ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ

Τμήμα Ψηφιακών Συστημάτων

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

«Υποδομή Δημόσιου Κλειδιού (PKI) – Ψηφιακές Υπογραφές»

Νικόλαος Παγανός

MTE1628

Επιβλέπων: Καθηγητής Κ. Λαμπρινουδάκης

Πειραιάς, Μάιος 2018

Επιτελική Σύνοψη

Η παρούσα διπλωματική εργασία έχει ως αντικείμενο τη παρουσίαση μιας πρότασης με σκοπό τη δημιουργία μιας πρότασης πολιτικής πιστοποίησης για τον Ελληνικό Στρατό. Επιπλέον θα οριστούν οι διαδικασίες πιστοποίησης που χρησιμοποιούνται από τις Αρχές Πιστοποίησης που συμμετέχουν στην Υποδομή Δημόσιου Κλειδιού του Ελληνικού Στρατού.

Η εν λόγω πρόταση Πολιτικής Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης περιγράφει το σύνολο κανόνων οι οποίοι εφαρμόζονται για την έκδοση πιστοποιητικών από την Υποδομή Δημοσίου Κλειδιού του ΕΣ, η οποία συμμορφώνεται επίσης με τις εκάστοτε Διαδικασίες Πιστοποίησης, οι οποίες περιγράφουν τους γενικότερους όρους που ακολουθούνται, ανάλογα με τον τύπο των ψηφιακών πιστοποιητικών που εκδίδονται.

Μετά από συζητήσεις με υπεύθυνους του Ελληνικού Στρατού και μετά από πολύωρες διαβουλεύσεις δημιουργήθηκε η ακόλουθη πρόταση, η οποία όταν υλοποιηθεί θα δώσει στον Ελληνικό Στρατό τη δυνατότητα να εκδίδει πιστοποιητικά μέσω μιας Υποδομής Δημοσίου Κλειδιού της ιδιοκτησίας του και άρα να εξελιχθεί.

Ευχαριστίες

Θα ήθελα να ευχαριστήσω την κοπέλα μου, Αλεξάνδρα, τους γονείς μου, Ευθύμιο και Χριστίνα, καθώς και τον αδερφό μου, Χαράλαμπο, για την αμέριστη και διαρκή υποστήριξή τους. Θα ήθελα να ξέρετε πως η πίστη σας στις δυνατότητές μου αποτέλεσε αρωγό στους στόχους και στα όνειρά μου.

Επίσης θα ήθελα να ευχαριστήσω τον κύριο Παναγιώτη Σιάνα, υπεύθυνο για το πρόγραμμα συνεργασίας του Ελληνικού Στρατού και του μεταπτυχιακού προγράμματος Ασφάλειας Ψηφιακών Συστημάτων, για εξαιρετική συνεργασία που είχαμε, το χρόνο που διέθεσε, την καθοδήγηση, καθώς και για τις πληροφορίες με τις οποίες με εφοδίασε.

Τέλος θα ήθελα να ευχαριστήσω τον κύριο Λαμπρινουδάκη για τη δυνατότητα που μου έδωσε να εκπονήσω τη συγκεκριμένη διπλωματική εργασία.

Αθήνα, Μάιος 2018

Νικόλαος Παγανός

Στην Αλεξάνδρα

Πίνακας Περιεχομένων

Εισαγωγή

Η παρούσα διπλωματική εργασία αποτελείται από δύο σκέλη: το θεωρητικό και το πρακτικό. Στο πρώτο παρουσιάζονται στον αναγνώστη το θεωρητικό υπόβαθρο των όσων διαδραματίζονται στο πρακτικό μέρους. Η εν λόγω διαδικασία είναι μέγιστης σημασίας για την καλύτερη κατανόηση του αντικειμένου που πραγματεύεται η εργασία.

Πιο συγκεκριμένα, στο θεωρητικό σκέλος δίνονται λεπτομέρειες σχετικά με ορισμένους από τους όρους που αναφέρονται εντός του πρακτικού σκέλους. Με αυτόν τον τρόπο θα μπορεί ο αναγνώστης και, σε ένα πιο γενικό πλαίσιο, ο Ελληνικός Στρατός να κατανοεί καλύτερα τα όσα αναλύονται στο εν λόγω μέρος και ως εκ τούτου να μπορεί να τα εφαρμόσει στην πράξη. Είναι ύψιστη σημασίας, καθώς μέσα από αυτό θα γίνει δυνατή η βέλτιστη εφαρμογή της πρότασης πολιτικής πιστοποίησης που ακολουθεί.

Στη συνέχεια παρουσιάζεται η προαναφερθείσα πρόταση πολιτικής πιστοποίησης. Μέσα στην εν λόγω πρόταση εμφανίζονται όλα τα κεφάλαια τα οποία πρέπει να περιλαμβάνονται και πρέπει να υλοποιηθούν, ώστε να αποκτήσει ο Ελληνικός Στρατός μια Υποδομή Δημόσιου Κλειδιού.

Γενικά στοιχεία

1. PKI

Η Υποδομή Δημόσιου Κλειδιού (PKI – Public Key Infrastructure) είναι ένας συνδυασμός από προγράμματα, τεχνολογίες κρυπτογράφησης διαδικασίες και υπηρεσίες οι οποίες χρησιμοποιούνται για την δημιουργία, διαχείριση, διανομή, χρήση και ανάκληση ψηφιακών πιστοποιητικών. Συγκεκριμένα πρόκειται για έναν τρόπο αντιστοίχησης δημοσίων κλειδιών με χρήστες, κάθε ένας εκ των οποίων έχει έναν συγκεκριμένο ρόλο και μία μοναδική ταυτότητα. Ο ρόλος που έχει κάθε χρήστης καθορίζει τους πόρους του δικτύου και των υπολογιστών του στους οποίους έχει πρόσβαση, ενώ σαν ταυτότητα εννοείται το φυσικό πρόσωπο στο οποίο αντιστοιχεί κάθε τέτοιο κλειδί. Παρακάτω όταν αναφερόμαστε σε έναν χρήστη του δικτύου θα εννοούμε τον συνδυασμό των δύο παραπάνω. Σε κάθε χρήστη χορηγείται ένα μοναδικό πιστοποιητικό το οποίο επιβεβαιώνει ότι ένα συγκεκριμένο δημόσιο κλειδί αντιστοιχεί σε αυτόν.

Τα κύρια μέρη που απαρτίζουν ένα σύστημα Υποδομής Δημόσιου Κλειδιού είναι τα παρακάτω:

- Η Αρχή Πιστοποιητικών (CA – Certificate Authority)
- Η Αρχή Καταχώρισης (RA – Registration Authority)
- Η Αρχή Επιβεβαίωσης (VA – Validation Authority)
- Ένας ασφαλής κεντρικός κατάλογος πιστοποιητικών στον οποίο κρατούνται και αποθηκεύονται τα κλειδιά κάθε χρήστη.

2. Αρχή Πιστοποίησης

Η Αρχή Πιστοποίησης (CA) είναι ο αξιόπιστος τρίτος υπεύθυνος για την επικύρωση της ταυτότητας ενός ατόμου ή ενός οργανισμού. Μόλις πιστοποιηθεί η ταυτότητα, ένας διακομιστής πιστοποιητικών δημιουργεί ένα ψηφιακό πιστοποιητικό που περιέχει το δημόσιο κλειδί του ατόμου. Το ψηφιακό πιστοποιητικό στη συνέχεια υπογράφεται ψηφιακά με το ιδιωτικό κλειδί της CA. Οι Αρχές Πιστοποίησης είναι πραγματικές οργανώσεις που αποτελούνται από ανθρώπους και τεχνολογίες των οποίων η δουλειά είναι να επικυρώνουν την ταυτότητα όσων αναζητούν ψηφιακά πιστοποιητικά. Οι διαδικασίες μιας CA περιγράφονται σε έγγραφα γνωστά ως πρακτικές πιστοποίησης (CPS). Αυτό το έγγραφο περιγράφει θέματα όπως το πώς επιβεβαιώνονται οι ταυτότητες και πώς διατηρούνται και μεταδίδονται τα ψηφιακά πιστοποιητικά. Πριν από τη συμμετοχή στις υπηρεσίες μιας CA είναι σημαντική η προσεκτική ανάγνωση του CPS του οργανισμού.

3. Αρχή Καταχώρισης

Η Αρχή Καταχώρισης (RA) είναι το στοιχείο ενός PKI που είναι υπεύθυνο για την αποδοχή αιτημάτων για ψηφιακά πιστοποιητικά και την εξακρίβωση της ταυτότητας του ατόμου ή του οργανισμού που υποβάλλει το αίτημα. Η συγκεκριμένη διαδικασία επαλήθευσης ταυτότητας που χρησιμοποιείται εξαρτάται από την κλάση του πιστοποιητικού που ζητείται:

Κλάση 1 - Περιλαμβάνει την επαλήθευση ενός ατόμου μέσω ηλεκτρονικού ταχυδρομείου. Ένα πιστοποιητικό κλάσης 1 μπορεί να χρησιμοποιηθεί για την ψηφιακή υπογραφή μηνυμάτων email. Συνήθως απαιτείται διεύθυνση ηλεκτρονικού ταχυδρομείου, πλήρες όνομα και φυσική διεύθυνση. Η

διαδικασία αίτησης θα περπατήσει επίσης ο αιτών μέσω της διαδικασίας δημιουργίας ζευγαριού δημόσιου / ιδιωτικού κλειδιού.

Κλάση 2 - Χρησιμοποιείται για την υπογραφή λογισμικού, έτσι ώστε ένα άτομο που χρησιμοποιεί το λογισμικό να μπορεί να επαληθεύσει την αυθεντικότητα του πωλητή λογισμικού.

Κλάση 3 - Παρέχεται σε εταιρείες που επιθυμούν να δημιουργήσουν δική τους αρχή πιστοποίησης.

Μόλις ολοκληρωθεί η διαδικασία επικύρωσης, η RA μεταδίδει το αίτημα στην CA που την μεταβιβάζει στο Διακομιστή Πιστοποιητικών (CS). Ο CS δημιουργεί το ψηφιακό πιστοποιητικό, συμπεριλαμβανομένων των κατάλληλων πληροφοριών (συμπεριλαμβανομένου του δημόσιου κλειδιού του αιτούντος) και αποστέλλει το πιστοποιητικό στον αιτούντα.

4. Αρχή Επιβεβαίωσης

Η Αρχή Επιβεβαίωσης (VA) είναι προαιρετική και δεν υπάρχει σε αρκετά συστήματα. Πρόκειται για μία Τρίτη αρχή που μπορεί να παρέχει στην Αρχή Πιστοποιητικών κάποιες επιπλέον πληροφορίες με τις οποίες θα επιβεβαιώνεται η μοναδική ταυτότητα του χρήστη.

5. Ηλεκτρονικά Πιστοποιητικά

Τα ηλεκτρονικά πιστοποιητικά είναι η βάση της Υποδομής Δημόσιου κλειδιού. Πρόκειται για ένα έγγραφο το οποίο χρησιμοποιεί μία ηλεκτρονική υπογραφή για να αντιστοιχίσει με μοναδικό τρόπο ένα δημόσιο κλειδί με έναν συγκεκριμένο χρήστη. Τυπικά ένα ηλεκτρονικό πιστοποιητικό περιέχει τις παρακάτω πληροφορίες:

- Την ταυτότητα του χρήστη που χρησιμοποιεί το πιστοποιητικό. Δεν πρόκειται απαραίτητα για ένα φυσικό πρόσωπο, καθώς ένα πιστοποιητικό μπορεί να αντιστοιχεί σε έναν υπολογιστή, μία συσκευή που συνδέεται στο δίκτυο ή μία υπηρεσία του.
- Πληροφορίες σχετικά με την Αρχή πιστοποίησης που εξέδωσε το πιστοποιητικό.
- Το δημόσιο κλειδί που είναι συνδεδεμένο με αυτό το πιστοποιητικό. Προφανώς ο κάτοχος του πιστοποιητικού έχει και το αντίστοιχο ιδιωτικό κλειδί από το οποίο δημιουργήθηκε.
- Τα ονόματα των αλγορίθμων κρυπτογράφησης και υπογραφής που υποστηρίζονται από αυτό το πιστοποιητικό.
- Πληροφορίες σχετικά με το πώς μπορεί να ελεγχθεί η εγκυρότητα του πιστοποιητικού και το αν έχει ανακληθεί ή όχι.

6. Αποθήκες πιστοποιητικών

Μόλις έχουν δημιουργηθεί τα πιστοποιητικά και τα αντίστοιχα δημόσια κλειδιά, αποθηκεύονται γενικά σε μια δημόσια προσβάσιμη τοποθεσία γνωστή ως αποθήκη πιστοποιητικών. Τα αποθετήρια πιστοποιητικών είναι συνήθως συμβατά με το Lightweight Directory Access Protocol (LDAP), καθιστώντας την πρόσβαση και την αναζήτηση αποθετηρίων συμβατών με τα ανοικτά πρότυπα. Ένα ειδικό αποθετήριο ασφαλείας είναι συνήθως διαθέσιμο για κάθε συγκεκριμένο περιβάλλον PKI.

Κεντρικές και αποκεντρωμένες υποδομές

Τα ζεύγη κλειδιών που χρησιμοποιούνται σε ένα PKI δημιουργούνται χρησιμοποιώντας συγκεντρωτικές ή αποκεντρωμένες μεθόδους. Η επιλογή της προσέγγισης συνήθως εξαρτάται από την πολιτική

ασφαλείας ενός οργανισμού. Τα κλειδιά που παράγονται και αποθηκεύονται σε τοπικά συστήματα υπολογιστών για χρήση από αυτά τα συστήματα λέγεται ότι συμμορφώνονται με την αποκεντρωμένη προσέγγιση. Τα κλειδιά που παράγονται από κεντρικό εξυπηρετητή και μεταδίδονται στους κεντρικούς υπολογιστές με βάση τις ανάγκες, αναφέρονται κεντρικά. Είναι σημαντικό να σημειωθεί ότι αυτές οι διακρίσεις δεν απαρτίζονται αναγκαστικά αμοιβαία και ότι υπάρχει περιθώριο για κάποια επικάλυψη. Για παράδειγμα, σε ένα αποκεντρωμένο περιβάλλον εξακολουθεί να είναι δυνατή η δημιουργία των κλειδιών από το τοπικό σύστημα και το δημόσιο κλειδί που παρέχεται στον κεντρικό διακομιστή για τη δημιουργία και τη διανομή του αντίστοιχου πιστοποιητικού.

7. Γενικά στοιχεία για το eIDAS

Η ηλεκτρονική ταυτοποίηση (eID) και οι ηλεκτρονικές υπηρεσίες εμπιστευτικότητας (eTS) αποτελούν τα βασικά στοιχεία για ασφαλείς διασυνοριακές ηλεκτρονικές συναλλαγές και κεντρικά δομικά στοιχεία της Ψηφιακής Ενιαίας Αγοράς. Ο κανονισμός (ΕΕ) αριθ. 910/2014 σχετικά με τις ηλεκτρονικές υπηρεσίες αναγνώρισης και εμπιστοσύνης για ηλεκτρονικές συναλλαγές στην εσωτερική αγορά (κανονισμός eIDAS) που εγκρίθηκε από τους συννομοθέτες στις 23 Ιουλίου 2014 αποτελεί ορόσημο για την παροχή ασφαλούς ρυθμιστικού περιβάλλοντος μεταξύ επιχειρήσεων, πολιτών και δημόσιων αρχών.

Ο κανονισμός eIDAS διασφαλίζει ότι οι άνθρωποι και οι επιχειρήσεις μπορούν να χρησιμοποιούν τα δικά τους εθνικά συστήματα ηλεκτρονικής αναγνώρισης (eID) για να έχουν πρόσβαση σε δημόσιες υπηρεσίες σε άλλες χώρες της ΕΕ όπου υπάρχουν διαθέσιμα eID. Επίσης δημιουργεί μια ευρωπαϊκή εσωτερική αγορά για το eTS, δηλαδή τις ηλεκτρονικές υπογραφές, τις ηλεκτρονικές σφραγίδες, τη χρονική σφραγίδα, την ηλεκτρονική υπηρεσία παράδοσης και την εξακρίβωση της ταυτότητας του δικτυακού τόπου, εξασφαλίζοντας ότι θα εργαστούν διασυνοριακά και θα έχουν το ίδιο νομικό καθεστώς με τις παραδοσιακές διαδικασίες που βασίζονται στο χαρτί. Μόνο με την εξασφάλιση της νομικής εγκυρότητας όλων αυτών των υπηρεσιών, οι επιχειρήσεις και οι πολίτες θα χρησιμοποιούν τις ψηφιακές αλληλεπιδράσεις ως τον φυσικό τρόπο αλληλεπίδρασής τους.

