείται από το JRC στη βάση δεδομένων για τις in vitro διαγνωστικές συσκευές και τις μεθόδους δοκιμών για τη νόσο COVID-19, στην ακόλουθη διεύθυνση: https://covid-19-diagnostics.jrc.ec.europa.eu/devices/hsc-common-recognition-rat

Για το συγκεκριμένο κωδικό σύστημα χρησιμοποιούνται τα σχετικά πεδία, όπως το αναγνωριστικό της διαγνωστικής συσκευής, η ονομασία της δοκιμής και του κατασκευαστή, σύμφωνα με τον δομημένο μορφότυπο του JRC που είναι διαθέσιμος στην ακόλουθη διεύθυνση: https://covid-19-diagnostics.jrc.ec.europa.eu/devices

9. **Αποτέλεσμα του διαγνωστικού ελέγχου**

Προτιμώμενο κωδικό σύστημα: SNOMED CT.

Πρέπει να χρησιμοποιείται στο πιστοποιητικό 2.

Οι κωδικοί που επιλέγονται παρέχουν τη δυνατότητα διάκρισης μεταξύ των θετικών και των αρνητικών αποτελεσμάτων του διαγνωστικού ελέγχου (είτε ανιχνεύονται είτε όχι). Παρέχεται η δυνατότητα προσθήκης επιπλέον τιμών (όπως οι μη προσδιοριζόμενες), εάν αυτό απαιτείται βάσει των περιπτώσεων χρήσης.

Παραδείγματα κωδικών που θα πρέπει να χρησιμοποιούνται από τα προτιμώμενα κωδικά συστήματα αποτελούν οι κωδικοί 260415000 (μη ανιχνεύσιμο) και 260373001 (ανιχνεύσιμο).

ΠΑΡΑΡΤΗΜΑ III

ΚΟΙΝΗ ΔΟΜΗ ΤΟΥ ΜΟΝΑΔΙΚΟΥ ΑΝΑΓΝΩΡΙΣΤΙΚΟΥ ΚΩΔΙΚΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ

1. **Εισαγωγή**

Κάθε Ψηφιακό Πιστοποιητικό COVID της ΕΕ (DCC) περιλαμβάνει έναν μοναδικό αναγνωριστικό κωδικό πιστοποιητικού (unique certificate identifier, UCI), με το οποίο υποστηρίζεται η διαλειτουργικότητα των εν λόγω πιστοποιητικών. Το UCI μπορεί να χρησιμοποιείται για την επαλήθευση του πιστοποιητικού. Τα κράτη μέλη είναι αρμόδια για την εφαρμογή του UCI. Το UCI αποτελεί μέσο για την επαλήθευση της ακρίβειας του πιστοποιητικού και, κατά περίπτωση, για τη σύνδεση του πιστοποιητικού με σύστημα καταχώρισης (για παράδειγμα, σύστημα IIS). Οι εν λόγω αναγνωριστικοί κωδικοί δίνουν επίσης τη δυνατότητα στα κράτη μέλη να επιβεβαιώνουν (σε έντυπη και ψηφιακή μορφή) ότι τα άτομα έχουν εμβολιαστεί ή έχουν υποβληθεί σε διαγνωστικό έλεγχο.

2. **Σύνθεση του μοναδικού αναγνωριστικού κωδικού πιστοποιητικού**

Το UCI ακολουθεί κοινή δομή και μορφότυπο που διευκολύνει τη δυνατότητα ερμηνείας των πληροφοριών από τον άνθρωπο ή με μηχανικά μέσα και ενδέχεται να συνδέεται με στοιχεία όπως το κράτος μέλος του εμβολιασμού, το εμβόλιο αυτό καθαυτό και τον ειδικό αναγνωριστικό κωδικό κράτους μέλους. Εξασφαλίζει στα κράτη μέλη την ευελιξία να μορφοποιούν τα εν λόγω στοιχεία, τηρώντας πλήρως τη νομοθεσία για την προστασία δεδομένων. Η σειρά των χωριστών στοιχείων ακολουθεί καθορισμένη ιεραρχία, η οποία παρέχει τη δυνατότητα μελλοντικών τροποποιήσεων των τμημάτων, με τη διατήρηση ταυτόχρονα της δομικής ακεραιότητα της σύνθεσης.

Οι πιθανές λύσεις για τη σύνθεση του UCI διαμορφώνουν ένα φάσμα, στο οποίο η δομοστοιχείωση και η δυνατότητα ερμηνείας από τον άνθρωπο αποτελούν τις δύο βασικές διαφοροποιημένες παραμέτρους και ένα θεμελιώδες χαρακτηριστικό:

— Δομοστοιχείωση: ο βαθμός στον οποίο ο κωδικός αποτελείται από διακριτά τμήματα δόμησης που περιέχουν διαφορετικές πληροφορίες σε σημασιολογικό επίπεδο.

— Δυνατότητα ερμηνείας από τον άνθρωπο: ο βαθμός στον οποίο ο κωδικός βγάζει κάποιο νόημα ή μπορεί να ερμηνευτεί από τον άνθρωπο αναγνώστη.

— Παγκόσμια μοναδικός: ο αναγνωριστικός κωδικός χώρας ή αρχής αποτελεί αντικείμενο ορθής διαχείρισης· και κάθε χώρα (αρχή) αναμένεται να διαχειρίζεται με ορθό τρόπο το τμήμα του χώρου ονομάτων που της αναλογεί, χωρίς ποτέ να ανακυκλώνει ή να επανεκδίδει αναγνωριστικούς κωδικούς. Ο συνδυασμός των στοιχείων αυτών συνιστά διασφάλιση ώστε κάθε αναγνωριστικός κωδικός να είναι παγκόσμια μοναδικός.

3. **Γενικές απαιτήσεις**

Θα πρέπει να πληρούνται οι ακόλουθες γενικές απαιτήσεις σε σχέση με το UCI:

(1) Σύνολο χαρακτήρων: επιτρέπονται μόνο κεφαλαίοι αλφαριθμητικοί χαρακτήρες του κώδικα US-ASCII («A» έως «Z», «0» έως «9»)· επιτρέπονται επιπλέον ειδικοί χαρακτήρες για τον διαχωρισμό από το RFC 3986 [1] [2], δηλαδή {«/»,«#»,«:»}·

(2) μέγιστο μήκος: οι σχεδιαστές θα πρέπει να στοχεύουν σε μήκος 27-30 χαρακτήρων [3]·

(3) πρόθεμα έκδοσης: αναφέρεται στην έκδοση του σχήματος UCI. Το πρόθεμα έκδοσης είναι «01» για την παρούσα έκδοση του εγγράφου· το πρόθεμα έκδοσης αποτελείται από δύο ψηφία·

(4) πρόθεμα χώρας: ο κωδικός χώρας καθορίζεται από το πρότυπο ISO 3166-1. Μεγαλύτεροι κωδικοί [π.χ. άνω των 3 χαρακτήρων (για παράδειγμα «UNHCR»)] προορίζονται για μελλοντική χρήση·

(5) κωδικός επιθήματος/άθροισμα ελέγχου:

5.1. Τα κράτη μέλη θα πρέπει να χρησιμοποιούν άθροισμα ελέγχου σε περίπτωση πιθανής διαβίβασης, μεταγραφής (από άνθρωπο) ή άλλων αλλοιώσεων (δηλαδή όταν γίνεται χρήση έντυπης μορφής).

5.2. Για την επικύρωση του πιστοποιητικού δεν πρέπει να βασίζονται στο άθροισμα ελέγχου, το οποίο, από τεχνικής άποψης, δεν αποτελεί μέρος του αναγνωριστικού κωδικού, αλλά χρησιμοποιείται για την επαλήθευση της ακεραιότητας του κωδικού. Το άθροισμα ελέγχου θα πρέπει να είναι η σύνοψη του ISO-7812-1 (LUHN-10) [4] για ολόκληρο το UCI σε ψηφιακό/ενσύρματο μορφότυπο μεταφοράς. Το άθροισμα ελέγχου χωρίζεται από το υπόλοιπο UCI με τον χαρακτήρα «#».

---

[1] rfc3986 (ietf.org).

[2] Πεδία όπως το φύλο, ο αριθμός δέσμης/παρτίδας, το κέντρο χορήγησης, η ταυτοποίηση επαγγελματία υγείας, η ημερομηνία επόμενου εμβολιασμού μπορεί να απαιτούνται μόνο για ιατρικούς σκοπούς.

[3] Για την εφαρμογή με κωδικούς QR, τα κράτη μέλη θα μπορούσαν να εξετάσουν το ενδεχόμενο εισαγωγής ενός επιπλέον συνόλου χαρακτήρων, συνολικού μήκους έως 72 χαρακτήρων (συμπεριλαμβανομένου του μήκους των 27-30 χαρακτήρων του ίδιου του αναγνωριστικού κωδικού), το οποίο θα μπορούσε να χρησιμοποιείται για τη διαβίβαση άλλων πληροφοριών. Ο καθορισμός της προδιαγραφής για τις εν λόγω πληροφορίες συνιστά αρμοδιότητα των κρατών μελών.

[4] Ο αλγόριθμος «Luhn mod N» αποτελεί επέκταση του αλγόριθμου Luhn (επίσης γνωστός ως αλγόριθμος «mod 10»), ο οποίος λειτουργεί με αριθμητικούς κωδικούς και χρησιμοποιείται, π.χ., για τον υπολογισμό του αθροίσματος ελέγχου των πιστωτικών καρτών. Η επέκταση επιτρέπει στον αλγόριθμο να λειτουργεί με ακολουθίες τιμών σε οποιαδήποτε βάση (στην προκειμένη περίπτωση με χαρακτήρες «alpha»).

Θα πρέπει να διασφαλίζεται οπισθόδρομη συμβατότητα: κράτη μέλη τα οποία με την πάροδο του χρόνου, αλλάζουν τη δομή των αναγνωριστικών κωδικών τους (εντός της κύριας έκδοσης, η οποία ορίζεται επί του παρόντος ως «v1») πρέπει να διασφαλίζουν ότι δύο αναγνωριστικοί κωδικοί που είναι πανομοιότυποι αναπαριστούν το ίδιο πιστοποιητικό/βεβαίωση εμβολιασμού. Ή, με άλλα λόγια, τα κράτη μέλη δεν μπορούν να ανακυκλώνουν τους αναγνωριστικούς κωδικούς.

4. **Επιλογές όσον αφορά τους μοναδικούς αναγνωριστικούς κωδικούς πιστοποιητικού για πιστοποιητικά εμβολιασμού**

Οι κατευθυντήριες γραμμές του δικτύου eHealth σχετικά με τα επαληθεύσιμα πιστοποιητικά εμβολιασμού και τα βασικά στοιχεία διαλειτουργικότητας ([5]) παρέχουν διάφορες επιλογές που είναι διαθέσιμες στα κράτη μέλη και άλλες οντότητες και οι οποίες μπορούν να συνυπάρχουν μεταξύ των διαφόρων κρατών μελών. Τα κράτη μέλη μπορούν να χρησιμοποιούν τις εν λόγω επιλογές σε διαφορετική έκδοση του σχήματος UCI.

([5]) https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf

ΠΑΡΑΡΤΗΜΑ IV

ΔΙΑΧΕΙΡΙΣΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ

1. **Εισαγωγή**

Η ασφαλής και αξιόπιστη ανταλλαγή των κλειδιών υπογραφής για Ψηφιακά Πιστοποιητικά COVID της ΕΕ (DCC) μεταξύ των κρατών μελών πραγματοποιείται μέσω της πύλης Ψηφιακού Πιστοποιητικού COVID της ΕΕ (DCCG), η οποία λειτουργεί ως κεντρικό αποθετήριο για τα δημόσια κλειδιά. Με την DCCG, τα κράτη μέλη έχουν την εξουσία να δημοσιεύουν τα δημόσια κλειδιά που αντιστοιχούν στα ιδιωτικά κλειδιά τα οποία χρησιμοποιούνται για την υπογραφή ψηφιακών πιστοποιητικών COVID. Τα κράτη μέλη που βασίζονται στην υπηρεσία μπορούν να χρησιμοποιούν την DCCG για να λαμβάνουν εγκαίρως επικαιροποιημένο υλικό δημόσιου κλειδιού. Σε μεταγενέστερο στάδιο είναι δυνατή η επέκταση της DCCG στην ανταλλαγή αξιόπιστων συμπληρωματικών πληροφοριών που παρέχουν τα κράτη μέλη, όπως κανόνες επικύρωσης των DCC. Το μοντέλο εμπιστοσύνης για το πλαίσιο του DCC είναι υποδομή δημόσιου κλειδιού (Public Key Infrastructure, PKI). Κάθε κράτος μέλος διαθέτει μία ή περισσότερες εθνικές αρχές πιστοποίησης (CSCA), τα πιστοποιητικά των οποίων είναι σχετικά μακράς διάρκειας. Με απόφαση του κράτους μέλους, η CSCA μπορεί να είναι η ίδια ή διαφορετική από τη CSCA που χρησιμοποιείται για μηχανικώς αναγνώσιμα ταξιδιωτικά έγγραφα. Η CSCA εκδίδει πιστοποιητικά δημόσιου κλειδιού για τους υπογράφοντες εθνικά, σύντομης διάρκειας, έγγραφα (π.χ. υπογράφοντες για DCC), τα οποία ονομάζονται πιστοποιητικά του υπογράφοντος το έγγραφο (DSC). Η CSCA ενεργεί ως άγκυρα εμπιστοσύνης, ώστε τα κράτη μέλη που εμπιστεύονται την αρχή να μπορούν να χρησιμοποιούν το πιστοποιητικό CSCA για την επικύρωση της γνησιότητας και της ακεραιότητας των DSC που αλλάζουν ανά τακτά χρονικά διαστήματα. Αφού ολοκληρωθεί η επικύρωση, τα κράτη μέλη μπορούν να παρέχουν τα εν λόγω πιστοποιητικά (ή μόνο τα δημόσια κλειδιά που περιέχονται σε αυτά) στις εφαρμογές που διαθέτουν για την επικύρωση του DCC. Εκτός από τα πιστοποιητικά CSCA και DSC, η DCCG βασίζεται επίσης στην υποδομή δημόσιου κλειδιού για τον έλεγχο ταυτότητας των συναλλαγών, των δεδομένων υπογραφής, ως βάση για την απόδειξη της ταυτότητας και ως μέσο για τη διασφάλιση της ακεραιότητας των διαύλων επικοινωνίας μεταξύ των κρατών μελών και της DCCG.

Οι ψηφιακές υπογραφές μπορούν να χρησιμοποιούνται για τη διασφάλιση της ακεραιότητας και της γνησιότητας των δεδομένων. Οι υποδομές δημόσιων κλειδιών δημιουργούν κλίμα εμπιστοσύνης μέσω της σύνδεσης των δημόσιων κλειδιών με επαληθευμένες ταυτότητες (ή εκδότες). Αυτό είναι απαραίτητο διότι δίνεται η δυνατότητα σε άλλους συμμετέχοντες να επαληθεύουν την προέλευση των δεδομένων και την ταυτότητα του εταίρου επικοινωνίας, και να λαμβάνουν αποφάσεις ως προς την εμπιστοσύνη. Στην DCCG χρησιμοποιούνται πολλαπλά πιστοποιητικά δημόσιου κλειδιού για λόγους γνησιότητας. Στο παρόν παράρτημα καθορίζονται τα πιστοποιητικά δημόσιου κλειδιού που χρησιμοποιούνται, καθώς και ο τρόπος με τον οποίο σχεδιάζονται ώστε να εξασφαλίζεται η δυνατότητα ευρείας διαλειτουργικότητας μεταξύ των κρατών μελών. Περιλαμβάνει περισσότερες λεπτομέρειες σχετικά με τα αναγκαία πιστοποιητικά δημόσιου κλειδιού και παρέχει καθοδήγηση σχετικά με τα υποδείγματα πιστοποιητικών και τις περιόδους ισχύος για τα κράτη μέλη που επιθυμούν να διαχειρίζονται τη δική τους CSCA. Δεδομένου ότι τα DCC είναι επαληθεύσιμα για ορισμένο χρονικό διάστημα (το οποίο ξεκινά από την έκδοση του πιστοποιητικού και λήγει μετά την παρέλευση ορισμένης προθεσμίας), είναι αναγκαίο να καθοριστεί μοντέλο επαλήθευσης για όλες τις υπογραφές που εφαρμόζονται στα πιστοποιητικά δημόσιου κλειδιού και στα DCC.