Με την eIDAS, η ΕΕ έχει κατορθώσει να δημιουργήσει τα σωστά θεμέλια και ένα προβλέψιμο νομικό πλαίσιο για άτομα, επιχειρήσεις (ιδίως ΜΜΕ) και δημόσιες διοικήσεις για την ασφαλή πρόσβαση σε υπηρεσίες και για συναλλαγές σε απευθείας σύνδεση και διασυνοριακά μόνο με ένα κλικ. Πράγματι, η υλοποίηση του eIDAS σημαίνει μεγαλύτερη ασφάλεια και περισσότερη ευκολία για οποιαδήποτε δραστηριότητα στο διαδίκτυο, όπως η υποβολή φορολογικών δηλώσεων, η εγγραφή σε αλλοδαπό πανεπιστήμιο, η εξ αποστάσεως ανοίγματος τραπεζικού λογαριασμού, η σύσταση επιχείρησης σε άλλο κράτος μέλος, η εξακρίβωση της ταυτότητας για πληρωμές στο διαδίκτυο, πρόσκληση υποβολής προσφορών κ.λπ. Στις 8 Σεπτεμβρίου 2015, η Ευρωπαϊκή Επιτροπή ολοκλήρωσε την έγκριση όλων των εκτελεστικών πράξεων που πρέπει να εκδοθούν έως τις 18 Σεπτεμβρίου 2015.

8. Γενικά στοιχεία για τον GDPR

Κάθε εταιρία που χειρίζεται προσωπικά δεδομένα τα οποία αφορούν σε άτομα εντός της Ευρωπαϊκής Ένωσης, θα είναι υποχρεωμένος να συμμορφωθεί πλήρως με το νέο κανονισμό της Ευρωπαικής ένωσης GDPR (EU General Data Protection Regulation), επανεξετάζοντας ή και αναθεωρώντας όλες τις διαδικασίες διαχείρισης των πληροφοριών του και αποτελεί τη μεγαλύτερη αλλαγή στην νομοθεσία περί προστασίας των δεδομένων τα τελευταία σχεδόν 20 χρόνια.

Αυτά μπορεί να αποκαλύπτουν την ταυτότητα του ατόμου, το φύλο του, την ηλικία του, τον τόπο διαμονής, την οικογενειακή του κατάσταση, την εργασιακή του σχέση αλλά και ακόμη πιο προσωπικές πληροφορίες όπως τις συνήθειές του, και τις προτιμήσεις του.

Η εταιρεία πρέπει να εξετάσει την αλλαγή ή και προσαρμογή των πληροφοριακών της συστημάτων για να συμμορφωθεί με όρους όπως:

- Προσεκτική συγκέντρωση και ασφαλής αποθήκευση προσωπικών δεδομένων.
- Καμία επεξεργασία των προσωπικών δεδομένων χωρίς συγκατάθεση
- Κωδικοποίηση αυτών για αποφυγή αναγνώρισης ταυτότητας (profiling)
- Αποφυγή συσχετισμού βάσεων δεδομένων (linked data)
- Δυνατότητα διαγραφής ή εξαγωγής και παράδοσης των δεδομένων κατ' απαίτηση.
- Εφαρμογής της αρχής «τόσα δεδομένα όσα είναι απαραίτητα»
- Διασφάλιση συμμόρφωσης στον Κανονισμό και από τις συνεργαζόμενες εταιρείες που διαχειρίζονται τα προσωπικά δεδομένα για λογαριασμό της.

Πρόταση Πολιτικής Πιστοποίησης

1. Εισαγωγή

Το έγγραφο αυτό ορίζει την πολιτική και τις διαδικασίες πιστοποίησης που χρησιμοποιούνται από τις Αρχές Πιστοποίησης που συμμετέχουν στην Υποδομή Δημοσίου Κλειδιού (ΥΔΚ) του Ελληνικού Στρατού (ΕΣ).

1.1. Επισκόπηση

Η παρούσα Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης περιγράφει το σύνολο κανόνων οι οποίοι εφαρμόζονται για την έκδοση πιστοποιητικών από την Υποδομή Δημοσίου Κλειδιού του ΕΣ. Η ΥΔΚ ΕΣ συμμορφώνεται επίσης με τις εκάστοτε Διαδικασίες Πιστοποίησης, οι οποίες περιγράφουν τους γενικότερους όρους που ακολουθούνται, ανάλογα με τον τύπο των ψηφιακών πιστοποιητικών που εκδίδονται.

Οι Αρχές Πιστοποίησης του ΕΣ εκδίδουν Πιστοποιητικά Χρήστη, Πιστοποιητικά Δικτυακών Συσκευών (π.χ. εξυπηρετητές, δρομολογητές κλπ.) και Πιστοποιητικά Υφιστάμενων Αρχών Πιστοποίησης. Όλα τα πιστοποιητικά περιέχουν αναφορά προς το παρόν κείμενο. Οι κάτοχοι πιστοποιητικών, ιδιωτικών κλειδιών, καθώς και οι οντότητες που βασίζονται στην εγκυρότητα των πιστοποιητικών, θα πρέπει να λαμβάνουν γνώση και να συμμορφώνονται με το παρόν κείμενο.

1.2. Κοινότητα εφαρμογής της ΥΔΚ

Η κοινότητα που διέπεται από αυτή την Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης είναι το σύνολο των οντοτήτων που χρησιμοποιούν τα πιστοποιητικά που εκδίδονται από την Υποδομή Δημοσίου Κλειδιού του ΕΣ.

1.2.1. Αρχές πιστοποίησης

Οι Αρχές Πιστοποίησης είναι οι οντότητες της Υποδομής Δημόσιου Κλειδιού που εκδίδουν τα πιστοποιητικά. Κάθε αρχή Πιστοποίησης χρησιμοποιεί μία η περισσότερες Αρχές Καταχώρισης για τη μεταβίβαση των αιτήσεων των συνδρομητών στην Αρχή Πιστοποίησης.

Η Ιεραρχία της Υπηρεσίας Πιστοποίησης αποτελείται από τις παρακάτω οντότητες:

1. **Κεντρική Αρχή Πιστοποίησης (Central Certification Authority)** η οποία εκδίδει ψηφιακά πιστοποιητικά αποκλειστικά για υφιστάμενες Αρχές Πιστοποίησης που λειτουργούν υπό το νομικό πρόσωπο του Ελληνικού Στρατού. Το εν λόγω πιστοποιητικό έχει διάρκεια ισχύος οκτώ (8) έτη.
2. **Υφιστάμενες Αρχές Πιστοποίησης (Existing Certification Authority)**, που μπορούν να λειτουργούν για διαχειριστικούς λόγους του ΕΣ, οι οποίες εξυπηρετούν διοικητικές μονάδες του ΕΣ ή νομικά πρόσωπα όπου συμμετέχει ο ΕΣ, οι οποίες συμμορφώνονται και υιοθετούν πλήρως την παρούσα Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης. Τα πιστοποιητικά των Υφιστάμενων Αρχών Πιστοποίησης έχουν διάρκεια ισχύος έως τέσσερα (4) έτη. Αρχικά λειτουργούν:
    - Μία (1) υφιστάμενη Αρχή Πιστοποίησης για τις οντότητες που ανήκουν στη ομάδα διαχείρισης της ΥΔΚ ΕΣ, η οποία εκδίδει πιστοποιητικά σε χρήστες και εξυπηρετητές/συσκευές του ΕΣ της εν λόγω ομάδας.

- Δύο (2) υφιστάμενες Αρχές Πιστοποίησης για τις οντότητες όλων των διοικητικών μονάδων του ΕΣ οι οποίες θα εκδίδουν πιστοποιητικά για χρήστες και εξυπηρετητές/συσκευές αντίστοιχα.

Οι Αρχές Πιστοποίησης ταξινομούνται στους εξής δύο ρόλους:

1. **Signing CA:** Αφορά την πιστοποίηση των χρηστών και δεν αποθηκεύει το ιδιωτικό κλειδί. Το ΓΕΣ/Β1 (ΔΙΠΡΟ) είναι αρμόδιο για τις ταυτότητες και για τον εν λόγω ρόλο.
2. **Crypto CA:** Αφορά τις υποδομές (IT Infrastructure) και αποθηκεύει το ιδιωτικό κλειδί. Επίσης αφορά τους developers, οι οποίοι όπως θα τονιστεί παρακάτω έχουν δύο ρόλους (ως χρήστες και ως developers).

1.2.2. Αρχές Καταχώρισης

Οι Αρχές Καταχώρισης είναι οντότητες αρμόδιες για την πιστοποίηση της ταυτότητας των εγγραφόμενων πριν από την έκδοση του πιστοποιητικού. Οι ΑΚ διαβιβάζουν με ασφαλή τρόπο τις αιτήσεις στην αρμόδια Αρχή Πιστοποίησης.

1.2.3. Συνδρομητές (Subscribers)

Συνδρομητές στην Υπηρεσία Πιστοποίησης είναι όσοι αιτούνται και αποκτούν ψηφιακό πιστοποιητικό υπογεγραμμένο από Αρχή Πιστοποίησης του ΕΣ. Συνδρομητές στην Υπηρεσία μπορούν να είναι φυσικά πρόσωπα που έχουν συμβατική σχέση με τον ΕΣ, καθώς και συσκευές που λειτουργεί ο ΕΣ.

1.2.4. Οντότητες που βασίζονται στην Υπηρεσία (Relying Parties)

Οι οντότητες που βασίζονται στις παρεχόμενες υπηρεσίες πιστοποίησης ή αλλιώς τα «μέρη που βασίζονται στην υπηρεσία» (Relying Parties) ή απλά «χρήστες» των υπηρεσιών πιστοποίησης μπορεί να είναι οποιεσδήποτε οντότητες, εντός ή εκτός του ΕΣ, οι οποίες χρησιμοποιούν κατ' οποιονδήποτε τρόπο τα τεκμήρια πιστοποίησης (ψηφιακά πιστοποιητικά, ψηφιακές υπογραφές, χρονοσφραγίδες κλπ) και επαφίενται στις πληροφορίες που περιέχουν.

Για την ακρίβεια, οι οντότητες που εμπιστεύονται την Υπηρεσία Πιστοποίησης είναι τα φυσικά ή νομικά πρόσωπα που, αφού ενημερωθούν και συμφωνήσουν με τους όρους και τις προϋποθέσεις χρήσης του πιστοποιητικού που βρίσκονται στο παρόν κείμενο και τη σχετική πολιτική πιστοποιητικού και αφού ελέγξουν και επαληθεύσουν την εγκυρότητα ενός πιστοποιητικού που έχει εκδοθεί από την Υπηρεσία Πιστοποίησης του ΕΣ σύμφωνα με τα παραπάνω, αποφασίζουν τα ίδια αν θα βασισθούν ή όχι στα περιεχόμενα του πιστοποιητικού και κατά συνέπεια να προβούν σε συγκεκριμένες ενέργειες ή να αποκτήσουν τη δικαιολογημένη πεποίθηση για ένα γεγονός.

Για την επαλήθευση της εγκυρότητας ενός πιστοποιητικού, ο χρήστης θα πρέπει να ελέγξει ότι:

- Βρίσκεται εντός της περιόδου ισχύος του, δηλαδή έχει ξεκινήσει και δεν έχει λήξει η ισχύς του,
- Είναι έγκυρα υπογεγραμμένο από έμπιστη Αρχή Πιστοποίησης,
- Δεν έχει ανακληθεί για οποιοδήποτε λόγο,
- Τα στοιχεία ταυτότητας του υποκειμένου που περιέχει ταιριάζουν με τα στοιχεία που παραθέτει ο υπογράφων,
- Η χρήση για την οποία υποβάλλεται το πιστοποιητικό συμφωνεί με την χρήση για την οποία έχει εκδοθεί από την ΑΠ,
- Ακολουθούνται οι όροι και οι συνθήκες που περιγράφονται στο παρόν κείμενο.

1.3. Χρήση των πιστοποιητικών

1.3.1. Κατάλληλες χρήσεις των πιστοποιητικών

Τα πιστοποιητικά μπορούν να χρησιμοποιηθούν μόνο για καθορισμένους σκοπούς, σε όλες τις δικτυακές υπηρεσίες και εφαρμογές, στις οποίες το απαιτούμενο επίπεδο ασφάλειας είναι ίσο ή χαμηλότερο από αυτό της διαδικασίας έκδοσης των πιστοποιητικών.

Ενδεικτικές εφαρμογές στις οποίες μπορούν να χρησιμοποιηθούν τα ψηφιακά πιστοποιητικά που εκδίδονται από την Υπηρεσία είναι οι ακόλουθες:

i. Στην υπογραφή ενός «ηλεκτρονικού εγγράφου» από ένα φυσικό πρόσωπο με τη χρήση του ψηφιακού πιστοποιητικού του και κατά προτίμηση με τη χρήση μιας «ασφαλούς διάταξης δημιουργίας υπογραφής» (π.χ. smart card ή e-token), ώστε να εξασφαλίζονται τουλάχιστο τα παρακάτω χαρακτηριστικά: 1) η αυθεντικότητα της προέλευσης (authenticity), 2) η ακεραιότητα του υπογεγραμμένου κειμένου (integrity) δηλαδή ότι το περιεχόμενό του δεν έχει τροποποιηθεί από τη στιγμή της υπογραφής του, και 3) η δέσμευση του υπογράφοντα ως προς το περιεχόμενο του εγγράφου και η μη άρνηση της υπογραφής του (non-repudiation).
ii. Στην υπογραφή «μηνυμάτων ηλεκτρονικού ταχυδρομείου», για την εξασφάλιση της αυθεντικότητας της διεύθυνσης ηλεκτρονικού ταχυδρομείου του αποστολέα και για όλες τις ιδιότητες που περιγράφηκαν στο α). Επιπλέον μπορούν να χρησιμοποιηθούν για την αποστολή «ασφαλών αποδείξεων παραλαβής μηνυμάτων» (non-repudiation of receipt).
iii. Στην «ισχυρή απόδειξη της ταυτότητας» (Strong Authentication) ενός φυσικού προσώπου ή μιας συσκευής κατά την επικοινωνία τους με άλλες οντότητες, εξασφαλίζοντας επιπλέον χαρακτηριστικά ασφάλειας, ισχυρότερα από αυτά που παρέχει η κλασική μέθοδος πρόσβασης με συνθηματικό χρήστη.
iv. Στην «κρυπτογράφηση εγγράφων και μηνυμάτων» με την χρήση του δημοσίου κλειδιού κάποιας οντότητας, εξασφαλίζοντας ότι μόνο ο επιδιωκόμενος παραλήπτης και κάτοχος του αντίστοιχου ιδιωτικού κλειδιού μπορεί να αποκρυπτογραφήσει και να διαβάσει το έγγραφο ή το μήνυμα.
v. Στην «πιστοποίηση άλλων παρόχων υπηρεσιών πιστοποίησης» είτε πρόκειται για υφιστάμενες Αρχές Πιστοποίησης (Subordinate CAs) είτε πρόκειται για παροχή επιπλέον υπηρεσιών πιστοποίησης όπως για παράδειγμα η χρονοσήμανση, οι συμβολαιογραφικές πράξεις και η μακροπρόθεσμη ασφαλής αποθήκευση δεδομένων.
vi. Στην υλοποίηση ασφαλών δικτυακών πρωτοκόλλων, όπως τα SSL, secure DNS, IPSec κλπ.

1.3.2. Απαγορευμένες χρήσεις των πιστοποιητικών

Τα πιστοποιητικά δεν μπορούν να χρησιμοποιηθούν για συναλλαγές που εμπεριέχουν νομικές δεσμεύσεις.