2. **Ορολογία**

Ο πίνακας που ακολουθεί περιέχει τις συντομεύσεις και την ορολογία που χρησιμοποιούνται σε ολόκληρο το παράρτημα.

Όρος	Ορισμός
Πιστοποιητικό	Ή πιστοποιητικό δημόσιου κλειδιού. Πιστοποιητικό X.509 v3 που περιέχει το δημόσιο κλειδί μιας οντότητας
CSCA	Εθνική αρχή πιστοποίησης
DCC	Ψηφιακό Πιστοποιητικό COVID της ΕΕ. Υπογεγραμμένο ψηφιακό έγγραφο το οποίο περιέχει πληροφορίες εμβολιασμού, διαγνωστικού ελέγχου ή ανάρρωσης.
DCCG	Πύλη Ψηφιακού Πιστοποιητικού COVID της ΕΕ. Το εν λόγω σύστημα χρησιμοποιείται για την ανταλλαγή DSC μεταξύ των κρατών μελών.
$DCCG_{TA}$	Το πιστοποιητικό άγκυρας εμπιστοσύνης της DCCG. Το αντίστοιχο ιδιωτικό κλειδί χρησιμοποιείται για την υπογραφή του καταλόγου όλων των πιστοποιητικών CSCA εκτός σύνδεσης.
$DCCG_{TLS}$	Το πιστοποιητικό διακομιστή TLS της DCCG
DSC	Πιστοποιητικό υπογράφοντος εγγράφου. Το πιστοποιητικό δημόσιου κλειδιού της αρχής του κράτους μέλους που υπογράφει το έγγραφο (για παράδειγμα, επιτρεπόμενο σύστημα για την υπογραφή των DCC). Το εν λόγω πιστοποιητικό εκδίδεται από τη CSCA του κράτους μέλους.
EC-DSA	Αλγόριθμος ελλειπτικής καμπύλης ψηφιακής υπογραφής. Αλγόριθμος κρυπτογράφησης υπογραφής βάσει ελλειπτικών καμπυλών
Κράτος μέλος	Κράτος μέλος της Ευρωπαϊκής Ένωσης

Όρος	Ορισμός
mTLS	Αμοιβαίο TLS. Το πρωτόκολλο ασφάλειας επιπέδου μεταφοράς με αμοιβαίο έλεγχο ταυτότητας
Σημείωση	Εθνικό σύστημα λειτουργιών παρασκηνίου
NB_{CSCA}	Το πιστοποιητικό CSCA κράτους μέλους (θα μπορούσε να είναι περισσότερα του ενός)
NB_{TLS}	Το πιστοποιητικό ελέγχου ταυτότητας πελάτη μέσω TLS από εθνικό σύστημα λειτουργιών παρασκηνίου
NB_{UP}	Το πιστοποιητικό που χρησιμοποιεί ένα εθνικό σύστημα λειτουργιών παρασκηνίου για την υπογραφή πακέτων δεδομένων που μεταφορτώνονται στην DCCG
PKI	Υποδομή δημόσιου κλειδιού Μοντέλο εμπιστοσύνης που βασίζεται σε πιστοποιητικά δημόσιου κλειδιού και σε αρχές πιστοποίησης
RSA	Ασύμμετρος κρυπτογραφικός αλγόριθμος που βασίζεται στην παραγοντοποίηση του ακεραίου που χρησιμοποιείται για τις ψηφιακές υπογραφές ή την ασύμμετρη κρυπτογράφηση.

3. **Ροές επικοινωνίας και υπηρεσίες ασφάλειας της DCCG**

Στο παρόν τμήμα παρέχεται επισκόπηση των ροών επικοινωνίας και των υπηρεσιών ασφάλειας στο σύστημα της DCCG. Ορίζονται επίσης τα κλειδιά και τα πιστοποιητικά που χρησιμοποιούνται για την ασφάλεια της επικοινωνίας, των πληροφοριών που μεταφορτώνονται και των DCC, καθώς και υπογεγραμμένος κατάλογος εμπιστοσύνης, στον οποίο περιέχονται όλα τα πιστοποιητικά CSCA που έχουν καταχωριστεί. Η DCCG λειτουργεί ως κόμβος δεδομένων που παρέχει στα κράτη μέλη τη δυνατότητα ανταλλαγής υπογεγραμμένων πακέτων δεδομένων.

Τα μεταφορτωμένα πακέτα δεδομένων παρέχονται από την DCCG «ως έχουν», δηλαδή η DCCG δεν προσθέτει ούτε διαγράφει DSC από τα πακέτα που λαμβάνει. Το εθνικό σύστημα λειτουργιών παρασκηνίου (National Backend, NB) των κρατών μελών έχει τη δυνατότητα να επαληθεύει την ακεραιότητα και τη γνησιότητα των μεταφορτωμένων δεδομένων από τερματικό σε τερματικό. Επιπλέον, τα εθνικά συστήματα λειτουργιών παρασκηνίου και η DCCG θα χρησιμοποιούν τον αμοιβαίο έλεγχο ταυτότητας μέσω TLS για τη δημιουργία ασφαλούς σύνδεσης. Η λειτουργία αυτή προστίθεται στις υπογραφές κατά την ανταλλαγή δεδομένων.

3.1. *Επαλήθευση ταυτότητας και δημιουργία σύνδεσης*

Η DCCG χρησιμοποιεί το πρωτόκολλο ασφάλειας επιπέδου μεταφοράς (Transport Layer Security, TLS) με αμοιβαίο έλεγχο ταυτότητας για τη δημιουργία κρυπτογραφημένου διαύλου με έλεγχο ταυτότητας μεταξύ των εθνικών συστημάτων λειτουργιών παρασκηνίου (NB) του κράτους μέλους και του περιβάλλοντος της πύλης. Κατά συνέπεια, η DCCG διαθέτει πιστοποιητικό διακομιστή TLS, σε συντομογραφία «$DCCG_{TLS}$», και το εθνικό σύστημα λειτουργιών παρασκηνίου διαθέτει πιστοποιητικό πελάτη TLS, σε συντομογραφία NB_{TLS}. Υποδείγματα πιστοποιητικών περιλαμβάνονται στο *τμήμα 5*. Κάθε εθνικό σύστημα λειτουργιών παρασκηνίου μπορεί να παρέχει το δικό του πιστοποιητικό TLS. Το εν λόγω πιστοποιητικό θα περιλαμβάνεται ρητά στη λευκή λίστα και μπορεί, συνεπώς, να εκδίδεται από δημοσίως έμπιστη αρχή πιστοποίησης (για παράδειγμα, από αρχή πιστοποίησης που τηρεί τις βασικές απαιτήσεις του φόρουμ «CA Browser»), από εθνική αρχή πιστοποίησης ή μπορεί να είναι αυθυπόγραφο. Κάθε κράτος μέλος είναι αρμόδιο για τα εθνικά δεδομένα του και την προστασία του ιδιωτικού κλειδιού που χρησιμοποιείται για τη δημιουργία της σύνδεσης με την DCCG. Η προσέγγιση «Χρήση οικείου πιστοποιητικού» («Bring your own certificate») προϋποθέτει άρτια καθορισμένη διαδικασία καταχώρισης και ταυτοποίησης, καθώς και διαδικασίες ανάκλησης και ανανέωσης, όπως αναφέρονται στα *τμήματα 4.1, 4.2* και *4.3*. Η DCCG χρησιμοποιεί τη λευκή λίστα (κατάλογο εγκεκριμένων πιστοποιητικών), στην οποίο προστίθενται τα πιστοποιητικά TLS των εθνικών συστημάτων λειτουργιών παρασκηνίου μετά την επιτυχή καταχώρισή τους. Μόνο τα εθνικά συστήματα λειτουργιών παρασκηνίου που διενεργούν τα ίδια τον έλεγχο ταυτότητας με ιδιωτικό κλειδί που αντιστοιχεί σε πιστοποιητικό από τη λευκή λίστα μπορούν να δημιουργήσουν ασφαλή σύνδεση με την DCCG. Η DCCG θα χρησιμοποιεί, επίσης, πιστοποιητικό TLS που δίνει τη δυνατότητα στα εθνικά συστήματα λειτουργιών παρασκηνίου να επαληθεύουν ότι δημιουργείται όντως σύνδεση με την «πραγματική» DCCG και όχι με κάποια κακόβουλη οντότητα που εμφανίζεται ως DCCG. Το πιστοποιητικό της DCCG θα παρέχεται στα εθνικά συστήματα λειτουργιών παρασκηνίου μετά την επιτυχή καταχώριση. Το πιστοποιητικό $DCCG_{TLS}$ θα εκδίδεται από δημοσίως έμπιστη αρχή πιστοποίησης (CA) (η οποία περιλαμβάνεται σε όλα τα βασικά προγράμματα περιήγησης). Τα κράτη μέλη είναι αρμόδια να επαληθεύουν ότι η σύνδεσή τους με την DCCG είναι ασφαλής (για παράδειγμα, με έλεγχο του αποτυπώματος του πιστοποιητικού $DCCG_{TLS}$ του συνδεδεμένου διακομιστή έναντι του αποτυπώματος που παρέχεται μετά την καταχώριση).

3.2. *Εθνικές αρχές πιστοποίησης και μοντέλο επικύρωσης*

Τα κράτη μέλη που εντάσσονται στο πλαίσιο της DCCG πρέπει να χρησιμοποιούν τις εθνικές αρχές πιστοποίησης (CSCA) για την έκδοση των DSC. Τα κράτη μέλη ενδέχεται να έχουν περισσότερες από μία CSCA (για παράδειγμα, σε περίπτωση διοικητικής αποκέντρωσης σε επίπεδο περιφερειών). Κάθε κράτος μέλος μπορεί είτε να χρησιμοποιεί υφιστάμενες αρχές πιστοποίησης είτε να ιδρύσει ειδική (πιθανώς αυθυπόγραφη) αρχή πιστοποίησης για το σύστημα του DCC.

Τα κράτη μέλη πρέπει να υποβάλλουν τα πιστοποιητικά CSCA στον χειριστή της DCCG κατά τη διάρκεια της επίσημης διαδικασίας καταχώρισης. Μετά την επιτυχή καταχώριση του κράτους μέλους (*βλέπε τμήμα 4.1 για περισσότερες λεπτομέρειες*), ο χειριστής της DCCG θα επικαιροποιεί τον υπογεγραμμένο κατάλογο εμπιστοσύνης, στον οποίο περιέχονται όλα τα πιστοποιητικά CSCA που είναι ενεργά στο πλαίσιο του DCC. Ο διαχειριστής της DCCG θα χρησιμοποιεί ένα ειδικό ασύμμετρο ζεύγος κλειδιών για την υπογραφή του καταλόγου εμπιστοσύνης σε περιβάλλον εκτός σύνδεσης. Το ιδιωτικό κλειδί δεν θα αποθηκεύεται στο επιγραμμικό σύστημα της DCCG, ώστε, σε περίπτωση που το επιγραμμικό σύστημα εκτεθεί σε κίνδυνο, ο εισβολέας να μην μπορεί να παραβιάσει τον κατάλογο εμπιστοσύνης. Το αντίστοιχο πιστοποιητικό άγκυρας εμπιστοσύνης $DCCG_{TA}$ θα παρέχεται στα εθνικά συστήματα λειτουργιών παρασκηνίου κατά τη διάρκεια της διαδικασίας καταχώρισης.

Τα κράτη μέλη μπορούν να ανακτούν τον κατάλογο εμπιστοσύνης από την DCCG για τις οικείες διαδικασίες επαλήθευσης. Η CSCA ορίζεται ως η αρχή πιστοποίησης που εκδίδει τα DSC και, συνεπώς, τα κράτη μέλη που χρησιμοποιούν πολυεπίπεδη ιεραρχία αρχών πιστοποίησης [για παράδειγμα, αρχή CA ρίζας (Root CA) -> CSCA -> DSC] πρέπει να παρέχουν την υφιστάμενη αρχή πιστοποίησης που εκδίδει τα DSC. Στην περίπτωση αυτή, εάν το κράτος μέλος χρησιμοποιεί υφιστάμενη αρχή πιστοποίησης, τότε το σύστημα του DCC θα αγνοεί οποιαδήποτε αρχή είναι ανώτερη από τη CSCA και θα καταχωρίζει μόνο τη CSCA στη λευκή λίστα ως άγκυρα εμπιστοσύνης (παρόλο που μπορεί να πρόκειται για υφιστάμενη αρχή πιστοποίησης). Πρόκειται για το μοντέλο του ΔΟΠΑ, το οποίο παρέχει τη δυνατότητα χρήσης ακριβώς 2 επιπέδων — μιας «αρχής CSCA ρίζας» και ενός «φύλλου» DSC που υπογράφεται μόνο από την εν λόγω CSCA.

Σε περίπτωση που κράτος μέλος χρησιμοποιεί τη δική του CSCA, το εν λόγω κράτος μέλος είναι αρμόδιο για την ασφαλή λειτουργία και τη διαχείριση κλειδιών της εν λόγω αρχής πιστοποίησης. Η CSCA λειτουργεί ως άγκυρα εμπιστοσύνης για τα DSC και, ως εκ τούτου, η προστασία του ιδιωτικού κλειδιού της CSCA έχει καίρια σημασία για την ακεραιότητα του περιβάλλοντος του DCC. Το μοντέλο επαλήθευσης στην υποδομή δημόσιου κλειδιού DCC αποτελεί το μοντέλο κέλυφος, στο οποίο δηλώνεται ότι όλα τα πιστοποιητικά στη διαδρομή επικύρωσης πιστοποιητικών πρέπει να είναι έγκυρα σε μια συγκεκριμένη χρονική στιγμή (δηλαδή κατά τον χρόνο επικύρωσης της υπογραφής). Επομένως, ισχύουν οι ακόλουθοι περιορισμοί:

— η CSCA δεν εκδίδει πιστοποιητικά που έχουν μεγαλύτερη διάρκεια ισχύος απ' ό,τι το ίδιο το πιστοποιητικό της αρχής πιστοποίησης,

— ο υπογράφων το έγγραφο δεν υπογράφει έγγραφα που έχουν μεγαλύτερη διάρκεια ισχύος από ότι το DSC αυτό καθαυτό,

— τα κράτη μέλη που διαχειρίζονται τη δική τους CSCA πρέπει να ορίζουν τις περιόδους ισχύος για την οικεία CSCA, καθώς και για όλα τα πιστοποιητικά που εκδίδονται, ενώ πρέπει επίσης να μεριμνούν για την ανανέωση των πιστοποιητικών.

Στο *τμήμα 4.2* περιλαμβάνονται συστάσεις για τις περιόδους ισχύος.