2. Δημοσιοποίηση και Αποθήκες

2.1. Αποθήκες

Η ΥΔΚ ΕΣ διαθέτει κεντρική αποθήκη δεδομένων όπου δημοσιεύονται κείμενα πολιτικής, πιστοποιητικά Αρχών Πιστοποίησης και τελικά πιστοποιητικά συνδρομητών/συσκευών. Κατά περίπτωση μπορεί να υπάρχουν κατανεμημένες αποθήκες για κάθε ενδιάμεση Αρχή Πιστοποίησης/Αρχή Καταχώρισης που συμμετέχει στην ΥΔΚ.

2.2. Δημοσιοποίηση πληροφοριών της Αρχής Πιστοποίησης

Η ΑΠ τηρεί αποθήκη διαθέσιμη μέσω του διαδικτύου στην οποία δημοσιεύει το Ψηφιακό Πιστοποιητικό της Κεντρικής Αρχής Πιστοποίησης (τύπου X.509.v3), τα Ψηφιακά Πιστοποιητικά που εκδίδονται σύμφωνα με τη Δήλωση Διαδικασιών Πιστοποίησης, την τρέχουσα ΛΑΠ, το κείμενο των Διαδικασιών Πιστοποίησης και άλλα κείμενα σχετικά με τη λειτουργία της (πχ συμφωνίες συνεργασίας).

Η ΑΠ εκτελεί όλες τις ενέργειες για την αδιάλειπτη - κατά το δυνατόν - διαθεσιμότητα της αποθήκης.

2.3. Συχνότητα δημοσιοποίησης

Η η ΛΑΠ θα εκδίδεται τουλάχιστον κάθε πέντε (5) ημέρες. Η ΛΑΠ θα ισχύει για χρονικό διάστημα ίσο πέντε (5) ημέρες. Σε περίπτωση έκθεσης μυστικού κλειδιού συνδρομητή ή άλλου σημαντικού συμβάντος θα εκδίδεται άμεσα ενημερωμένη ΛΑΠ.

Τα πιστοποιητικά που εκδίδονται από την ΑΠ, δημοσιοποιούνται άμεσα, μετά την παραλαβή τους προς τον εγγραφόμενο.

2.4. Έλεγχος Πρόσβασης

Η πρόσβαση στο τμήμα της αποθήκης που περιέχει τα πιστοποιητικά που έχουν εκδοθεί είναι δημόσια και γίνεται μόνο με τη μορφή αναζήτησης. Η αναζήτηση γίνεται είτε με το σειριακό αριθμό του πιστοποιητικού, οπότε προβάλλεται μια εγγραφή, ή με τμήμα του διακεκριμένου ονόματος του αντικειμένου του πιστοποιητικού, οπότε είναι πιθανό να επιστραφεί λίστα πιστοποιητικών.

Ενδέχεται να επιβάλλεται περιορισμένη πρόσβαση στην αποθήκη μόνο για λόγους προστασίας της διαθεσιμότητάς της από επιθέσεις.

3. Αναγνώριση και απόδειξη ταυτότητας

3.1. Ονοματολογία

Τα ονόματα που χρησιμοποιούνται για την έκδοση των πιστοποιητικών εξαρτώνται από την κατηγορία του πιστοποιητικού και ακολουθούν το πρότυπο X.500.

3.1.1. Τύποι ονομάτων

3.1.1.1. Πιστοποιητικά Χρηστών

Τα πιστοποιητικά χρήστη πρέπει να περιλαμβάνουν το ονοματεπώνυμο του χρήστη, την ηλεκτρονική του διεύθυνση, το όνομα της μονάδας στην οποία ανήκει, και το διακριτικό ga=Greek Army.

Επίσης μπορούν να περιλαμβάνονται (προαιρετικά), συμπληρωματικά στοιχεία όπως η οργανωτική υπο-μονάδα στην οποία ανήκει ο χρήστης, τοποθεσία στην οποία βρίσκεται και κατηγορία πιστοποιητικού.

Τα πιστοποιητικά χρηστών εκδίδονται μέσα από signing CA, χωρίς την αποθήκευση του ιδιωτικού κλειδιού.

3.1.1.2. Πιστοποιητικά συσκευών/υπηρεσιών

Τα πιστοποιητικά συσκευής (διακομιστής, δρομολογητής ή άλλη δικτυακή συσκευή) πρέπει να περιλαμβάνουν το πλήρες διακεκριμένο όνομα της συσκευής κατά την υπηρεσία ονοματολογίας (FQDN

DNS), το όνομα της μονάδας στην οποία ανήκει, και το διακριτικό “ga=Greek Army, c=gr”. Δεν επιτρέπεται η πιστοποίηση διευθύνσεων IP ή γενικών ονομάτων συσκευών (hostnames).

Επίσης μπορούν να περιλαμβάνονται (προαιρετικά) συμπληρωματικά στοιχεία όπως η οργανωτική υπο-μονάδα στην οποία ανήκει η συσκευή και η τοποθεσία στην οποία βρίσκεται.

Τα πιστοποιητικά συσκευών/υπηρεσιών εκδίδονται μέσα από crypto CA, κρατώντας ταο ιδιωτικό κλειδί.

3.1.2. Υποχρέωση τα ονόματα να έχουν συγκεκριμένο νόημα

Τα ονόματα που περιλαμβάνονται στα πιστοποιητικά χρηστών, πρέπει να συσχετίζονται με τον συνδρομητή/δικαιούχο του πιστοποιητικού. Πιο συγκεκριμένα, σε ότι αφορά τους χρήστες, το όνομα πρέπει να περιλαμβάνει τα εξής στοιχεία: Όνομα, Επώνυμο, Όνομα Πατρός, Όνομα Μητρός. Από την άλλη, σε ότι αφορά το IT, το όνομα πρέπει να περιλαμβάνει το Domain Name, για το οποίο υπάρχει η προτροπή να μη χρησιμοποιούνται wildcards. Επίσης δεν πρέπει να περιλαμβάνεται στο όνομα η διεύθυνση IP του μηχανήματος, καθώς σε περίπτωση μεταφοράς θα αλλάξει η διεύθυνση.

3.1.3. Δυνατότητα έκδοσης ανώνυμων πιστοποιητικών ή πιστοποιητικών με ψευδώνυμα

Η ΥΔΚ του ΕΕ δεν επιτρέπει την έκδοση πιστοποιητικών σε ανώνυμους χρήστες. Η έκδοση πιστοποιητικών με την ύπαρξη ψευδωνύμων στο διακεκριμένο όνομα π.χ. «Στρατηγός», δεν προβλέπεται στην παρούσα δήλωση διαδικασιών πιστοποίησης αλλά και δεν απαγορεύεται. Για τα συγκεκριμένου τύπου διακριτά ονόματα, μπορεί να δημιουργηθεί ενδιάμεση Αρχή Πιστοποίησης ειδικού σκοπού.

3.1.4. Κανόνες σύνταξης των ονομάτων

Τα ονόματα συντάσσονται ανάλογα με την κατηγορία του πιστοποιητικού. Το όνομα του συνδρομητή που συντάσσεται σύμφωνα με τους κανόνες της παρούσας ενότητας, ονομάζεται Διακεκριμένο Όνομα (ΔΟ).

3.1.4.1. Πιστοποιητικά χρηστών

Στα πιστοποιητικά χρήστη, το ονοματεπώνυμο χρήστη αντιστοιχίζεται στο χαρακτηριστικό «CN», η ηλεκτρονική διεύθυνση στο χαρακτηριστικό «E», το όνομα του φορέα όπου ανήκει στο χαρακτηριστικό «O» ή/και «OU», η χώρα στο χαρακτηριστικό «C», και προαιρετικά, η τοποθεσία όπου βρίσκεται στο χαρακτηριστικό «L». Είναι επιθυμητό, σε κάθε περίπτωση, να ακολουθείται η ονοματοδοσία που χρησιμοποιείται από την εθνική υπηρεσία καταλόγου (σήμερα στεγάζεται στο ds.grnet.gr). Τα Πιστοποιητικά χρηστών του ΕΣ πρέπει στο Διακεκριμένο Όνομα να περιλαμβάνουν τα χαρακτηριστικά “O=Greek Army, C=GR”.

3.1.4.2. Πιστοποιητικά συσκευών/υπηρεσιών

Στα πιστοποιητικά συσκευής, το όνομα της (FQDN κατά DNS) αντιστοιχίζεται στο χαρακτηριστικό «CN», το όνομα του φορέα όπου ανήκει στο χαρακτηριστικό «O» ή/και «OU», η χώρα στο χαρακτηριστικό «C» και προαιρετικά, η τοποθεσία στην οποία βρίσκεται στο χαρακτηριστικό «L». Τα Πιστοποιητικά συσκευών του ΕΣ πρέπει στο Διακεκριμένο Όνομα να περιλαμβάνουν τα χαρακτηριστικά “O=Greek Army, C=GR”.

3.1.4.3. Πιστοποιητικά υπογραφής κώδικα (code signing)

Τα πιστοποιητικά υπογραφής κώδικα (code signing certificates), παρέχονται μέσω των πιστοποιητικών χρηστών. Ο χρήστης, επιπλέον από τους όρους που αναφέρονται στα πιστοποιητικά χρηστών, δεσμεύεται (μέσω τυποποιημένης διαδικασίας της ΑΚ) να παρέχει πλήρεις, ακριβείς και αληθείς πληροφορίες (πχ όνομα εφαρμογής, URL με πληροφορίες της εφαρμογής, περιγραφή εφαρμογής, κ.α.) στον κώδικα που υπογράφει ψηφιακά.

Ο χρήστης που έχει το ρόλο του developer διαθέτει δύο πιστοποιητικά. Το πρώτο πιστοποιητικό αφορά την ιδιότητά του εντός του ΕΣ και το δεύτερο αφορά ο ρόλο του developer.

Επίσης, απαγορεύεται ρητά η ψηφιακή υπογραφή κακόβουλου κώδικα (malware).

Παράβαση των όρων, μπορεί να οδηγήσει σε αυτεπάγγελτη ανάκληση του πιστοποιητικού που υπέγραψε τον κώδικα, καθώς επίσης στην επιβολή των ανάλογων πειθαρχικών και νομικών κυρώσεων απέναντι στον χρήστη με την ιδιότητα του developer.

3.1.5. Μοναδικότητα οντοτήτων

Το Διακεκριμένο Όνομα του εγγραφόμενου με ιδιότητα μέλους του ΕΣ πρέπει να είναι μοναδικό για τη συγκεκριμένη ΑΠ που εκδίδει το πιστοποιητικό, ενώ είναι επιθυμητό να είναι μοναδικό και σε ολόκληρη την ιεραρχία πιστοποίησης του ΕΣ. Επιτρέπεται η έκδοση περισσότερων του ενός πιστοποιητικού με το ίδιο Διακεκριμένο Όνομα μόνο στην περίπτωση διαφορετικής κλάσης ή χρήσης των πιστοποιητικών.

3.2. Αρχική Επαλήθευση ταυτότητας

3.2.1. Τρόπος απόδειξης κατοχής ιδιωτικού κλειδιού

Η Αρχή Καταχώρισης πρέπει να επαληθεύει ότι ο φερόμενος ως συνδρομητής κατέχει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που περιλαμβάνεται στο προς έκδοση πιστοποιητικό. Αυτό επιτυγχάνεται με την εξής διαδικασία :

- Πιστοποιείται η ταυτότητα του συνδρομητή.
- Υποβάλλεται αίτηση για έκδοση πιστοποιητικού η οποία περιέχει το δημόσιο κλειδί του συνδρομητή και έχει υπογραφεί με το ιδιωτικό κλειδί του συνδρομητή.
- Ελέγχεται η αντιστοιχία των κλειδιών.

3.2.2. Απόδειξη ταυτότητας οργανισμού

Η Αρχή Καταχώρισης πρέπει να επιβεβαιώνει ότι ο συνδρομητής ανήκει στον Ελληνικό Στρατό, το όνομα του οποίου περιλαμβάνεται στο πιστοποιητικό.

Ο συνδρομητής πρέπει:

α) να είναι εγγεγραμμένος στην επίσημη υπηρεσία καταλόγου του ΕΣ ή

β) να διαθέτει διεύθυνση ηλεκτρονικού ταχυδρομείου σε επίσημη υπηρεσία του ΕΣ και η διοίκηση του ΕΣ να επιβεβαιώσει τη σχέση του συνδρομητή.

3.2.3. Απόδειξη ταυτότητας φυσικού προσώπου

3.2.3.1. Πρόσωπο που αιτείται την έκδοση πιστοποιητικού

Όλα τα πιστοποιητικά φυσικών προσώπων που εκδίδονται στον Ελληνικό Στρατό πρέπει να ελέγχονται για ταυτοπροσωπία. Προβλέπονται δύο κλάσεις πιστοποιητικών χρηστών. Η κλάση Α περιλαμβάνει πιστοποιητικά των οποίων το ιδιωτικό κλειδί δημιουργείται και παραμένει εντός κάποιας ασφαλής κρυπτοσυσκευής (eToken ή smartcatd) και πιστοποιούνται παρουσία εξουσιοδοτημένου προσωπικού της Αρχής Καταχώρισης. Η κλάση Β, περιλαμβάνει πιστοποιητικά των οποίων το ιδιωτικό κλειδί δημιουργείται με χρήση κάποιου λογισμικού (software certificate store). Διευκρινίζεται ότι και στις δύο κλάσεις πιστοποιητικών, υπάρχει ασφαλής ταυτοποίηση του δικαιούχου με φυσική παρουσία και εμφάνιση αποδεκτού επίσημου εγγράφου που αποδεικνύει την ταυτότητα του αιτούντος.

Η Αρχή Καταχώρισης εκχωρεί τον έλεγχο της ταυτότητας σε υπηρεσίες των μονάδων όπου ανήκουν οι συνδρομητές και χρησιμοποιεί τρόπους πιστοποίησης ταυτότητας του χρήστη που είναι διαθέσιμοι στις μονάδες για να εκτελέσει τον έλεγχο ταυτότητας. Οι συνεργαζόμενες μονάδες είναι υποχρεωμένες να έχουν πιστοποιήσει την ταυτότητα του χρήστη από κάποιο επίσημο έγγραφο που φέρει τη φωτογραφία του δικαιούχου (π.χ. αστυνομική ταυτότητα, διαβατήριο, δίπλωμα οδήγησης, στρατιωτική ταυτότητα) και το οποίο θεωρείται αξιόπιστο από την οικεία μονάδα. Εναλλακτικά, η ίδια η ΑΚ του ΕΣ μπορεί να εκτελέσει την παραπάνω διαδικασία ταυτοποίησης του αιτούντος.

Εφόσον η οικεία μονάδα του χρήστη, σύμφωνα με την πολιτική της, έχει ήδη εκτελέσει διαδικασία φυσικής ταυτοποίησης του χρήστη στο παρελθόν (π.χ. για την εκχώρηση ισχυρού κωδικού πρόσβασης ή λογαριασμού e-mail) τότε δεν είναι απαραίτητη η επανάληψη της διαδικασίας, αλλά θεωρείται αρκετή μία τυπική επιβεβαίωση της αίτησης μέσω της πιστοποιημένης διεύθυνσης ηλεκτρονικής αλληλογραφίας.

Τα πιστοποιητικά της κλάσης Α πρέπει να περιέχουν ένα επιπλέον πεδίο οργανωτικής μονάδας (OU) στο πεδίο του αντικειμένου με τιμή ‘Class A – Private Key created and stored in hardware CSP ’. Τα πιστοποιητικά της κλάσης Β πρέπει να περιέχουν ένα επιπλέον πεδίο οργανωτικής μονάδας (OU) στο πεδίο του αντικειμένου με τιμή ‘Class B – Private Key created and stored in software CSP ’.

3.2.3.2. Πρόσωπο που αιτείται πιστοποιητικό συσκευής

Το άτομο που δηλώνει αρμόδιος για τη λειτουργία και τη συμμόρφωση της συσκευής στην πολιτική πιστοποίησης, πρέπει να είναι κάτοχος πιστοποιητικού που έχει εκδοθεί από ΑΠ η οποία συμμορφώνεται με τη «Δήλωση Διαδικασιών Πιστοποίησης/Πολιτική Πιστοποίησης του ΕΣ».

Ο συνδρομητής συμπληρώνει την αίτηση για έκδοση πιστοποιητικού σε ιστοσελίδα όπου πρέπει να πιστοποιηθεί η ταυτότητά του παρουσιάζοντας το προσωπικό πιστοποιητικό του. Έπειτα, αποστέλλεται ένα μήνυμα e-mail σε εξουσιοδοτημένο Διαχειριστή του RA ο οποίος ελέγχει το FQDN του αιτήματος αν είναι έγκυρο καθώς και αν ο χρήστης που αιτείται το πιστοποιητικό είναι διαχειριστής του συγκεκριμένου FQDN μέσω του μητρώου χρηστών/υπολογιστών που τηρείται στο ΕΣ.

3.2.4. Μη επιβεβαιωμένα στοιχεία του συνδρομητή

Τα πιστοποιητικά που εκδίδονται δεν περιλαμβάνουν μη επιβεβαιωμένα στοιχεία του συνδρομητή.

3.2.5. Επικύρωση ιδιότητας αιτούμενου

Οι Αρχές Καταχώρισης διαθέτουν διαδικασίες με τις οποίες πιστοποιείται και επικυρώνεται η ιδιότητα του κάθε συνδρομητή και η συμβατική του σχέση με τον ΕΣ. Αυτό γίνεται είτε με ηλεκτρονικές λίστες που

συγκεντρώνει η κάθε ΑΚ από τις αρμόδιες -για κάθε κατηγορία- πηγές, είτε με προσκόμιση επικυρωμένων έγγραφων βεβαιώσεων των συνδρομητών όπου πιστοποιείται η σχέση του ενδιαφερόμενου με τον ΕΣ.

3.3. Επαλήθευση ταυτότητας για έκδοση νέων κλειδιών-πιστοποιητικών

3.3.1. Επαλήθευση ταυτότητας για συνηθισμένη αίτηση έκδοσης νέου κλειδιού-πιστοποιητικού

Ο χρήστης μπορεί να αιτηθεί την έκδοση νέου κλειδιού-Πιστοποιητικού του δεκαπέντε (15) μέρες πριν την λήξη του ισχύοντος πιστοποιητικού, ακολουθώντας την διαδικασία που περιγράφεται στην παράγραφο 3.2.

3.3.2. Επαλήθευση ταυτότητας και εξουσιοδότηση για αίτηση έκδοσης νέου κλειδιού-πιστοποιητικού μετά από ανάκληση

Ο χρήστης μπορεί να αιτηθεί την έκδοση νέου κλειδιού-Πιστοποιητικού αμέσως μετά την ανάκληση του αρχικού πιστοποιητικού του, ακολουθώντας την διαδικασία που περιγράφεται στην παράγραφο 3.2.

3.3.3. Επαλήθευση ταυτότητας για αιτήματα ανάκλησης

Η ΑΠ και ο συνδρομητής συμφωνούν κατά την παραλαβή του πιστοποιητικού, μυστικό ισχυρό κωδικό ανάκλησης του πιστοποιητικού. Ο συνδρομητής μπορεί να αιτηθεί την ανάκληση του πιστοποιητικού του μέσω κατάλληλης ιστοσελίδας, με τη χρήση του μυστικού ισχυρού κωδικού ανάκλησης. Εναλλακτικά, μπορεί να ζητηθεί ανάκληση πιστοποιητικού με τηλεφωνική επικοινωνία του εγγραφόμενου με την αρμόδια Αρχή Πιστοποίησης, οπότε και θα πρέπει να ακολουθήσει επιβεβαίωση της ταυτότητάς του.

4. Απαιτήσεις λειτουργίας, κύκλος ζωής πιστοποιητικών

4.1. Επεξεργασία των αιτήσεων πιστοποιητικών

4.1.1. Διαδικασίες ελέγχου ταυτότητας και ιδιότητας συνδρομητή

Όλα τα αιτήματα ελέγχονται ως προς την εγκυρότητά τους. Ελέγχονται επίσης η απόδειξη ταυτότητας των δικαιούχων συνδρομητών καθώς και η ύπαρξη ή όχι συμβατικής σχέσης τους με τον ΕΣ.

4.1.2. Έγκριση ή απόρριψη αιτήσεων πιστοποιητικών

Μετά από όλους τους ελέγχους ταυτότητας/ιδιότητας του αιτούμενου συνδρομητή, ελέγχεται και το περιεχόμενο της αίτησης ψηφιακού πιστοποιητικού. Σε περίπτωση που ο αιτούμενος δεν δικαιούται ψηφιακό πιστοποιητικό ή η ψηφιακή αίτηση περιέχει σφάλματα, η αίτηση απορρίπτεται. Διαφορετικά η αίτηση εγκρίνεται.

4.1.3. Χρόνος επεξεργασίας αιτήσεων πιστοποιητικών

Τα αιτήματα πιστοποιητικών εξυπηρετούνται σε διάστημα το πολύ δέκα (10) εργάσιμων ημερών, εκτός από τις περιπτώσεις ανωτέρας βίας.

4.2. Έκδοση πιστοποιητικών

4.2.1. Διαδικασίες Αρχών Πιστοποίησης κατά την έκδοση Πιστοποιητικών

Τα πιστοποιητικά εκδίδονται μετά την ασφαλή μεταφορά των αιτήσεων από την Αρχή Καταχώρισης στην ΑΠ και μετά από έλεγχο του διακεκριμένου ονόματος του πιστοποιητικού. Το διακεκριμένο όνομα του πιστοποιητικού του αιτούντος πρέπει να είναι σύμφωνο με όσα αναφέρονται στην παράγραφο 3.1.

4.2.2. Ενημέρωση του συνδρομητή από την ΑΠ σχετικά με την έκδοση του πιστοποιητικού

Η ΑΠ ενημερώνει το συνδρομητή για την έκδοση ή απόρριψη έκδοσης του πιστοποιητικού με ηλεκτρονικό ταχυδρομείο. Στο ίδιο μήνυμα και εφόσον η αίτηση έχει γίνει αποδεκτή, ζητείται από το συνδρομητή η αποδοχή και παραλαβή του πιστοποιητικού από συγκεκριμένη ιστοσελίδα της ΑΚ.

4.3. Αποδοχή των πιστοποιητικών

4.3.1. Συμπεριφορά που διέπει την παραλαβή πιστοποιητικών

Οι συνδρομητές της ΥΔΚ ΕΣ, πρέπει να παραλάβουν (να ανακτήσουν και να εγκαταστήσουν) το νέο πιστοποιητικό μέσα σε τριάντα (30) ημέρες, διαφορετικά το Πιστοποιητικό αυτόματα ανακαλείται και ο συνδρομητής πρέπει να κάνει εκ νέου αίτηση. Προκειμένου να ανακτήσουν το πιστοποιητικό τους, δηλώνουν σε συγκεκριμένη ιστοσελίδα ότι έχουν ελέγξει όλα τα στοιχεία του πιστοποιητικού, ότι αυτά είναι σωστά και αληθή και τέλος αποδέχονται και παραλαμβάνουν το πιστοποιητικό.

4.3.2. Δημοσίευση πιστοποιητικών από τις ΑΠ

Οι ΑΠ δημοσιεύουν τα πιστοποιητικά μόνο εφόσον έχει γίνει παραλαβή τους από τους δικαιούχους.

4.4. Ζεύγος κλειδιών και χρήσεις των πιστοποιητικών

4.4.1. Υποχρεώσεις συνδρομητών σχετικά με τη χρήση ιδιωτικών κλειδιών και πιστοποιητικών

Οι συνδρομητές της ΥΔΚ ΕΣ επιτρέπεται να χρησιμοποιούν τα ιδιωτικά κλειδιά και τα πιστοποιητικά τους σε χρήσεις για τις οποίες αυτά έχουν εκδοθεί.

4.4.2. Υποχρεώσεις μερών που βασίζονται στην υπηρεσία (Relying parties) σχετικά με τη χρήση των δημοσίων κλειδιών και πιστοποιητικών

Τα μέρη που βασίζονται στην υπηρεσία μπορούν να χρησιμοποιούν τα δημόσια κλειδιά και τα πιστοποιητικά των συνδρομητών της Υποδομής Δημοσίου Κλειδιού ΕΣ. Οι λειτουργίες που μπορούν να εκτελέσουν είναι:

- Επαλήθευση ψηφιακά υπογεγραμμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου μέσω πρωτοκόλλου S/MIME
- Κρυπτογράφηση μηνυμάτων ηλεκτρονικού ταχυδρομείου μέσω πρωτοκόλλου S/MIME
- Επαλήθευση ψηφιακά υπογεγραμμένων κειμένων/κώδικα εφαρμογών
- Επαλήθευση ψηφιακών χρονοσφραγίδων σε κείμενα
- Κρυπτογράφηση αρχείων και δεδομένων καθώς και καναλιών επικοινωνίας
- Έλεγχος ταυτότητας (authentication)
- Έλεγχος δικαιώματος πρόσβασης (authorization)

4.5. Ανανέωση πιστοποιητικών

4.5.1. Συνθήκες κατά τις οποίες μπορεί να γίνει ανανέωση πιστοποιητικών

Ανανεώσεις πιστοποιητικών επιτρέπονται εφόσον δεν ξεπεραστεί το χρονικό όριο ισχύος των κλειδιών που συνοδεύουν τα πιστοποιητικά. Η μέγιστη διάρκεια χρήσης των κλειδιών ορίζεται σε δέκα (10) έτη για Κεντρική ΑΠ, σε πέντε (5) έτη για ενδιάμεση ΑΠ και σε τρία (3) έτη για πιστοποιητικά τελικών χρηστών και συσκευών. Η διάρκεια χρήσης σε κάθε περίπτωση θα πρέπει να αποφασίζεται σε συνάρτηση με το

μέγεθος των κλειδιών και με τις τρέχουσες τεχνολογικές εξελίξεις στο χώρο της κρυπτογραφίας, έτσι ώστε να εξασφαλίζεται το βέλτιστο επίπεδο ασφάλειας αλλά και αποτελεσματικότητας χρήσης.

4.5.2. Ποιος μπορεί να καταθέσει αίτημα ανανέωσης πιστοποιητικού

Το αίτημα ανανέωσης κατατίθεται από τον ίδιο τον δικαιούχο συνδρομητή μέσω πιστοποιημένης ιστοσελίδας μετά από διαδικασία ελέγχου ταυτότητας (authentication) στην οποία επιλέγει την ανανέωση

4.5.3. Διαδικασίες των ΑΚ, ΑΠ για επεξεργασία αιτημάτων ανανέωσης

- Αρχικά ελέγχεται αν έχουν γίνει ανανεώσεις του ίδιου πιστοποιητικού στο παρελθόν
- Στη συνέχεια ελέγχεται αν το πιστοποιητικό ή τα πιστοποιητικά που περιείχαν το ίδιο κλειδί βρίσκονται σε ισχύ για μικρότερο χρονικό διάστημα από τη μέγιστη διάρκεια ισχύος του κλειδιού.
- Για το υπόλοιπο επιτρεπόμενο χρονικό διάστημα εκδίδεται νέο πιστοποιητικό χρησιμοποιώντας το αρχικό certificate request που βρίσκεται αποθηκευμένο στην Αρχή Καταχώρισης.

Για παράδειγμα, ένας χρήστης που έχει ενεργό πιστοποιητικό το οποίο ισχύει για ένα χρόνο, μπορεί να το ανανεώσει (χωρίς να αλλάξει το ιδιωτικό κλειδί) για άλλο ένα έτος, επειδή η μέγιστη διάρκεια ισχύος ιδιωτικού κλειδιού για πιστοποιητικά χρηστών είναι δύο (2) χρόνια.

4.5.4. Ενημέρωση συνδρομητών για τα ανανεωμένα πιστοποιητικά

Η ΑΠ ενημερώνει το συνδρομητή για την ανανέωση του πιστοποιητικού με ηλεκτρονικό ταχυδρομείο. Στο ίδιο μήνυμα και εφόσον η ανανέωση έχει γίνει αποδεκτή, ζητείται από το συνδρομητή η αποδοχή και παραλαβή του πιστοποιητικού από συγκεκριμένη ιστοσελίδα της ΑΚ.

4.5.5. Αποδοχή ανανεωμένων πιστοποιητικών

Οι συνδρομητές της ΥΔΚ ΕΣ, πρέπει να παραλάβουν το ανανεωμένο πιστοποιητικό μέσα σε τριάντα (30) ημέρες, διαφορετικά το Πιστοποιητικό αυτόματα ανακαλείται και ο συνδρομητής πρέπει να κάνει εκ νέου αίτηση. Προκειμένου να ανακτήσουν το πιστοποιητικό τους, δηλώνουν σε συγκεκριμένη ιστοσελίδα ότι έχουν ελέγξει όλα τα στοιχεία του πιστοποιητικού, ότι αυτά είναι σωστά και αληθή και τέλος αποδέχονται και παραλαμβάνουν το πιστοποιητικό.

4.5.6. Δημοσίευση ανανεωμένων πιστοποιητικών

Οι ΑΠ δημοσιεύουν τα πιστοποιητικά μόνο εφόσον έχει γίνει παραλαβή τους από τους δικαιούχους.

4.6. Επανέκδοση κλειδιών

4.6.1. Συνθήκες κατά τις οποίες μπορεί να γίνει επανέκδοση κλειδιών

Επανέκδοση κλειδιών πιστοποιητικών επιτρέπονται όταν πλησιάζει η λήξη ισχύοντος πιστοποιητικού ή όταν έχει ανακληθεί πιστοποιητικό και πρέπει να εκδοθεί καινούριο.

4.6.2. Πώς μπορεί να γίνει αίτημα επανέκδοσης κλειδιών πιστοποιητικών

Οι δικαιούχοι συνδρομητές, λαμβάνουν μήνυμα ηλεκτρονικού ταχυδρομείου από την Αρχή Καταχώρισης δεκαπέντε (15) μέρες πριν τη λήξη του πιστοποιητικού τους και ενημερώνονται για την επικείμενη λήξη του. Οι δικαιούχοι στη συνέχεια καταθέτουν αίτημα επανέκδοσης μέσω πιστοποιημένης ιστοσελίδας μετά από διαδικασία ελέγχου ταυτότητας (authentication) στην οποία επιλέγουν έκδοση νέου πιστοποιητικού.

4.6.3. Διαδικασίες των ΑΚ, ΑΠ για αιτήματα επανέκδοσης κλειδιών

Τα κλειδιά εκδίδονται μετά την ασφαλή μεταφορά των αιτήσεων από την Αρχή Καταχώρισης στην ΑΠ και μετά από έλεγχο του διακεκριμένου ονόματος του πιστοποιητικού.

4.6.4. Ενημέρωση συνδρομητών για τα πιστοποιητικά όπου πραγματοποιήθηκε επανέκδοση κλειδιού

Η ΑΠ ενημερώνει το συνδρομητή για την έκδοση ή απόρριψη έκδοσης του κλειδιού με ηλεκτρονικό ταχυδρομείο. Στο ίδιο μήνυμα και εφόσον η αίτηση έχει γίνει αποδεκτή, ζητείται από το συνδρομητή η αποδοχή και παραλαβή του κλειδιού από συγκεκριμένη ιστοσελίδα της ΑΚ.

4.6.5. Αποδοχή πιστοποιητικών στα οποία επανεκδόθηκε κλειδί

Οι συνδρομητές της ΥΔΚ ΕΣ, πρέπει να παραλάβουν το νέο κλειδί μέσα σε τριάντα (30) ημέρες, διαφορετικά το κλειδί αυτόματα ανακαλείται και ο συνδρομητής πρέπει να κάνει εκ νέου αίτηση. Προκειμένου να ανακτήσουν το κλειδί τους, δηλώνουν σε συγκεκριμένη ιστοσελίδα ότι έχουν ελέγξει όλα τα στοιχεία του κλειδιού, ότι αυτά είναι σωστά και αληθή και τέλος αποδέχονται και παραλαμβάνουν το κλειδί.

4.6.6. Δημοσίευση πιστοποιητικών στα οποία επανεκδόθηκε κλειδί

Οι ΑΠ δημοσιεύουν τα πιστοποιητικά μόνο εφόσον έχει γίνει παραλαβή τους από τους δικαιούχους.