3.3. *Ακεραιότητα και γνησιότητα των μεταφορτωμένων δεδομένων*

Τα εθνικά συστήματα λειτουργιών παρασκηνίου μπορούν να κάνουν χρήση της DCCG για τη μεταφόρτωση και την καταφόρτωση των ψηφιακά υπογεγραμμένων πακέτων δεδομένων μετά τον επιτυχή αμοιβαίο έλεγχο ταυτότητας. Αρχικά τα εν λόγω πακέτα δεδομένων περιέχουν τα DSC των κρατών μελών. Το ζεύγος κλειδιών που χρησιμοποιείται από το εθνικό σύστημα λειτουργιών παρασκηνίου για την ψηφιακή υπογραφή των μεταφορτωμένων πακέτων δεδομένων στο σύστημα της DCCG ονομάζεται μεταφόρτωση ζεύγους κλειδιών υπογραφής από το εθνικό σύστημα λειτουργιών παρασκηνίου και το αντίστοιχο πιστοποιητικό δημόσιου κλειδιού φέρει τη συντομογραφία «πιστοποιητικό NB_{UP}». Κάθε κράτος μέλος φέρει το δικό του πιστοποιητικό NB_{UP}, το οποίο μπορεί να είναι αυθυπόγραφο ή να εκδίδεται από υφιστάμενη αρχή πιστοποίησης, όπως δημόσια αρχή πιστοποίησης (δηλαδή αρχή πιστοποίησης που εκδίδει πιστοποιητικό σύμφωνα με τις βασικές απαιτήσεις του φόρουμ CAB). Το πιστοποιητικό NBUP διαφέρει από όλα τα άλλα πιστοποιητικά που χρησιμοποιεί το κράτος μέλος (δηλαδή τα πιστοποιητικά CSCA, πελάτη TLS ή DSC).

Τα κράτη μέλη πρέπει να παρέχουν το πιστοποιητικό μεταφόρτωσης στον διαχειριστή της DCCG κατά τη διάρκεια της αρχικής διαδικασίας καταχώρισης (*βλέπε τμήμα 4.1 για περισσότερες λεπτομέρειες*). Κάθε κράτος μέλος είναι αρμόδιο για τα εθνικά δεδομένα του και πρέπει να διασφαλίζει την προστασία του ιδιωτικού κλειδιού που χρησιμοποιείται για την υπογραφή των πιστοποιητικών που μεταφορτώνονται.

Άλλα κράτη μέλη μπορούν να επαληθεύουν τα υπογεγραμμένα πακέτα δεδομένων με τη χρήση των πιστοποιητικών μεταφόρτωσης που παρέχει η DCCG. Η DCCG επαληθεύει τη γνησιότητα και την ακεραιότητα των μεταφορτωμένων δεδομένων με το πιστοποιητικό μεταφόρτωσης του εθνικού συστήματος λειτουργιών παρασκηνίου προτού δοθούν σε άλλα κράτη μέλη.

3.4. *Απαιτήσεις σχετικά με την τεχνική δομή της DCCG*

Οι απαιτήσεις σχετικά με την τεχνική δομή της DCCG είναι οι εξής:

— η DCCG χρησιμοποιεί τον αμοιβαίο έλεγχο ταυτότητας μέσω TLS για τη δημιουργία κρυπτογραφημένης σύνδεσης με έλεγχο ταυτότητας με τα εθνικά συστήματα λειτουργιών παρασκηνίου. Επομένως, η DCCG διατηρεί λευκή λίστα καταχωρισμένων πιστοποιητικών πελάτη NB_{TLS}·

— η DCCG χρησιμοποιεί δύο ψηφιακά πιστοποιητικά ($DCCG_{TLS}$ και $DCCG_{TA}$) με δύο διακριτά ζεύγη κλειδιών. Το ιδιωτικό κλειδί του ζεύγους κλειδιού $DCCG_{TA}$ διατηρείται εκτός σύνδεσης (δεν διατηρείται στα επιγραμμικά στοιχεία της DCCG)·

— η DCCG διατηρεί κατάλογο εμπιστοσύνης των πιστοποιητικών NB_{CSCA}, ο οποίος υπογράφεται με το ιδιωτικό κλειδί $DCCG_{TA}$·

— Οι κρυπτογραφήσεις που χρησιμοποιούνται πρέπει να πληρούν τις απαιτήσεις του *τμήματος 5.1*.

4. **Διαχείριση κύκλου ζωής πιστοποιητικών**

4.1. *Καταχώριση εθνικών συστημάτων λειτουργιών παρασκηνίου*

Τα κράτη μέλη πρέπει να καταχωριστούν στον διαχειριστή της DCCG για να συμμετέχουν στο σύστημα της DCCG. Στο παρόν τμήμα περιγράφεται η τεχνική και επιχειρησιακή διαδικασία που πρέπει να τηρείται για την καταχώριση εθνικού συστήματος λειτουργιών παρασκηνίου.

Ο διαχειριστής της DCCG και το κράτος μέλος πρέπει να ανταλλάσσουν πληροφορίες για τους υπεύθυνους τεχνικών θεμάτων όσον αφορά τη διαδικασία έναρξης της διαδικασίας καταχώρισης. Θεωρείται ότι οι υπεύθυνοι τεχνικών θεμάτων εξουσιοδοτούνται από τα κράτη μέλη και διενεργείται ταυτοποίηση/έλεγχος ταυτότητας σε άλλους διαύλους. Για παράδειγμα, ο έλεγχος ταυτότητας μπορεί να επιτευχθεί όταν ο υπεύθυνος τεχνικών θεμάτων του κράτους μέλους παρέχει τα πιστοποιητικά ως αρχεία με κρυπτογραφημένο κωδικό πρόσβασης μέσω e-mail και κοινοποιεί τον αντίστοιχο κωδικό πρόσβασης στον διαχειριστή της DCCG μέσω τηλεφώνου. Μπορούν επίσης να χρησιμοποιηθούν και άλλοι ασφαλείς δίαυλοι που ορίζονται από τον διαχειριστή της DCCG.

Το κράτος μέλος πρέπει να παρέχει τρία ψηφιακά πιστοποιητικά κατά τη διάρκεια της διαδικασίας καταχώρισης και ταυτοποίησης:

— Το πιστοποιητικό TLS NB_{TLS} του κράτους μέλους

— Το πιστοποιητικό μεταφόρτωσης NB_{UP} του κράτους μέλους

— Τα πιστοποιητικά CSCA NB_{CSCA} του κράτους μέλους

Κάθε παρεχόμενο πιστοποιητικό πρέπει να πληροί τις απαιτήσεις που ορίζονται στο *τμήμα 5*. Ο διαχειριστής της DCCG θα επαληθεύει ότι το παρεχόμενο πιστοποιητικό πληροί τις απαιτήσεις που προβλέπονται στο *τμήμα 5*. Μετά την ταυτοποίηση και την καταχώριση, ο διαχειριστής της DCCG:

— προσθέτει το πιστοποιητικό (τα πιστοποιητικά) NB_{CSCA} στον υπογεγραμμένο κατάλογο εμπιστοσύνης με το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί DCC_{GTA}·

— προσθέτει το πιστοποιητικό NB_{TLS} στη λευκή λίστα του τελικού σημείου TLS της DCCG·

— προσθέτει το πιστοποιητικό NB_{UP} στο σύστημα της DCCG·

— παρέχει το πιστοποιητικό δημόσιου κλειδιού $DCCG_{TA}$ και $DCCG_{TLS}$ στο κράτος μέλος.