4.7. Μεταβολή Πιστοποιητικών

4.7.1. Συνθήκες κατά τις οποίες μπορεί να γίνει μεταβολή πιστοποιητικών

Μεταβολή στοιχείων πιστοποιητικών δεν επιτρέπονται. Σε περίπτωση που έχει γίνει λάθος κατά την έκδοση του πιστοποιητικού (ορθογραφικό ή άλλο), το πιστοποιητικό ανακαλείται και ακολουθείται η διαδικασία έκδοσης νέου πιστοποιητικού.

4.8. Αναστολή και ανάκληση πιστοποιητικών

4.8.1. Περιπτώσεις ανάκλησης

Το πιστοποιητικό ανακαλείται όταν αυτό δεν χρησιμοποιείται πλέον, όταν τα στοιχεία που περιέχει έχουν αλλάξει και όταν έχει εκτεθεί ή χαθεί ή υπάρχει υποψία ότι έχει εκτεθεί ή χαθεί το ιδιωτικό κλειδί. Επίσης, το πιστοποιητικό ανακαλείται όταν δεν το παραλάβει ο συνδρομητής μέσα στο χρονικό διάστημα που ορίζεται ή αν αποδειχθεί ότι η χρήση του δεν είναι σύμφωνη με τη δήλωση διαδικασιών πιστοποίησης/πολιτική πιστοποίησης. Τέλος, ανακαλείται εάν το πιστοποιητικό περιέχει λανθασμένες πληροφορίες.

Λόγος ανάκλησης είναι και η απώλεια της ιδιότητας ή της σχέσης, εργασιακής ή άλλης, του κατόχου με τον Ελληνικό Στρατό, ή με τη συγκεκριμένη μονάδα του στην οποία ανήκε όταν πιστοποιήθηκε.

4.8.2. Ποιος μπορεί να αιτηθεί ανάκληση

Το πιστοποιητικό ανακαλείται από τον ίδιο τον συνδρομητή ή από άλλη οντότητα η οποία μπορεί να αποδείξει την έκθεση του μυστικού κλειδιού ή την εκτός πολιτικής πιστοποίησης χρήση του πιστοποιητικού.

Οι υπηρεσίες προσωπικού των μονάδων του ΕΣ, αιτούνται ανάκληση για τα άτομα που χάνουν την ιδιότητα υπό την οποία πιστοποιήθηκαν.

4.8.3. Διαδικασία αιτήματος ανάκλησης

4.8.3.1. Ανάκληση του πιστοποιητικού από το συνδρομητή

Η ΑΠ και ο συνδρομητής συμφωνούν κατά την παραλαβή του πιστοποιητικού, μυστικό ισχυρό κωδικό ανάκλησης του πιστοποιητικού. Ο συνδρομητής μπορεί να αιτηθεί την ανάκληση του πιστοποιητικού του μέσω κατάλληλης ιστοσελίδας, με τη χρήση του μυστικού ισχυρού κωδικού ανάκλησης. Εναλλακτικά, μπορεί να ζητηθεί ανάκληση πιστοποιητικού με τηλεφωνική επικοινωνία του εγγραφόμενου με την αρμόδια Αρχή Πιστοποίησης, οπότε και θα πρέπει να ακολουθήσει επιβεβαίωση της ταυτότητάς του.

4.8.3.2. Ανάκληση του πιστοποιητικού από άλλη οντότητα

Απαιτείται κατά περίπτωση η υποβολή απόδειξης ότι α) έχει εκτεθεί το ιδιωτικό κλειδί του πιστοποιητικού ή β) η χρήση του πιστοποιητικού δεν είναι σύμφωνη με τη πολιτική πιστοποίησης, ή γ) έχει πάψει να υφίσταται η συμβατική σχέση του κατόχου του πιστοποιητικού με το ΕΣ.

4.8.4. Χρονική περίοδος στην οποία ο συνδρομητής μπορεί να καταθέσει αίτημα ανάκλησης

Ο συνδρομητής μπορεί να καταθέσει αίτημα ανάκλησης οποιαδήποτε στιγμή μέσα στη διάρκεια ισχύος του αρχικού πιστοποιητικού. Ανακλήσεις πιστοποιητικών μπορούν επίσης να γίνουν εφόσον η ΑΠ που τα εξέδωσε συνεχίζει να βρίσκεται σε λειτουργία.

4.8.5. Χρόνος απόκρισης της Υπηρεσίας Πιστοποίησης για ανακλήσεις πιστοποιητικών

Οι Αρχές Πιστοποίησης οφείλουν να επεξεργάζονται τα αιτήματα ανάκλησης εντός μίας (1) εργάσιμης ημέρας εκτός περιπτώσεων ανωτέρας βίας.

4.8.6. Μηχανισμοί με τους οποίους μέρη που βασίζονται στην υπηρεσία (Relying Parties) θα ελέγχουν την κατάσταση των πιστοποιητικών πάνω στα οποία θα βασίζονται.

Τα μέρη που βασίζονται στην υπηρεσία θα πρέπει κάθε φορά πριν εμπιστευθούν οποιοδήποτε πιστοποιητικό της ΥΔΚ ΕΣ, να μεταφορτώνουν τις Λίστες Ανάκλησης Πιστοποιητικών όλων των ενδιάμεσων Αρχών Πιστοποίησης που μεσολαβούν μέχρι την εκδότρια αρχή του τελικού πιστοποιητικού. Οι λίστες ανάκλησης βρίσκονται πάντα δημοσιευμένες στην Αποθήκη.

4.8.7. Συχνότητα έκδοσης ΛΑΠ

Η ΛΑΠ θα εκδίδεται τουλάχιστον κάθε πέντε (5) ημέρες. Η ΛΑΠ θα ισχύει για χρονικό διάστημα ίσο πέντε (5) ημέρες.

Σε περίπτωση έκθεσης μυστικού κλειδιού συνδρομητή ή άλλου σημαντικού συμβάντος θα εκδίδεται άμεσα ενημερωμένη ΛΑΠ.

4.8.8. Χρόνος δημοσίευσης ΛΑΠ στην αποθήκη

Μετά από την ανάκληση κάποιου πιστοποιητικού εκδίδεται η ΛΑΠ και ενημερώνεται η αποθήκη. Ο χρόνος που μεσολαβεί μεταξύ έκδοσης ΛΑΠ και δημοσίευσής της στην αποθήκη είναι της τάξης των λεπτών της ώρας. Στην αποθήκη το πιστοποιητικό χαρακτηρίζεται ως ανακληθέν.

Κατά την ανάκληση πιστοποιητικού ειδοποιείται ο συνδρομητής και ο υπεύθυνος ασφαλείας της ΑΠ σε περίπτωση έκθεσης ιδιωτικού κλειδιού.

4.8.9. Διαθεσιμότητα υπηρεσίας ελέγχου κατάστασης πιστοποιητικών σε πραγματικό χρόνο (OCSP)

Στην ΥΔΚ ΕΣ λειτουργεί υπηρεσία ελέγχου κατάστασης πιστοποιητικών σε πραγματικό χρόνο (On-line Certificate Status Protocol – OCSP). Η διεύθυνση της υπηρεσίας είναι ενσωματωμένη στα πιστοποιητικά που εκδίδονται.

4.8.10. Απαιτήσεις μερών που βασίζονται στην υπηρεσία (Relying Parties) για να ελέγχουν την κατάσταση των πιστοποιητικών πάνω στα οποία θα βασίζονται μέσω OCSP.

Τα μέρη που βασίζονται στην υπηρεσία θα πρέπει κάθε φορά πριν εμπιστευθούν οποιοδήποτε πιστοποιητικό της ΥΔΚ ΕΣ, να ελέγχουν την υπηρεσία OCSP της ΥΔΚ ΕΣ και να ρωτούν για την κατάσταση όλων των ενδιάμεσων Αρχών Πιστοποίησης που μεσολαβούν μέχρι την εκδότρια αρχή του τελικού πιστοποιητικού, καθώς και για την κατάσταση του τελικού πιστοποιητικού. Η διεύθυνση της υπηρεσίας OCSP βρίσκεται ενσωματωμένη σε κάθε πιστοποιητικό που έχει εκδοθεί.

4.8.11. Άλλες μορφές ανακοίνωσης ανάκλησης πιστοποιητικών

Στην αποθήκη πιστοποιητικών όπου λειτουργεί αναζήτηση πιστοποιητικών μέσω ιστοσελίδας, τα πιστοποιητικά που ανακαλούνται εμφανίζονται στην περιγραφή τους ως «Ανακληθέντα»

4.9. Υπηρεσίες ελέγχου κατάστασης πιστοποιητικών

4.9.1. Χαρακτηριστικά λειτουργίας

Τα μέρη που βασίζονται στην υπηρεσία, προκειμένου να αποφανθούν για την εγκυρότητα ή μη κάποιων πιστοποιητικών, μπορούν να χρησιμοποιήσουν μια από τις παρακάτω προσφερόμενες υπηρεσίες ελέγχου κατάστασης ή συνδυασμό τους.

4.9.1.1. Υπηρεσία ελέγχου κατάστασης πιστοποιητικών πραγματικού χρόνου OCSP

Τα μέρη που βασίζονται στην υπηρεσία θα πρέπει κάθε φορά πριν εμπιστευθούν οποιοδήποτε πιστοποιητικό της ΥΔΚ ΕΣ, να ελέγχουν την υπηρεσία OCSP της ΥΔΚ ΕΣ και να ρωτούν για την κατάσταση όλων των ενδιάμεσων Αρχών Πιστοποίησης που μεσολαβούν μέχρι την εκδότρια αρχή του τελικού πιστοποιητικού, καθώς και για την κατάσταση του τελικού πιστοποιητικού. Η διεύθυνση της υπηρεσίας OCSP βρίσκεται ενσωματωμένη σε κάθε πιστοποιητικό που έχει εκδοθεί.

4.9.1.2. On-line Αποθήκη πιστοποιητικών

Η on-line αποθήκη πιστοποιητικών, προσφέρει ένα περιβάλλον αναζήτησης πιστοποιητικών μέσω ιστοσελίδων, στο οποίο γίνονται ερωτήσεις που μπορεί να περιλαμβάνουν το σειριακό αριθμό ή τμήμα του διακεκριμένου ονόματος των πιστοποιητικών. Στα αποτελέσματα των αναζητήσεων, εμφανίζονται τα στοιχεία των πιστοποιητικών και μια περιγραφή που αναφέρει αν το πιστοποιητικό βρίσκεται σε ισχύ ή αν έχει ανακληθεί. Η αποθήκη πρέπει να εμφανίζει όλα τα πιστοποιητικά που έχουν εκδοθεί/ανακληθεί, για όσο διάστημα είναι λειτουργική η ΥΔΚ ΕΣ.

4.9.1.3. Χρήση των Λιστών Ανάκλησης Πιστοποιητικών (ΛΑΠ)

Τα μέρη που βασίζονται στην υπηρεσία θα πρέπει κάθε φορά πριν εμπιστευθούν οποιοδήποτε πιστοποιητικό της ΥΔΚ ΕΣ, να μεταφορτώνουν τις Λίστες Ανάκλησης Πιστοποιητικών όλων των ενδιάμεσων Αρχών Πιστοποίησης που μεσολαβούν μέχρι την εκδότρια αρχή του τελικού πιστοποιητικού. Οι λίστες ανάκλησης βρίσκονται πάντα δημοσιευμένες στην Αποθήκη.

4.9.2. Διαθεσιμότητα υπηρεσίας ελέγχου κατάστασης πιστοποιητικών

Θα καταβάλλεται προσπάθεια για πολύ υψηλή διαθεσιμότητα (~99%) των υπηρεσιών ελέγχου κατάστασης πιστοποιητικών.

4.10. Λήξη συνδρομής

Μετά τη λήξη της χρονικής ισχύος των πιστοποιητικών της ΥΔΚ ΕΣ, δεν είναι απαραίτητη η ανάκλησή τους παρά μόνο αν συντρέχει κάποιος από τους λόγους που αναφέρονται στην παράγραφο 4.9.1. Πιο συγκεκριμένα, το πιστοποιητικό ανακαλείται όταν αυτό δεν χρησιμοποιείται πλέον, όταν τα στοιχεία που περιέχει έχουν αλλάξει και όταν έχει εκτεθεί ή χαθεί ή υπάρχει υποψία ότι έχει εκτεθεί ή χαθεί το ιδιωτικό κλειδί. Επίσης, το πιστοποιητικό ανακαλείται όταν δεν το παραλάβει ο συνδρομητής μέσα στο χρονικό διάστημα που ορίζεται ή αν αποδειχθεί ότι η χρήση του δεν είναι σύμφωνη με τη δήλωση διαδικασιών πιστοποίησης/πολιτική πιστοποίησης. Τέλος, ανακαλείται εάν το πιστοποιητικό περιέχει λανθασμένες πληροφορίες.

Λόγος ανάκλησης είναι και η απώλεια της ιδιότητας ή της σχέσης, εργασιακής ή άλλης, του κατόχου με τον Ελληνικό Στρατό, ή με τη συγκεκριμένη μονάδα του στην οποία ανήκε όταν πιστοποιήθηκε.

5. Διοικητικοί, τεχνικοί και λειτουργικοί έλεγχοι

5.1. Φυσική ασφάλεια και έλεγχος πρόσβασης

5.1.1. Τοποθεσία εγκαταστάσεων

Οι εν λόγω έλεγχοι αναφέρονται σε όλες τις στρατιωτικές εγκαταστάσεις, καθώς και στα επιμέρους τμήματα κάθε εγκατάστασης.

5.1.2. Φυσική πρόσβαση

Η φυσική πρόσβαση στον εξοπλισμό των ΑΠ και της Αρχής Καταχώρισης επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό. Απαγορεύεται η σύνδεση της ΚΑΠ σε δίκτυο ή οποιοδήποτε τηλεπικοινωνιακό μέσο.

Επίσης, κατά την είσοδο σε κάθε στρατιωτική εγκατάσταση και σε κάθε επιμέρους τμήμα υπάρχει αυστηρός έλεγχος προς όλους τους εισερχόμενους.

5.1.3. Κλιματισμός και ρύθμιση τροφοδοσίας με ρεύμα

Όλος ο εξοπλισμός της Υποδομής Δημοσίου Κλειδιού που είναι υπό τη διαχείριση του ΚΛΔ ΕΣ, βρίσκεται σε κλιματιζόμενους χώρους με παροχή ρεύματος που προστατεύεται από μονάδες αδιάλειπτης παροχής (UPS) και εφεδρικά ηλεκτροπαραγωγά ζεύγη.

5.1.4. Έκθεση σε νερό

Ο εξοπλισμός της ΥΔΚ που είναι υπό τη διαχείριση του ΚΛΔ ΕΣ βρίσκεται σε χώρο που δεν κινδυνεύει σε μεγάλο βαθμό από πλημμύρες.

5.1.5. Πρόληψη και προστασία από φωτιά

Οι εγκαταστάσεις του ΚΛΔ ΕΣ υπόκεινται στην ελληνική νομοθεσία σχετικά με την πρόληψη και την προστασία πυρκαγιάς στα δημόσια κτίρια.

5.1.6. Αποθηκευτικά μέσα

Τα ιδιωτικά κλειδιά των Αρχών Πιστοποίησης πρέπει να βρίσκονται σε αποσπώμενα αποθηκευτικά μέσα (CD Roms) ή άλλο αφαιρούμενο μέσο σε κρυπτογραφημένη μορφή, με ισχυρό κωδικό (passphrase) που γνωρίζει μόνο εξουσιοδοτημένο προσωπικό του ΕΣ και μάλιστα τμηματικά. Κανένα μέλος του προσωπικού δεν μπορεί –ατομικά- να γνωρίζει το σύνολο του ισχυρού κωδικού κρυπτογράφησης ενός ιδιωτικού κλειδιού.

Αντίγραφα ασφαλείας όλης της Υποδομής Δημοσίου Κλειδιού του ΕΣ, βρίσκονται σε μαγνητικές ταινίες ή memory flash disks που κατέχουν εξουσιοδοτημένα στελέχη του ΕΣ.

Και τα δύο παραπάνω αποθηκευτικά μέσα βρίσκονται σε φυσικές τοποθεσίες διαφορετικές από το ΚΛΔ ΕΣ, προστατευμένα από έκθεση σε νερό και φωτιά.

5.1.7. Διάθεση απορριμμάτων

Απορρίμματα που περιέχουν οποιαδήποτε εμπιστευτική πληροφορία όπως εύκαμπτοι μαγνητικοί δίσκοι, σκληροί δίσκοι κ.α. καταστρέφονται πριν απορριφθούν.

5.1.8. Τήρηση αντιγράφων ασφαλείας εκτός εγκαταστάσεων

Τηρούνται αντίγραφα ασφαλείας εκτός εγκαταστάσεων του ΚΛΔ ΕΣ. Το ιδιωτικό κλειδί της κάθε ΑΠ αποθηκεύεται πάντα κρυπτογραφημένο. Η μυστική φράση αποκρυπτογράφησης του κλειδιού είναι γνωστή στο αρμόδιο έμπιστο προσωπικό των ΑΠ. Τα ιδιωτικά κλειδιά των Αρχών Πιστοποίησης που διαχειρίζεται το ΚΛΔ ΕΣ, βρίσκονται σε αποσπώμενα αποθηκευτικά μέσα. Αντίγραφο ασφαλείας όλης της Υποδομής Δημοσίου Κλειδιού του ΕΣ, βρίσκεται σε μαγνητική ταινία που κατέχει εξουσιοδοτημένο προσωπικό του ΕΣ. Κανένα μέλος του αρμόδιου προσωπικού δεν έχει δυνατότητα, ατομικά, να αποκτήσει πρόσβαση σε κάποιο ιδιωτικό κλειδί ΑΠ και τη μυστική φράση αποκρυπτογράφησης του κλειδιού, ταυτόχρονα.

Και τα δύο παραπάνω αποθηκευτικά μέσα βρίσκονται σε φυσικές τοποθεσίες διαφορετικές από το ΚΛΔ ΕΣ, προστατευμένες από έκθεση σε νερό και φωτιά.

5.2. Έλεγχος διαδικασιών

5.2.1. Έμπιστοι ρόλοι

Το προσωπικό που ορίζεται για να λειτουργεί τις ΑΠ θεωρείται έμπιστο και είναι εξουσιοδοτημένο να εκτελεί όλες τις εργασίες των ΑΠ και των αρχών καταχώρισης. Το προσωπικό που ορίζεται να διαχειρίζεται τους εξυπηρετητές των Αρχών Καταχώρισης και των Αρχών Πιστοποίησης, είναι εξουσιοδοτημένο να εκτελεί τις εργασίες τήρησης αντιγράφων ασφαλείας των αρχείων συναλλαγών.

5.2.2. Αριθμός ατόμων που απαιτούνται ανά εργασία

Δεν ορίζεται.

5.2.3. Εξακρίβωση ταυτότητας για κάθε ρόλο

Δεν ορίζεται.

5.3. Έλεγχος ασφαλείας προσωπικού

5.3.1. Προσόντα, εμπειρία και ειδικές εξουσιοδοτήσεις που πρέπει το προσωπικό να διαθέτει

Το προσωπικό που χειρίζεται ρόλους των Αρχών Πιστοποίησης και των Αρχών Καταχώρισης πρέπει να διαθέτει εμπειρία σε θέματα ψηφιακών πιστοποιητικών και σε θέματα υποδομής δημοσίου κλειδιού. Επίσης, πρέπει να διαθέτει προϋπηρεσία σε διαχείριση ευαίσθητων προσωπικών δεδομένων και γενικά απόρρητων πληροφοριών.

5.3.2. Διαδικασίες ελέγχου παρελθόντος για το προσωπικό των ΑΠ και το λοιπό προσωπικό

Ακολουθείται η κείμενη νομοθεσία και το πλαίσιο που ισχύει για το προσωπικό του ΕΣ.

5.3.3. Απαιτήσεις και διαδικασίες εκπαίδευσης

Το προσωπικό που λειτουργεί τις ΑΠ και τις ΑΚ και έχει πρόσβαση σε κρυπτογραφικές διαδικασίες, εκπαιδεύεται και καταρτίζεται στα θέματα της Υποδομής Δημοσίου Κλειδιού του ΕΣ από τεχνικούς του ΚΛΔ ΕΣ. Για το σκοπό αυτό υπάρχει κατάλληλη τεκμηρίωση που περιγράφει όλες τις λειτουργικές διαδικασίες της υποδομής. Το προσωπικό που λειτουργεί μέσα στην ΥΔΚ ΕΣ πρέπει να γνωρίζει μεταξύ άλλων όλα τα κείμενα πολιτικής/διαδικασιών και ειδικά την Δήλωση Διαδικασιών Πιστοποίησης και την Πολιτική Πιστοποίησης της ΥΔΚ ΕΣ.

5.3.4. Διαδικασίες και συχνότητα επανεκπαιδεύσεων

Δεν ορίζεται.

5.3.5. Εναλλαγή και σειρά αλλαγής ρόλων

Δεν ορίζεται.

5.3.6. Κυρώσεις που επιβάλλονται για μη εξουσιοδοτημένες ενέργειες

Ακολουθούνται όλες οι νόμιμες διαδικασίες που προβλέπονται για συγκεκριμένα αδικήματα και ο κανονισμός λειτουργίας του Δικτύου Δεδομένων του ΕΣ.

5.3.7. Έλεγχος σε προσωπικό ανεξάρτητων εργολάβων που εργάζονται εκτός του ΕΣ και εμπλέκονται με την ΥΔΚ ΕΣ

Σε περίπτωση κλήσης ανεξάρτητων εργολάβων για εργασίες στην ΥΔΚ ΕΣ, ο εργολάβος θα πρέπει να υπογράφει δέσμευση μέσω μνημονίου συνεργασίας και - συμφωνητικό εμπιστευτικότητας. Το ίδιο ισχύει και στις περιπτώσεις ελέγχων μέσω ομάδας Εξωτερικών Ελεγκτών (External Auditors).

5.3.8. Τεκμηρίωση που παρέχεται στο προσωπικό κατά τη διάρκεια εκπαίδευσης

Σχετικό υλικό τεκμηρίωσης βρίσκεται διαθέσιμο στο ΚΛΔ ΕΣ και παρέχεται στους εκπαιδευόμενους που αναλαμβάνουν συγκεκριμένους ρόλους μέσα στην ΥΔΚ ΕΣ.

5.4. Διαδικασίες παρακολούθησης συναλλαγών-συμβάντων

5.4.1. Τύποι συναλλαγών-συμβάντων που καταγράφονται

Τα συστήματα της ΥΔΚ ΕΣ καταγράφουν τις αιτήσεις για έκδοση πιστοποιητικού, τα εκδιδόμενα πιστοποιητικά, τις εκδιδόμενες ΛΑΠ και τα μηνύματα που ανταλλάχθηκαν με την Αρχή Καταχώρισης. Επίσης καταγράφονται σε όλους τους εξυπηρετητές της ΥΔΚ ΕΣ και άλλες διεργασίες των λειτουργικών συστημάτων και των εφαρμογών όπως π.χ. η είσοδος-έξοδος των διαχειριστών από τα συστήματα, οι

http συνδέσεις με τους εξυπηρετητές ιστοσελίδων κ.α. Όλες οι καταγραφές γίνονται με χρονοσφραγίδες που είναι συγχρονισμένες μέσω πρωτοκόλλου NTP.

5.4.2. Συχνότητα αρχειοθέτησης των επεξεργασμένων συναλλαγών-συμβάντων

Το σύστημα αρχειοθετεί όλες τις συναλλαγές καθημερινά.

5.4.3. Διάστημα τήρησης του αρχείου συναλλαγών-συμβάντων

Τα αρχεία συναλλαγών-συμβάντων τηρούνται για χρονικό διάστημα δύο (2) ετών, ώστε να είναι διαθέσιμα για ενδεχόμενο νόμιμο έλεγχο. Το διάστημα αυτό δύναται να τροποποιηθεί ανάλογα με τις εξελίξεις της σχετικής νομοθεσίας.

5.4.4. Προστασία του αρχείου συναλλαγών-συμβάντων

Δεν επιτρέπεται η πρόσβαση στο αρχείο συναλλαγών παρά μόνο για ανάγνωση και προσθήκη από εξουσιοδοτημένα συστήματα και εξουσιοδοτημένο προσωπικό. Δεν επιτρέπονται διαγραφές εγγραφών του αρχείου.

5.4.4.1. Πρόσβαση

Πρόσβαση στο αρχείο των συναλλαγών επιτρέπεται μόνο για ανάγνωση από συγκεκριμένες εφαρμογές των ΑΠ και ΑΚ καθώς και σε εξουσιοδοτημένο προσωπικό.

5.4.4.2. Προστασία κατά των μεταβολών αρχείων συναλλαγών

Εφαρμόζεται πολιτική πρόσβασης η οποία δεν επιτρέπει τις μεταβολές παρά μόνο στους διαχειριστές του λειτουργικού συστήματος της ΑΠ και ΑΚ.

5.4.4.3. Προστασία κατά των διαγραφών αρχείων συναλλαγών

Εφαρμόζεται πολιτική πρόσβασης η οποία δεν επιτρέπει τις διαγραφές παρά μόνο στους διαχειριστές του λειτουργικού συστήματος της ΑΠ και ΑΚ.

5.4.5. Διαδικασίες αντιγράφων ασφαλείας αρχείων συναλλαγών-συμβάντων

Τηρείται αντίγραφο ασφαλείας του αρχείου συναλλαγών-συμβάντων.

5.5. Αρχειοθέτηση εγγραφών

5.5.1. Τύποι εγγραφών που αρχειοθετούνται

Όλα τα αρχεία συναλλαγών αρχειοθετούνται, καθώς και όλα τα συνοδευτικά έγγραφα που σχετίζονται με αιτήματα έκδοσης/ανάκλησης ψηφιακών πιστοποιητικών.

5.5.2. Διάστημα διατήρησης του αρχείου εγγραφών

Τα αρχεία εγγραφών τηρούνται για χρονικό διάστημα δύο (2) ετών, ώστε να είναι διαθέσιμα για ενδεχόμενο νόμιμο έλεγχο. Το διάστημα αυτό δύναται να τροποποιηθεί ανάλογα με τις εξελίξεις της σχετικής νομοθεσίας.

5.5.3. Προστασία του αρχείου εγγραφών

Δεν επιτρέπεται η πρόσβαση στο αρχείο εγγραφών παρά μόνο για ανάγνωση από εξουσιοδοτημένα συστήματα και εξουσιοδοτημένο προσωπικό. Δεν επιτρέπονται διαγραφές ή μεταβολές εγγραφών του αρχείου.

5.5.3.1. Πρόσβαση

Πρόσβαση στο αρχείο των εγγραφών επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.

5.5.3.2. Προστασία κατά των μεταβολών αρχείων εγγραφών

Εφαρμόζεται πολιτική πρόσβασης η οποία δεν επιτρέπει τις μεταβολές.

5.5.3.3. Προστασία κατά των διαγραφών αρχείων εγγραφών

Εφαρμόζεται πολιτική πρόσβασης η οποία δεν επιτρέπει τις διαγραφές.

5.5.3.4. Προστασία κατά της φθοράς των μέσων αποθήκευσης

Δεν ορίζεται.

5.5.3.5. Προστασία κατά της μελλοντικής έλλειψης διαθεσιμότητας συσκευών ανάγνωσης των παλαιών μέσων αποθήκευσης

Δεν ορίζεται.

5.5.4. Διαδικασίες αντιγράφων ασφαλείας αρχείων εγγραφών

Τηρείται αντίγραφο ασφαλείας των αρχείων εγγραφών.

5.5.5. Απαίτηση χρονοσήμανσης-χρονοσφραγίδας αρχείων εγγραφών

Στην παρούσα φάση δεν απαιτείται χρονοσήμανση-χρονοσφράγιση των αρχείων εγγραφών.

5.5.6. Σύστημα συγκέντρωσης αρχείων εγγραφών (εσωτερικό ή εξωτερικό σε σχέση με την οντότητα)

Δεν ορίζεται.

5.5.7. Διαδικασίες για ανάκτηση και επαλήθευση των στοιχείων των αρχείων εγγραφών

Δεν ορίζεται.

5.6. Ριζική αλλαγή κλειδιού

Σε περίπτωση αλλαγής κλειδιού κάποιας Αρχής Πιστοποίησης, τα κλειδιά των τελικών πιστοποιητικών πρέπει να ακυρωθούν και να ξαναδημιουργηθούν.

5.7. Ανάκαμψη από παραβίαση ασφάλειας και καταστροφή

5.7.1. Διαδικασίες και χειρισμός περιστατικών παραβίασης

Τα αρχεία καταγραφής ελέγχονται περιοδικά για ανίχνευση παραβίασης ασφάλειας συστημάτων ή υποσυστημάτων. Σε περίπτωση που ανιχνευθεί κάποια ανωμαλία ή υπάρχει υποψία παραβίασης, διακόπτεται η παροχή της υπηρεσίας και γίνεται ενδελεχής έλεγχος όλων των συστημάτων.

5.7.2. Διαδικασίες αντιμετώπισης σε περίπτωση παραβίασης-καταστροφής ή υποψίας παραβίασης-καταστροφής υπολογιστικών συστημάτων, λογισμικού, δεδομένων

Σε περίπτωση υποψίας παραβίασης, διακόπτεται η παροχή της υπηρεσίας και γίνεται ενδελεχής έλεγχος όλων των συστημάτων. Σε περίπτωση που επιβεβαιωθεί παραβίαση, ελέγχεται αν υπάρχει παραβίαση σε ιδιωτικά κλειδιά. Σε περίπτωση παραβίασης χωρίς απώλεια ιδιωτικών κλειδιών, γίνεται επαναφορά των συστημάτων από αντίγραφα ασφαλείας στα οποία δεν υπάρχει υποψία παραβίασης, γίνονται νέοι έλεγχοι ασφάλειας ώστε να βρεθούν πιθανά κενά και στη συνέχεια η υπηρεσία επανέρχεται. Σε περίπτωση απώλειας κλειδιών, ακολουθούνται οι διαδικασίες της επομένης παραγράφου.

5.7.3. Διαδικασίες αντιμετώπισης σε περίπτωση απώλειας ιδιωτικών κλειδιών

Σε περίπτωση απώλειας ιδιωτικών κλειδιών τελικών πιστοποιητικών, γίνεται ανάκλησή τους από την υπηρεσία πιστοποίησης και έκδοση νέων χωρίς την διακοπή της υπηρεσίας. Σε περίπτωση απώλειας

ιδιωτικού κλειδιού ενδιάμεσης Αρχής Πιστοποίησης, ειδοποιούνται όλοι οι συνδρομητές της συγκεκριμένης ενδιάμεσης ΑΠ, ανακαλούνται όλα τα τελικά πιστοποιητικά που εκδόθηκαν από τη συγκεκριμένη Αρχή, καθώς και το πιστοποιητικό της ίδιας της Αρχής. Σε περίπτωση απώλειας του ιδιωτικού κλειδιού της Κορυφαίας Αρχής Πιστοποίησης, η ΑΠ οφείλει να διακόψει την υπηρεσία, να ειδοποιήσει όλους τους συνδρομητές όλων των ενδιάμεσων Αρχών Πιστοποίησης, να προχωρήσει στην ανάκληση όλων των πιστοποιητικών, να εκδώσει μια τελευταία ΛΑΠ και τέλος να ειδοποιήσει τις σχετικές επαφές ασφάλειας. Στη συνέχεια η Υποδομή Δημοσίου Κλειδιού θα πρέπει να επανασυσταθεί με δημιουργία νέων Αρχών Πιστοποίησης, ξεκινώντας από νέα Κεντρική Αρχή Πιστοποίησης.

5.7.4. Δυνατότητες αδιάλειπτης λειτουργίας της υπηρεσίας σε περίπτωση φυσικών ή άλλων καταστροφών

Η ΑΠ του ΕΣ έχει προβλέψει δυνατότητες αδιάλειπτης λειτουργίας με αποθήκευση αντιγράφων όλων των συστημάτων/υποσυστημάτων σε ασφαλή τοποθεσία εκτός των χώρων του ΕΣ.