4.2. *Αρχές πιστοποίησης, περίοδοι ισχύος και ανανέωση*

Σε περίπτωση που κράτος μέλος επιθυμεί να διαχειρίζεται τη δική του CSCA, τα πιστοποιητικά που εκδίδει η εν λόγω αρχή μπορούν να συνιστούν αυθυπόγραφα πιστοποιητικά. Λειτουργούν ως άγκυρα εμπιστοσύνης του κράτους μέλους και, ως εκ τούτου, το κράτος μέλος πρέπει να διασφαλίζει σε μεγάλο βαθμό την προστασία των ιδιωτικών κλειδιών που αντιστοιχούν στο δημόσιο κλειδί των πιστοποιητικών CSCA. Συνιστάται στα κράτη μέλη να χρησιμοποιούν σύστημα εκτός σύνδεσης για τη CSCA, δηλαδή ένα σύστημα επεξεργασίας δεδομένων που δεν είναι συνδεδεμένο σε δίκτυο. Διενεργείται έλεγχος από πολλά πρόσωπα για την πρόσβαση στο σύστημα (για παράδειγμα, σύμφωνα με την αρχή του διπλού ελέγχου). Μετά την υπογραφή των DSC, εφαρμόζονται επιχειρησιακοί έλεγχοι και το σύστημα που διαθέτει το ιδιωτικό κλειδί CSCA αποθηκεύεται με ασφάλεια μέσω ισχυρών ελέγχων πρόσβασης. Είναι δυνατή η χρήση ασφαλούς κρυπτογραφικής μονάδας ή έξυπνων καρτών για τη διασφάλιση υψηλότερου επιπέδου προστασίας του ιδιωτικού κλειδιού CSCA. Τα ψηφιακά πιστοποιητικά περιέχουν περίοδο ισχύος η οποία καθιστά υποχρεωτική την ανανέωση του πιστοποιητικού. Η ανανέωση είναι αναγκαία για τη χρήση νέων κλειδιών κρυπτογράφησης και την προσαρμογή των μεγεθών των κλειδιών σε περίπτωση που νέες βελτιώσεις στους υπολογισμούς ή νέες επιθέσεις απειλήσουν την ασφάλεια του κρυπτογραφικού αλγορίθμου που χρησιμοποιείται. Εφαρμόζεται το μοντέλο κέλυφος (*βλέπε τμήμα 3.2*).

Δεδομένης της ετήσιας ισχύος των ψηφιακών πιστοποιητικών COVID, συνιστώνται οι ακόλουθες περίοδοι ισχύος:

— CSCA: 4 έτη

— DSC: 2 έτη

— Μεταφόρτωση: 1-2 έτη

— Έλεγχος ταυτότητας πελάτη μέσω TLS: 1-2 έτη

Για έγκαιρη ανανέωση, συνιστάται η ακόλουθη περίοδος χρήσης ιδιωτικών κλειδιών:

— CSCA: 1 έτος

— DSC: 6 μήνες

Τα κράτη μέλη πρέπει να δημιουργούν νέα πιστοποιητικά μεταφόρτωσης και πιστοποιητικά TLS εγκαίρως, για παράδειγμα, έναν μήνα πριν από τη λήξη, ώστε να είναι δυνατή η διασφάλιση της ομαλής λειτουργίας. Τα πιστοποιητικά CSCA και DSC θα πρέπει να ανανεώνονται τουλάχιστον έναν μήνα πριν από τη λήξη της χρήσης του ιδιωτικού κλειδιού (λαμβανομένων υπόψη των αναγκαίων λειτουργικών διαδικασιών). Τα κράτη μέλη πρέπει να παρέχουν επικαιροποιημένα πιστοποιητικά CSCA, πιστοποιητικά μεταφόρτωσης και πιστοποιητικά TLS στον διαχειριστή της DCCG. Τα πιστοποιητικά που έχουν λήξει θα πρέπει να διαγράφονται από τη λευκή λίστα και τον κατάλογο εμπιστοσύνης.

Τα κράτη μέλη και ο διαχειριστής της DCCG πρέπει να ελέγχουν την εγκυρότητα των δικών τους πιστοποιητικών. Δεν υπάρχει κεντρική οντότητα που να καταγράφει την εγκυρότητα των πιστοποιητικών και να ενημερώνει τους συμμετέχοντες.

4.3. *Ανάκληση πιστοποιητικών*

Κατά γενικό κανόνα, τα ψηφιακά πιστοποιητικά μπορούν να ανακαλούνται από τις αρχές πιστοποίησης που τα εκδίδουν με τη χρήση των καταστάσεων ανάκλησης πιστοποιητικών ή της απόκρισης του πρωτοκόλλου κατάστασης ηλεκτρονικού πιστοποιητικού (OCSP). Τα πιστοποιητικά CSCA για το σύστημα DCC θα πρέπει να παρέχουν καταστάσεις ανάκλησης πιστοποιητικών (CRL). Ακόμη και αν οι εν λόγω καταστάσεις ανάκλησης πιστοποιητικών δεν χρησιμοποιούνται επί του παρόντος από άλλα κράτη μέλη, θα πρέπει να ενσωματώνονται για μελλοντικές εφαρμογές. Σε περίπτωση που η CSCA αποφασίσει να μην παρέχει καταστάσεις ανάκλησης πιστοποιητικών, τα DSC που εκδίδει η εν λόγω CSCA πρέπει να ανανεώνονται όταν οι καταστάσεις ανάκλησης πιστοποιητικών καταστούν υποχρεωτικές. Οι ελεγκτές δεν θα πρέπει να χρησιμοποιούν το OCSP για την επικύρωση των DSC και θα πρέπει να χρησιμοποιούν τις καταστάσεις ανάκλησης πιστοποιητικών. Συνιστάται το εθνικό σύστημα λειτουργιών παρασκηνίου να διενεργεί την απαιτούμενη επικύρωση των DSC που καταφορτώνονται από την πύλη του DCC και να προωθεί μόνο το σύνολο των έμπιστων και επικυρωμένων DSC στα προγράμματα επικύρωσης του εθνικού DCC. Τα προγράμματα επικύρωσης του DCC δεν θα πρέπει να εκτελούν έλεγχο ανάκλησης ενός DSC κατά τη διάρκεια της διαδικασίας επικύρωσής του. Ένας λόγος είναι η διασφάλιση της προστασίας της ιδιωτικής ζωής των κατόχων του DCC με την αποφυγή κάθε περίπτωσης κατά την οποία η χρήση του συγκεκριμένου DSC μπορεί να παρακολουθείται από την οικεία συνδεδεμένη απόκριση OCSP.

Τα κράτη μέλη μπορούν να διαγράφουν μόνα τους τα DSC από την DCCG με τη χρήση έγκυρων πιστοποιητικών μεταφόρτωσης και πιστοποιητικών TLS. Η διαγραφή ενός DSC σημαίνει ότι όλα τα DCC που έχουν εκδοθεί με το συγκεκριμένο DSC θα καταστούν άκυρα όταν τα κράτη μέλη λάβουν τους ενημερωμένους καταλόγους των DSC. Η προστασία του υλικού ιδιωτικού κλειδιού που αντιστοιχεί σε DSC είναι καίριας σημασίας. Τα κράτη μέλη πρέπει να ενημερώνουν τον διαχειριστή της DCCG όταν πρέπει να ανακαλέσουν πιστοποιητικά μεταφόρτωσης ή πιστοποιητικά TLS, για παράδειγμα, λόγω παραβίασης του εθνικού συστήματος λειτουργιών παρασκηνίου. Ο διαχειριστής της DCCG μπορεί στη συνέχεια να απαλείφει το χαρακτηριστικό «έμπιστος» από το επηρεαζόμενο πιστοποιητικό, διαγράφοντας, για παράδειγμα, το πιστοποιητικό από τη λευκή λίστα πιστοποιητικών TLS. Ο διαχειριστής της DCCG μπορεί να διαγράφει τα πιστοποιητικά μεταφόρτωσης από τις βάσεις δεδομένων της πύλης. Τα πακέτα που έχουν υπογραφεί με ιδιωτικά κλειδιά που αντιστοιχούν στο εν λόγω πιστοποιητικό μεταφόρτωσης θα καταστούν άκυρα σε περίπτωση που τα εθνικά συστήματα λειτουργιών παρασκηνίου απαλείψουν το χαρακτηριστικό «έμπιστος» από τα ανακληθέντα πιστοποιητικά μεταφόρτωσης. Σε περίπτωση που πρέπει να ανακληθεί ένα πιστοποιητικό CSCA, τα κράτη μέλη ενημερώνουν τον διαχειριστή της DCCG, καθώς και τα άλλα κράτη μέλη με τα οποία έχουν σχέσεις εμπιστοσύνης. Ο διαχειριστής της DCCG θα εκδώσει νέο κατάλογο εμπιστοσύνης στον οποίο δεν περιέχεται πλέον το επηρεαζόμενο πιστοποιητικό. Όλα τα DSC που εκδίδει η εν λόγω CSCA θα καταστούν άκυρα όταν τα κράτη μέλη ενημερώσουν τον οικείο χώρο αποθήκευσης έμπιστων πιστοποιητικών του εθνικού συστήματος λειτουργιών παρασκηνίου. Σε περίπτωση που πρέπει να ανακληθούν τα πιστοποιητικά $DCCG_{TLS}$ και $DCCG_{TA}$, ο διαχειριστής της DCCG και τα κράτη μέλη πρέπει να συνεργαστούν για τη δημιουργία νέας σύνδεσης έμπιστων πιστοποιητικών TLS, καθώς και νέου καταλόγου εμπιστοσύνης.