5.8. Τερματισμός Αρχής Πιστοποίησης – Αρχής Καταχώρησης

Κατά τον τερματισμό της, η ΑΠ ενημερώνει τους συνδρομητές, ανακαλεί όλα τα πιστοποιητικά που έχει εκδώσει, ανακοινώνει τη σχετική ΛΑΠ και ανακαλεί και το δικό της πιστοποιητικό. Τέλος, ενημερώνει τους υπεύθυνους ασφαλείας συνεργαζόμενων φορέων και δημοσιοποιεί το τερματισμό της λειτουργίας της. Τα αρχεία καταγραφής των ΑΚ και ΑΠ τηρούνται για χρονικό διάστημα δύο (2) ετών, ώστε να είναι διαθέσιμα για ενδεχόμενο νόμιμο έλεγχο. Το διάστημα αυτό δύναται να τροποποιηθεί ανάλογα με τις εξελίξεις της σχετικής νομοθεσίας.

6. Έλεγχοι ασφάλειας τεχνικού επιπέδου

6.1. Δημιουργία ζεύγους κλειδιών και εγκατάσταση

6.1.1. Δημιουργία ζεύγους κλειδιών

Τα κλειδιά των συνδρομητών των Signing CA δημιουργούνται από υλικό και κατάλληλο λογισμικό στην πλευρά των υποψήφιων συνδρομητών και παραμένουν κάτω από τον απόλυτο έλεγχό τους, σε όλη τη διάρκεια της ισχύος τους. Οι διαχειριστές συστήματος (sys admins) δεν παράγουν κλειδιά. Τα εν λόγω κλειδιά παράγονται από τους crypto CA.

Σε περίπτωση που κάποια Αρχή Πιστοποίησης επιτρέψει στις διαδικασίες της να ισχύει η δημιουργία κλειδιών για λογαριασμό τρίτου μαζικά από την ΑΠ, θα πρέπει να προβλέπεται η καταστροφή όλων των αντιγράφων ιδιωτικών κλειδιών μετά την παράδοσή τους στους χρήστες, ώστε στο τέλος το ιδιωτικό κλειδί να βρίσκεται μόνο στην κατοχή του δικαιούχου συνδρομητή. Ειδικά για την περίπτωση που κάποιος συνδρομητής επιθυμεί να αποκτήσει πιστοποιητικό κλάσης Α, θα πρέπει να πραγματοποιήσει την αίτηση παρουσία τεχνικού Αρχής Καταχώρησης ώστε να πιστοποιηθεί η χρήση της hardware κρυπτοσυσκευής.

Τα κλειδιά των ΑΠ δημιουργούνται από λογισμικό ή ειδικές hardware κρυπτοσυσκευές (eToken, smartcard) οι οποίες είναι εγκατεστημένες στην ΑΠ και πληρούν τις προδιαγραφές FIPS 140-2. Πρέπει να ελέγχεται κατά το χρόνο δημιουργίας των κλειδιών η ύπαρξη πληροφοριών για σφάλματα του λογισμικού ή του υλικού που χρησιμοποιείται, που αφορούν τη δημιουργία κλειδιών.

6.1.2. Παράδοση ιδιωτικού κλειδιού σε οντότητα

Δεν επιτρέπεται η δημιουργία κλειδιών από οποιαδήποτε οντότητα για λογαριασμό του υποψήφιου συνδρομητή ή άλλης οντότητας ούτε από την ΑΠ για λογαριασμό των συνδρομητών. Δεν επιτρέπεται η παράδοση του ιδιωτικού κλειδιού του υποψήφιου συνδρομητή σε οποιαδήποτε τρίτη οντότητα. Σε περίπτωση που κάποια Αρχή Πιστοποίησης επιτρέψει στις διαδικασίες της να ισχύει η δημιουργία κλειδιών για λογαριασμό τρίτου, θα πρέπει να ακολουθείται η παρακάτω διαδικασία:

- Αν η ΑΠ έχει αρκετές πληροφορίες για να επιβεβαιώσει την εγκυρότητα της ταυτότητας του χρήστη εκ των προτέρων, έχει την δυνατότητα να δημιουργήσει ζεύγη κλειδιών και πιστοποιητικό για αυτόν τον χρήστη.
- Η εξακρίβωση της γνησιότητας αυτών των πιστοποιητικών υλοποιείται όταν οι ιδιοκτήτες τους παραλαμβάνουν τα διαπιστευτήρια (πιστοποιητικό και κλειδιά) τους από την Αρχή Καταχώρησης. Το μοντέλο αυτό ονομάζεται ομαδικό.
- Η ΑΠ πρέπει να έχει διαδικασία διαγραφής του μυστικού κλειδιού που σχετίζεται με το κάθε Ψηφιακό Πιστοποιητικό Ταυτότητας μόλις αυτό παραδοθεί στον δικαιούχο τελικό χρήστη, έτσι ώστε τελικά το ιδιωτικό κλειδί να βρίσκεται στην κατοχή αποκλειστικά του δικαιούχου.

6.1.3. Παράδοση δημόσιου κλειδιού συνδρομητή στην Αρχή Πιστοποίησης

Ο εγγραφόμενος υποβάλλει στην Αρχή Καταχώρισης το δημόσιο κλειδί του μέσω δομημένης αίτησης (π.χ. τύπου PKCS#10) για έκδοση πιστοποιητικού. Η αίτηση είναι υπογεγραμμένη με το σχετικό ιδιωτικό κλειδί. Η ΑΚ επαληθεύει την ορθότητα της υπογραφής και συμπεραίνει ότι ο αιτών κατέχει πράγματι το σχετικό με την αίτηση ιδιωτικό κλειδί.

6.1.4. Παράδοση του δημόσιου κλειδιού της Αρχής Πιστοποίησης σε οντότητες που εμπιστεύονται τα πιστοποιητικά

Οι ΑΠ παρέχουν μηχανισμούς για την ασφαλή παράδοση των ψηφιακών πιστοποιητικών τους. Το κάθε ψηφιακό πιστοποιητικό περιέχει το δημόσιο κλειδί όταν αυτό ζητείται από ενδιαφερόμενες οντότητες. Οι ενδιαφερόμενοι μπορούν να αποστέλλουν αίτηση με ηλεκτρονικό ταχυδρομείο. Η κάθε ΑΠ αποστέλλει με ταχυδρομείο σε μαγνητικό μέσο το πιστοποιητικό της, το οποίο περιέχει το δημόσιο κλειδί της. Εναλλακτικά, το πιστοποιητικό της κάθε ΑΠ δημοσιοποιείται μέσω ασφαλούς ιστοσελίδας, της οποίας η ταυτότητα πιστοποιείται από διαφορετική έμπιστη τρίτη οντότητα.

Η κάθε ΑΠ δημοσιοποιεί στην αποθήκη της παραγράφου 2.1 το Πιστοποιητικό της.

6.1.5. Μεγέθη κλειδιών

Το ελάχιστο επιτρεπτό μέγεθος κλειδιού είναι 2048 bits ανεξάρτητα από τη χρήση του κλειδιού αυτού.

6.1.6. Παράμετροι δημιουργίας κλειδιών

Δεν ορίζεται.

6.1.7. Σκοποί χρήσης των κλειδιών (ως προς το αντίστοιχο πεδίο του X.509)

Οι σκοποί χρήσης ενός κλειδιού αναφέρονται στο σχετικό βασικό πεδίο και στη σχετική επέκταση του πιστοποιητικού τύπου X.509v3. Οι αναφερόμενοι σκοποί χρήσης του πιστοποιητικού δεν είναι περιοριστικοί (π.χ. μη κρίσιμη επέκταση πιστοποιητικού) αλλά «προτεινόμενοι». Ο έλεγχος συμμόρφωσης με τους επιτρεπόμενους σκοπούς χρήσης γίνεται κατά την κρίση των βασιζόμενων μερών.

Ανάλογα με την κλάση του πιστοποιητικού, τα πεδία του πιστοποιητικού περιλαμβάνουν τουλάχιστο τις παρακάτω χρήσεις:

Κλάσεις πιστοποιητικών φυσικών προσώπων:

Βασικές χρήσεις: 'Digital Signature', 'Non-Repudiation', 'Data Encipherement', 'Key Encipherment'.

Επεκτάσεις: 'Client Authentication', 'Secure Email', 'Encrypting File System'

Κλάσεις πιστοποιητικών συσκευών:

Βασικές χρήσεις: 'Digital Signature', 'Key Encipherment'.

Επεκτάσεις: 'Client Authentication', 'Server Authentication'

Κλάσεις με επιπλέον χρήσεις ειδικών υπηρεσιών:

Επεκτάσεις: 'IP Security User', 'Timestamping', 'Code Signing', 'OCSPSigning'.

6.2. Προστασία ιδιωτικών κλειδιών

6.2.1. Προδιαγραφές για κρυπτογραφικές μονάδες

Δεν ορίζεται.

6.2.2. Συνοδεία ιδιωτικού κλειδιού (key escrow)

Δεν ορίζεται.

6.2.3. Αντίγραφα ασφαλείας ιδιωτικών κλειδιών

Το ιδιωτικό κλειδί κάθε Αρχής Πιστοποίησης πρέπει να φυλάσσεται σε αντίγραφα ασφαλείας. Το αντίγραφο του κλειδιού πρέπει να είναι πάντα κρυπτογραφημένο. Η πρόσβαση στο αντίγραφο ασφαλείας επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.

6.2.4. Αρχειοθέτηση αντιγράφων ασφαλείας ιδιωτικών κλειδιών

Το αντίγραφο ασφαλείας του ιδιωτικού κλειδιού κάθε Αρχής Πιστοποίησης πρέπει να αρχειοθετείται και να φυλάσσεται με ασφαλείς μεθόδους και σε ασφαλή χώρο. Τα ιδιωτικά κλειδιά στο αντίγραφο είναι ούτως ή άλλως πάντα κρυπτογραφημένα αλλά υπάρχει πρόσθετη προστασία κρυπτογράφησης των αρχειοθετημένων αντιγράφων ασφαλείας.

Τα ιδιωτικά κλειδιά των Αρχών Πιστοποίησης πρέπει να βρίσκονται σε αποσπώμενα αποθηκευτικά μέσα (CD Roms) ή άλλο αφαιρούμενο μέσο σε κρυπτογραφημένη μορφή, με κωδικό (passphrase) που γνωρίζει μόνο εξουσιοδοτημένο προσωπικό του ΕΣ και μάλιστα τμηματικά. Κανένα μέλος του προσωπικού δεν μπορεί –ατομικά- να γνωρίζει το σύνολο του κωδικού κρυπτογράφησης ενός ιδιωτικού κλειδιού.

Αντίγραφα ασφαλείας όλης της Υποδομής Δημοσίου Κλειδιού του ΕΣ, βρίσκονται σε μαγνητικές ταινίες ή memory flash disks που κατέχουν εξουσιοδοτημένα στελέχη του ΕΣ.

Και τα δύο παραπάνω αποθηκευτικά μέσα βρίσκονται σε φυσικές τοποθεσίες διαφορετικές από το ΚΛΔ ΕΣ, προστατευμένα από έκθεση σε νερό και φωτιά.

Η πρόσβαση στο αρχειοθετημένο αντίγραφο ασφαλείας επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.

6.2.5. Κάτω από ποιες προϋποθέσεις, αν ορίζονται, μπορεί ένα ιδιωτικό κλειδί να μεταφερθεί από και προς ένα κρυπτογραφικό σύστημα

Οι κάτοχοι των ιδιωτικών κλειδιών, απαγορεύεται να μεταφέρουν το ιδιωτικό κλειδί τους από ειδικό κρυπτογραφικό σύστημα μορφής λογισμικού (software certificate store) σε οποιοδήποτε κρυπτογραφικό σύστημα μορφής υλικού (hardware) πχ crypto-tokens, smartcards. Επίσης απαγορεύεται και η αντίστροφη διαδικασία (μεταφορά κλειδιού από hardware σε software certificate store).

6.2.6. Με ποια μορφή αποθηκεύεται ένα ιδιωτικό κλειδί σε κρυπτογραφικό σύστημα

Υπάρχουν οι δύο παρακάτω μορφές αποθήκευσης ενός ιδιωτικού κλειδιού σε κρυπτογραφικό σύστημα: α) ως software token και β) ως hardware token

6.2.7. Μέθοδοι ενεργοποίησης (προς χρήση) ιδιωτικών κλειδιών.

6.2.7.1. Ποιος μπορεί να ενεργοποιήσει (χρησιμοποιήσει) ιδιωτικό κλειδί;

Το ιδιωτικό κλειδί της κάθε ΑΠ βρίσκεται προστατευμένο (κρυπτογραφημένα) με κάποιον ισχυρό κωδικό. Κάθε εξουσιοδοτημένος διαχειριστής της ΑΠ γνωρίζει διαφορετικό τμήμα αυτού του ισχυρού κωδικού. Μόνο συνδυασμός από εξουσιοδοτημένους διαχειριστές μπορεί να αποκρυπτογραφήσει το ιδιωτικό κλειδί της κάθε ΑΠ προκειμένου να πραγματοποιήσουν κρυπτογραφικές διαδικασίες. Η διαδικασία περιγράφεται σε εσωτερικό κείμενο της ΥΔΚ ΕΣ που περιγράφει την «τελετή ενεργοποίησης Αρχών Πιστοποίησης».

Το ιδιωτικό κλειδί τελικών πιστοποιητικών συνδρομητών-συσκευών βρίσκεται επίσης προστατευμένο-κρυπτογραφημένο με κάποιους τρόπους. Μόνο ο δικαιούχος συνδρομητής ή διαχειριστής συσκευής ή υπηρεσίας, επιτρέπεται να ενεργοποιήσει και να χρησιμοποιήσει ιδιωτικό κλειδί που αντιστοιχεί στο τελικό πιστοποιητικό που διαχειρίζεται.

6.2.7.2. Ενέργειες που πρέπει να εκτελεστούν για την ενεργοποίηση ενός ιδιωτικού κλειδιού

Για την ενεργοποίηση ενός ιδιωτικού κλειδιού απαιτείται η εισαγωγή κάποιου ισχυρού κωδικού (pass-phrase) προκειμένου να αποκρυπτογραφηθεί και να χρησιμοποιηθεί το ιδιωτικό κλειδί σε συνδυασμό με το πιστοποιητικό. Ειδικά για κρυπτογραφικά συστήματα υλικού (πχ crypto-tokens) απαιτείται η εισαγωγή κάποιου PIN.

Για την ενεργοποίηση κλειδιών Αρχών Πιστοποίησης που βρίσκονται σε ειδικές κρυπτοσυσκευές, απαιτείται συνδυασμός ισχυρών κωδικών που γνωρίζει εξουσιοδοτημένο προσωπικό. Κάθε εξουσιοδοτημένος διαχειριστής της ΑΠ γνωρίζει διαφορετικό τμήμα του PIN ενεργοποίησης. Μόνο συνδυασμός από εξουσιοδοτημένους διαχειριστές μπορεί να ενεργοποιήσει ένα ιδιωτικό κλειδί.

Σε περιπτώσεις τελικών πιστοποιητικών χρηστών που χρησιμοποιούν κρυπτογραφικά συστήματα σε μορφή λογισμικού (πχ CryptoAPI στα MS Windows), ενδέχεται να μην ερωτάται ισχυρός κωδικός αλλά μια απλή ερώτηση επιβεβαίωσης χρήσης ή μη, του ιδιωτικού κλειδιού. Τέλος, τα ιδιωτικά κλειδιά που χρησιμοποιούνται σε συσκευές-υπηρεσίες ενδέχεται να είναι μονίμως ενεργοποιημένα και να μην προστατεύονται καθόλου από κάποιον κωδικό, εφόσον υπάρχουν άλλα ικανοποιητικά επίπεδα ασφάλειας σε επίπεδο αρχείων συστήματος και άλλων.

6.2.7.3. Από τη στιγμή ενεργοποίησης, για πόσο χρονικό διάστημα είναι το κλειδί «ενεργό»;

Δεν ορίζεται. Συνήθως το κλειδί παραμένει «ενεργό» για όσο διάστημα λειτουργεί η συγκεκριμένη εφαρμογή που το χρησιμοποιεί.

6.2.8. Μέθοδοι απενεργοποίησης ιδιωτικών κλειδιών.

Όταν αποσύρεται ένας εξυπηρετητής, τότε πρέπει και το αντίστοιχο πιστοποιητικό του να απενεργοποιείται, καθώς πλέον δεν είναι κάπου χρήσιμο.

6.2.9. Μέθοδοι καταστροφής ιδιωτικών κλειδιών.