5. **Υποδείγματα πιστοποιητικών**

Στο παρόν τμήμα περιλαμβάνονται κρυπτογραφικές απαιτήσεις και καθοδήγηση, καθώς και απαιτήσεις σχετικά με τα υποδείγματα πιστοποιητικών. Όσον αφορά τα πιστοποιητικά της DCCG, στο παρόν τμήμα ορίζονται τα υποδείγματα πιστοποιητικών.

5.1. *Κρυπτογραφικές απαιτήσεις*

Οι κρυπτογραφικοί αλγόριθμοι και οι κρυπτογραφημένες ακολουθίες TLS επιλέγονται βάσει της πρόσφατης σύστασης της γερμανικής Ομοσπονδιακής Υπηρεσίας για την Ασφάλεια στην Πληροφορική Τεχνολογία (BSI) ή της SOG-IS. Οι εν λόγω συστάσεις είναι παρόμοιες με τις συστάσεις άλλων φορέων και οργανισμών τυποποίησης. Οι συστάσεις περιλαμβάνονται στις τεχνικές κατευθυντήριες γραμμές TR 02102-1 και TR 02102-2 [1] ή στους συμφωνηθέντες κρυπτογραφικούς μηχανισμούς της SOG-IS [2].

5.1.1. Απαιτήσεις σχετικά με το DSC

Εφαρμόζονται οι απαιτήσεις που περιλαμβάνονται στο *παράρτημα I τμήμα 3.2.2*. Ως εκ τούτου, συνιστάται ιδιαίτερα στους υπογράφοντες τα έγγραφα να κάνουν χρήση του αλγόριθμου ελλειπτικής καμπύλης ψηφιακής υπογραφής (ECDSA) με τη χρήση της καμπύλης NIST-p-256 (όπως ορίζεται στο προσάρτημα D του FIPS PUB 186-4). Δεν υποστηρίζονται άλλες ελλειπτικές καμπύλες. Λόγω των περιορισμών χώρου στο DCC, τα κράτη μέλη δεν θα πρέπει να κάνουν χρήση του

[1] BSI - Technical Guidelines TR-02102 (bund.de)
[2] SOG-IS — Supporting documents (sogis.eu)

συστήματος RSA-PSS, ακόμη και αν επιτρέπεται ως εφεδρικός αλγόριθμος. Σε περίπτωση που τα κράτη μέλη χρησιμοποιούν το σύστημα RSA-PSS, θα πρέπει να χρησιμοποιούν ως τιμή τελεστή υπολοίπου διαίρεσης τα 2048 bit ή τα 3072 bit κατά μέγιστο. SHA-2 με μήκος εξόδου ≥ 256 bits χρησιμοποιείται ως κρυπτογραφική συνάρτηση κατακερματισμού (βλέπε ISO/IEC 10118-3: 2004) για την υπογραφή DSC.

5.1.2. Απαιτήσεις σχετικά με τα πιστοποιητικά TLS, μεταφόρτωσης και πιστοποιητικά CSCA

Για τα ψηφιακά πιστοποιητικά και τις κρυπτογραφικές υπογραφές στο περιβάλλον της DCCG, οι βασικές απαιτήσεις σχετικά με τους κρυπτογραφικούς αλγόριθμους και το μήκος των κλειδιών συνοψίζονται στον ακόλουθο πίνακα (στοιχεία του 2021):

Αλγόριθμος υπογραφής	Μέγεθος κλειδιού	Συνάρτηση κατακερματισμού
EC-DSA	Τουλάχιστον 250 Bit	SHA-2 με μήκος εξόδου ≥ 256 Bit
RSA-PSS (συνιστώμενη αναπλήρωση) RSA-PKCS#1 v1.5 (αναπλήρωση παλαιού τύπου)	Τελεστής υπολοίπου διαίρεσης RSA (N) τουλάχιστον 3000 Bit με δημόσιο εκθέτη e > 2^16	SHA-2 με μήκος εξόδου ≥ 256 Bit
DSA	Τουλάχιστον 3000 Bit για πρώτο p, 250 Bit για κλειδί q	SHA-2 με μήκος εξόδου ≥ 256 Bit

Η συνιστώμενη ελλειπτική καμπύλη για τον αλγόριθμο EC-DSA είναι η NIST-p-256 λόγω της ευρέως διαδεδομένης εφαρμογής της.

5.2. *Πιστοποιητικό CSCA (NB_{CSCA})*

Στον πίνακα που ακολουθεί παρέχεται καθοδήγηση σχετικά με το υπόδειγμα πιστοποιητικού NB_{CSCA}, σε περίπτωση που ένα κράτος μέλος αποφασίσει να διαχειρίζεται τη δική του CSCA για το σύστημα του DCC.

Απαιτούνται εγγραφές με **έντονους χαρακτήρες** (πρέπει να περιλαμβάνονται στο πιστοποιητικό), συνιστώνται εγγραφές με *πλάγιους χαρακτήρες* (θα πρέπει να περιλαμβάνονται). Δεν ορίζονται συστάσεις για πεδία που ελλείπουν.

Πεδίο	Τιμή
Θέμα	**cn=<μη κενό και μοναδικό κοινό όνομα>,***o=<πάροχος>*,**c=<κράτος μέλος που διαχειρίζεται την CSCA>**
Χρήση κλειδιού	**υπογραφή πιστοποιητικού,***υπογραφή CRL* (κατ' ελάχιστο)
Βασικοί περιορισμοί	**CA = αληθές, περιορισμοί μήκους διαδρομής = 0**

Το πεδίου του ονόματος θέματος δεν πρέπει να είναι κενό και πρέπει να είναι μοναδικό εντός του καθορισμένου κράτους μέλους. Ο κωδικός χώρας (c) πρέπει να αντιστοιχεί στο κράτος μέλος που θα κάνει χρήση πιστοποιητικού της εν λόγω CSCA. Το πιστοποιητικό πρέπει να περιέχει μοναδικό αναγνωριστικό κλειδιού θέματος (subject key identifier, SKI) σύμφωνα με το πρότυπο RFC 5280 ([3]).

5.3. *Πιστοποιητικό υπογραφής εγγράφου (DSC)*

Στον πίνακα που ακολουθεί παρέχεται καθοδήγηση σχετικά με το DSC. Απαιτούνται εγγραφές με **έντονους χαρακτήρες** (πρέπει να περιλαμβάνονται στο πιστοποιητικό), συνιστώνται εγγραφές με *πλάγιους χαρακτήρες* (θα πρέπει να περιλαμβάνονται). Δεν ορίζονται συστάσεις για πεδία που ελλείπουν.

Πεδίο	Τιμή
Αριθμός σειράς	**μοναδικός αριθμός σειράς**
Θέμα	**cn= <μη κενό και μοναδικό κοινό όνομα>,***o=<πάροχος>*,**c=<κράτος μέλος που χρησιμοποιεί το παρόν DSC>**
Χρήση κλειδιού	**ψηφιακή υπογραφή** (κατ' ελάχιστο)

([3]) rfc5280 (ietf.org).

Το DSC πρέπει να υπογράφεται με το ιδιωτικό κλειδί που αντιστοιχεί σε πιστοποιητικό της CSCA που χρησιμοποιεί το κράτος μέλος.

Πρέπει να χρησιμοποιούνται οι ακόλουθες επεκτάσεις:

— Το πιστοποιητικό πρέπει να περιέχει αναγνωριστικό κλειδιού αρχής (Authority Key Identifier, AKI) που αντιστοιχεί σε αναγνωριστικό κλειδιού θέματος (SKI) του πιστοποιητικού της εκδούσας CSCA.

— Το πιστοποιητικό θα πρέπει να περιέχει μοναδικό αναγνωριστικό κλειδιού θέματος (σύμφωνα με το πρότυπο RFC 5280 ([4]))

Επιπλέον, το πιστοποιητικό θα πρέπει να περιέχει την επέκταση σημείου διανομής της κατάστασης ανάκλησης πιστοποιητικών, με ένδειξη προς την κατάσταση ανάκλησης πιστοποιητικών (CRL) που παρέχει η CSCA η οποία έχει εκδώσει το DSC.

Το DSC μπορεί να περιέχει επέκταση εκτεταμένης χρήσης κλειδιού με καθόλου ή περισσότερους αναγνωριστικούς κωδικούς πολιτικής χρήσης κλειδιού, οι οποίοι περιορίζουν τους τύπους των HCERT που το εν λόγω πιστοποιητικό έχει τη δυνατότητα να επαληθεύει. Εάν υπάρχουν μία ή περισσότερες εκτεταμένες χρήσεις κλειδιού, οι ελεγκτές επαληθεύουν τη χρήση κλειδιού έναντι του αποθηκευμένου HCERT. Για τον σκοπό αυτόν, ορίζονται οι ακόλουθες τιμές εκτεταμένης χρήσης κλειδιού:

Πεδίο	Τιμή
εκτεταμένη χρήση κλειδιού	1.3.6.1.4.1.1847.2021.1.1 για εκδότες πιστοποιητικού διαγνωστικού ελέγχου
εκτεταμένη χρήση κλειδιού	1.3.6.1.4.1.1847.2021.1.2 για εκδότες πιστοποιητικού εμβολιασμού
εκτεταμένη χρήση κλειδιού	1.3.6.1.4.1.1847.2021.1.3 για εκδότες πιστοποιητικού ανάρρωσης

Ελλείψει επέκτασης της χρήσης κλειδιού, το εν λόγω πιστοποιητικό μπορεί να χρησιμοποιείται για την επικύρωση κάθε τύπου HCERT. Άλλα έγγραφα δύνανται να καθορίζουν τα αντίστοιχα επιπλέον αναγνωριστικά πολιτικής εκτεταμένης χρήσης κλειδιού με επικύρωση των HCERT.

5.4. *Πιστοποιητικά μεταφόρτωσης (NBUP)*

Στον πίνακα που ακολουθεί παρέχεται καθοδήγηση σχετικά με το πιστοποιητικό μεταφόρτωσης του εθνικού συστήματος λειτουργιών παρασκηνίου. Απαιτούνται εγγραφές με **έντονους χαρακτήρες** (πρέπει να περιλαμβάνονται στο πιστοποιητικό), συνιστώνται εγγραφές με *πλάγιους χαρακτήρες* (θα πρέπει να περιλαμβάνονται). Δεν ορίζονται συστάσεις για πεδία που ελλείπουν.

Πεδίο	Τιμή
Θέμα	**cn= <μη κενό και μοναδικό κοινό όνομα>,***o=<πάροχος>*, **c=<κράτος μέλος που χρησιμοποιεί το παρόν πιστοποιητικό μεταφόρτωσης>**
Χρήση κλειδιού	**ψηφιακή υπογραφή** (κατ' ελάχιστο)

5.5. *Έλεγχος ταυτότητας πελάτη μέσω TLS από το εθνικό σύστημα λειτουργιών παρασκηνίου (NB_{TLS})*

Στον πίνακα που ακολουθεί παρέχεται καθοδήγηση σχετικά με το πιστοποιητικό ελέγχου ταυτότητας πελάτη μέσω TLS του εθνικού συστήματος λειτουργιών παρασκηνίου. Απαιτούνται εγγραφές με **έντονους χαρακτήρες** (πρέπει να περιλαμβάνονται στο πιστοποιητικό), συνιστώνται εγγραφές με *πλάγιους χαρακτήρες* (θα πρέπει να περιλαμβάνονται). Δεν ορίζονται συστάσεις για πεδία που ελλείπουν.

Πεδίο	Τιμή
Θέμα	**cn= <μη κενό και μοναδικό κοινό όνομα>,***o=<πάροχος>*, **c=<κράτος μέλος στο Σημείωση>**
Χρήση κλειδιού	**ψηφιακή υπογραφή** (κατ' ελάχιστο)
Εκτεταμένη χρήση κλειδιού	**έλεγχος ταυτότητας πελάτη (1.3.6.1.5.5.7.3.2)**

([4]) rfc5280 (ietf.org).

Το πιστοποιητικό δύναται επίσης να περιέχει την εκτεταμένη χρήση κλειδιού *ελέγχου ταυτότητας διακομιστή* (*1.3.6.1.5.5.7.3.1*), η οποία όμως δεν απαιτείται.

5.6. *Κατάλογος εμπιστοσύνης πιστοποιητικών υπογραφής ($DCCG_{TA}$)*

Στους πίνακες που ακολουθούν ορίζεται το πιστοποιητικό άγκυρας εμπιστοσύνης της DCCG.

Πεδίο	Τιμή
Θέμα	**cn = πύλη ψηφιακού πράσινου πιστοποιητικού** ([5])**, o=<πάροχος>, c=<χώρα>**
Χρήση κλειδιού	**ψηφιακή υπογραφή** (κατ' ελάχιστο)

5.7. *Πιστοποιητικά διακομιστή TLS της DCCG ($DCCG_{TLS}$)*

Στους πίνακες που ακολουθούν ορίζεται το πιστοποιητικό TLS της DCCG.

Πεδίο	Τιμή
Θέμα	cn=<FQDN ή διεύθυνση IP της DCCG, o=<πάροχος>, c=<χώρα>
Εναλλακτικό όνομα θέματος	Όνομα dNS: <όνομα DNS της DCCG> ή διεύθυνση IP: <διεύθυνση IP της DCCG>
Χρήση κλειδιού	**ψηφιακή υπογραφή** (κατ' ελάχιστο)
Εκτεταμένη χρήση κλειδιού	**έλεγχος ταυτότητας διακομιστή (1.3.6.1.5.5.7.3.1**)

Το πιστοποιητικό δύναται επίσης να περιέχει την εκτεταμένη χρήση κλειδιού *ελέγχου ταυτότητας πελάτη* (*1.3.6.1.5.5.7.3.2*), η οποία όμως δεν απαιτείται.

Το πιστοποιητικό TLS της DCCG εκδίδεται από δημοσίως έμπιστη αρχή πιστοποίησης (η οποία περιλαμβάνεται σε όλα τα βασικά προγράμματα περιήγησης και τα λειτουργικά συστήματα, σύμφωνα με τις βασικές απαιτήσεις του φόρουμ CAB).

([5]) Η ορολογία του «ψηφιακού πράσινου πιστοποιητικού» αντί του «Ψηφιακού Πιστοποιητικού COVID της ΕΕ» διατηρήθηκε στο πλαίσιο αυτό, διότι πρόκειται για την ορολογία που χρησιμοποιήθηκε στο πιστοποιητικό, χωρίς δυνατότητα τροποποίησης, πριν οι συννομοθέτες λάβουν απόφαση για τη χρήση νέας ορολογίας.