Τα ιδιωτικά κλειδιά είτε καταστρέφονται είτε πραγματοποιείται σε αυτά επαναφορά εργοστασιακών ρυθμίσεων.

6.2.10. Βαθμολόγηση-αξιολόγηση κρυπτογραφικών συστημάτων

Δεν ορίζεται.

6.3. Άλλα θέματα διαχείρισης ζεύγους κλειδιών

6.3.1. Περίοδοι χρήσης των πιστοποιητικών και των ζευγών κλειδιών

Η διάρκεια χρήσης των ζευγών των κρυπτογραφικών κλειδιών προσδιορίζεται από την αντίστοιχη περίοδο ισχύος του σχετικού ψηφιακού πιστοποιητικού. Η μέγιστη διάρκεια χρήσης των κλειδιών ορίζεται σε δέκα (10) έτη για Κεντρική ΑΠ, σε πέντε (5) έτη για ενδιάμεση ΑΠ και σε τρία (3) έτη για πιστοποιητικά τελικών χρηστών και συσκευών. Η διάρκεια χρήσης σε κάθε περίπτωση θα πρέπει να αποφασίζεται σε συνάρτηση με το μέγεθος των κλειδιών και με τις τρέχουσες τεχνολογικές εξελίξεις στο χώρο της κρυπτογραφίας, έτσι ώστε να εξασφαλίζεται το βέλτιστο επίπεδο ασφάλειας αλλά και αποτελεσματικότητας χρήσης.

6.4. Δεδομένα ενεργοποίησης

6.4.1. Δημιουργία δεδομένων ενεργοποίησης και εγκατάσταση

Τα δεδομένα ενεργοποίησης, δηλαδή οι μυστικοί ισχυροί κωδικοί και τα PIN, πρέπει να επιλέγονται έτσι ώστε να είναι δύσκολο να ανακαλυφθούν. Το ελάχιστο μέγεθος του μυστικού ισχυρού κωδικού και του PIN είναι οκτώ (8) ψηφία.

Σε περίπτωση που χρησιμοποιείται μηχανισμός καταστροφής του ιδιωτικού κλειδιού μετά από ορισμένο αριθμό εσφαλμένων προσπαθειών πρόσβασης το μέγεθος του PIN μπορεί να είναι μικρότερο.

6.4.2. Προστασία δεδομένων ενεργοποίησης

Δεν ορίζεται.

6.4.3. Άλλα θέματα σχετικά με τα δεδομένα ενεργοποίησης

Δεν ορίζεται.

6.5. Έλεγχοι ασφαλείας υπολογιστών

6.5.1. Συγκεκριμένες τεχνικές απαιτήσεις ασφάλειας

- Οφείλονται να ακολουθούνται οι διαδικασίες που προβλέπονται από το πρότυπο ISO 27001
- Τα Λειτουργικά Συστήματα των υπολογιστών της ΥΔΚ ΕΣ διατηρούνται σε υψηλό επίπεδο ασφάλειας με εφαρμογή όλων των διεθνών προτύπων οδηγιών ασφάλειας

- Υπάρχουν συστήματα καταγραφής ενεργειών στους υπολογιστές της ΥΔΚ ΕΣ και περιοδικός έλεγχος των αρχείων καταγραφής για διαπίστωση τυχόν ανωμαλιών.
- Τα προγράμματα που συνοδεύουν το Λειτουργικό Σύστημα είναι τα απολύτως απαραίτητα για την εύρυθμη λειτουργία των ΑΚ/ΑΠ.

6.5.2. Βαθμολόγηση ασφάλειας υπολογιστών

Η βαθμολόγηση πραγματοποιείται μέσω όσων ορίζονται από το ISO 27001.

6.6. Έλεγχοι ασφαλείας κύκλου ζωής

6.6.1. Έλεγχοι ανάπτυξης συστημάτων

Οι έλεγχοι ανάπτυξης συστημάτων πραγματοποιούνται μέσω όσων ορίζονται από το ISO 27001.

6.6.2. Έλεγχοι διαχείρισης ασφάλειας

Οι έλεγχοι διαχείρισης ασφάλειας πραγματοποιούνται μέσω όσων ορίζονται από το ISO 27001.

6.6.3. Βαθμολόγηση ασφάλειας κύκλου ζωής

Η βαθμολόγηση πραγματοποιείται μέσω όσων ορίζονται από το ISO 27001.

6.7. Έλεγχοι ασφαλείας δικτύου

Απαγορεύεται η σύνδεση των ΑΠ σε ευρύτερα δίκτυα δεδομένων (πχ Internet) ή άλλο τηλεπικοινωνιακό μέσο (πχ στο τηλεφωνικό δίκτυο μέσω modem). Οι Αρχές Καταχώρισης προστατεύονται από το διαδίκτυο με ισχυρούς μηχανισμούς ασφάλειας συμπεριλαμβανομένου και firewall.

6.8. Χρονοσφραγίδες-Χρονοσήμανση

Όλες οι χρονοσφραγίδες και η χρονοσήμανση στην ΥΔΚ ΕΣ (είτε σε Αρχές Καταχώρισης είτε σε Αρχές Πιστοποίησης) συγχρονίζονται μέσω πρωτοκόλλου NTP (Network Time Protocol) και μέσω ενός GPS time server.

7. Περίγραμμα (profile) πιστοποιητικού, ΛΑΠ και OCSP

7.1. Περίγραμμα πιστοποιητικού

Χρησιμοποιείται περίγραμμα πιστοποιητικού σύμφωνα με το RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”

7.1.1. Έκδοση

Ο αριθμός έκδοσης του πιστοποιητικού είναι 2, που αντιστοιχεί στα πιστοποιητικά X.509v3.

7.1.2. Επεκτάσεις πιστοποιητικού

Σε κάθε πιστοποιητικό που εκδίδεται θα πρέπει να περιλαμβάνεται η επέκταση BasicConstraints χαρακτηρισμένη ως κρίσιμη και οι επεκτάσεις KeyUsage, SubjectKeyIdentifier, AuthorityKeyIdentifier και CertificatePolicies χαρακτηρισμένες ως μη κρίσιμες. Επίσης, πρέπει να περιλαμβάνεται η επέκταση CRLDistributionPoint χαρακτηρισμένη ως μη κρίσιμη.

7.1.3. Αναγνωριστικά αντικειμένων αλγορίθμων

Για την υπογραφή των πιστοποιητικών χρησιμοποιείται ο αλγόριθμος SHA2 ή ισχυρότερος. Απαγορεύεται η χρήση του αλγόριθμου MD5 ή άλλων για τους οποίους υπάρχουν αποδείξεις ότι έχουν παραβιαστεί.

7.1.4. Περιορισμοί ονομάτων

Η Κεντρική Αρχή Πιστοποίησης του ΕΣ εφαρμόζει περιορισμούς ονομάτων σε όλες τις ΑΠ σύμφωνα με το RFC 5280. Η συγκεκριμένη επέκταση χαρακτηρίζεται ως «μη κρίσιμη» και περιορίζεται στα domains ……..

7.1.5. Χρήση της επέκτασης περιορισμού πολιτικής

Δεν ορίζεται.

7.1.6. Σύνταξη και σημασιολογία του χαρακτηριστικού πολιτικής

Το χαρακτηριστικό πολιτικής είναι URI το οποίο δείχνει στην δημοσιευμένη ΠΠ/ΔΔΠ της ΥΔΚ ΕΣ.

7.1.7. Επεξεργασία σημασιολογίας για την κρίσιμη επέκταση πολιτικής πιστοποίησης

Δεν ορίζεται.

7.2. Περίγραμμα ΛΑΠ

7.2.1. Έκδοση

Ο αριθμός έκδοσης της είναι 1 ή/και 2, που αντιστοιχεί σε ΛΑΠ X.509v2, ακολουθώντας το RFC-3280.

7.2.2. ΛΑΠ και επεκτάσεις των εγγραφών της ΛΑΠ

Δεν ορίζεται.

7.3. Περίγραμμα OCSP

Το Online Certificate Status Protocol (OCSP) χρησιμοποιείται για την επικύρωση της κατάστασης ανάκλησης όλων των πιστοποιητικών που έχουν εκδοθεί από την Κορυφαία Κεντρική Αρχή Πιστοποίησης. Η χρήση του OCSP είναι υποχρεωτική για τις υφιστάμενες Αρχές Πιστοποίησης. Οι εξυπηρετητές OCSP πρέπει να συμμορφώνονται με το RFC2560.

7.3.1. Έκδοση

Υποστηρίζεται η έκδοση 1 των προδιαγραφών OCSP όπως αυτή ορίζεται στο RFC2560.

7.3.2. OCSP και επεκτάσεις των εγγραφών

Η υπηρεσία OCSP χρησιμοποιεί ασφαλή χρονοσφραγίδα και μέγιστη περίοδο εγκυρότητας 5 λεπτών για να επιβεβαιώσει την εγκυρότητα της υπογεγραμμένης απάντησης. Ο αλγόριθμος κατακερματισμού που χρησιμοποιείται για το όνομα και το κλειδί του εκδότη είναι ο SHA1.

Η επέκταση nonce υποστηρίζεται από τον εξυπηρετητή OCSP. Αιτήματα τα οποία περιέχουν ένα nonce θα πρέπει να το χρησιμοποιούν για να επιβεβαιώσουν την εγκυρότητα της απάντησης. Διαφορετικά, πρέπει να χρησιμοποιηθεί το τοπικό ρολόι και η χρονοσφραγίδα που περιέχεται στην απάντηση.

8. Έλεγχοι συμμόρφωσης και άλλες εκτιμήσεις

Η ΥΔΚ ΕΣ καλύπτει τις τεχνικές προδιαγραφές του ETSI TS 101 456 “Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates”. Ένας εξωτερικός έλεγχος συμμόρφωσης απαιτείται σε ετήσια βάση για την εξέταση της συμμόρφωσης της ΥΔΚ προς την ΠΠ/ΔΔΠ.

Έλεγχος συμμόρφωσης μπορεί να διεξαχθεί από τους ενδιαφερόμενους για συνεργασία με την Υπηρεσία, μετά από άδεια του φορέα που λειτουργεί την Υπηρεσία και εφόσον ο ενδιαφερόμενος καλύψει όλα τα έξοδα του ελέγχου.

9. Διοικητικά και Νομικά θέματα

9.1. Κόστη εγγραφής

Δεν καταβάλλονται τέλη για τις παρεχόμενες υπηρεσίες. Απαγορεύεται ρητά κάθε είδους μεταπώληση ή άλλου τύπου εκμετάλλευση των παρεχόμενων υπηρεσιών από τους αποδέκτες τους.

9.1.1. Κόστος έκδοσης και ανανέωσης πιστοποιητικών

Δεν ορίζεται

9.1.2. Κόστος πρόσβασης σε πιστοποιητικά

Δεν ορίζεται

9.1.3. Κόστος ανάκλησης ή ερώτηση κατάστασης πιστοποιητικών

Δεν ορίζεται

9.1.4. Κόστος άλλων υπηρεσιών όπως πρόσβαση στα κείμενα πολιτικής και διαδικασιών πιστοποίησης

Δεν ορίζεται

9.1.5. Διαδικασίες επιστροφής χρημάτων

Δεν ορίζεται

9.2. Οικονομική ευθύνη

Η Υποδομή Δημοσίου Κλειδιού ΕΣ δεν αναλαμβάνει, ούτε μπορεί να της αποδοθεί οικονομική ευθύνη.

9.3. Εμπιστευτικότητα πληροφοριών εμπορικού χαρακτήρα

Η ΥΔΚ ΕΣ δεν χειρίζεται πληροφορίες εμπορικού χαρακτήρα.

9.4. Εμπιστευτικότητα πληροφοριών προσωπικού χαρακτήρα

9.4.1. Σχέδιο εμπιστευτικότητας

Ο Ε.Σ. συμμορφώνεται με ότι προβλέπει ο νέος Γενικός Κανονισμός Προστασίας Δεδομένων (GDPR), τόσο στα τεχνικά και οργανωτικά μέτρα όσο και στα μέτρα σε επίπεδο δεδομένων.

9.4.2. Πληροφορίες που χαρακτηρίζονται εμπιστευτικές

Πληροφορίες που τηρούνται από την Υπηρεσία και θεωρούνται ως εμπιστευτικές, είναι τα ιδιωτικά κλειδιά των Αρχών Πιστοποίησης που λειτουργούν, καθώς και ο μηχανισμός ασφαλούς αποθήκευσης και χρήσης τους. Εμπιστευτικές θεωρούνται επίσης οι πληροφορίες φυσικής πρόσβασης και ασφάλειας του χώρου όπου εγκαθίστανται και λειτουργούν τα συστήματα των Αρχών Καταχώρισης και των Αρχών Πιστοποίησης.

Οι Αρχές Καταχώρισης είναι πιθανό να επεξεργάζονται προσωπικά δεδομένα κατά τον έλεγχο της ταυτότητας των αιτούντος.

9.4.3. Πληροφορίες που δεν θεωρούνται εμπιστευτικές

Δεν θεωρούνται εμπιστευτικές οι πληροφορίες που περιέχονται στα ψηφιακά πιστοποιητικά που εκδίδονται

9.4.4. Δήλωση προστασίας δεδομένων προσωπικού χαρακτήρα

Η διαχείριση από την ΥΔΚ ΕΣ, των δεδομένων που χαρακτηρίζονται εμπιστευτικά και προσωπικού χαρακτήρα, συμμορφώνεται με τη σχετική νομοθεσία περί προστασίας Προσωπικών Δεδομένων.

9.4.5. Διάθεση πληροφοριών σε αρχές επιβολής του νόμου

Οι μη εμπιστευτικές πληροφορίες που τηρεί η Υπηρεσία είναι διαθέσιμες στις δικαστικές αρχές, μετά από έγγραφη αίτησή τους. Για τη διάθεση στις δικαστικές αρχές εμπιστευτικών πληροφοριών ή προσωπικών δεδομένων των εγγραφόμενων, θα γίνεται αίτηση σύμφωνα με την ισχύουσα νομοθεσία και μέσω της Πρυτανείας του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης. Ιδιωτικά κλειδιά που χρησιμοποιούνται από την Υπηρεσία για την υπογραφή πιστοποιητικών, δεν δημοσιοποιούνται σε τρίτους σε καμία περίπτωση, εκτός αν ο νόμος το απαιτεί ρητά.

9.4.6. Πληροφορίες που μπορούν να διατεθούν για τη αναζήτηση οντοτήτων

Οι μη εμπιστευτικές πληροφορίες που τηρεί η Υπηρεσία είναι διαθέσιμες για την αναζήτηση οντοτήτων, μετά από αίτηση.

9.4.7. Όροι για τη διάθεση πληροφοριών μετά από αίτημα του ιδιοκτήτη τους

Οι πληροφορίες που τηρεί η κάθε ΑΠ είναι διαθέσιμες στον ιδιοκτήτη τους, μετά από αίτησή του.

9.4.8. Άλλες περιπτώσεις στις οποίες διατίθενται εμπιστευτικές πληροφορίες

Δεν ορίζεται.

9.5. Δικαιώματα πνευματικής ιδιοκτησίας

Η ΥΔΚ ΕΣ δεν έχει δικαιώματα πνευματικής ιδιοκτησίας στα εκδιδόμενα πιστοποιητικά.

Οποιοσδήποτε, μπορεί να αντιγράφει μέρη της παρούσας ΠΠ/ΔΔΠ με την προϋπόθεση αναφοράς του αρχικού κειμένου.

Η εν λόγω πληροφορία είναι αδιαβάθμιτη και μη αναρτήσιμη στο διαδίκτυο.

9.6. Αντιπροσωπεύσεις και εξουσιοδοτήσεις

Δεν ορίζεται

9.7. Αποκηρύξεις και Εγγυήσεις

Δεν ορίζεται

9.8. Περιορισμοί ευθυνών

Η Υποδομή Δημοσίου Κλειδιού του ΕΣ δεν ευθύνεται για προβλήματα ή ζημιές που μπορεί να προκύψουν από την ανυπαίτια πλημμελή λειτουργία της ή από την κακή χρήση των πιστοποιητικών που εκδίδει. Η χρήση της ΥΔΚ ΕΣ και των υπηρεσιών Πιστοποίησης προϋποθέτει την ανεπιφύλακτη παραδοχή εκ μέρους του χρήστη ότι η ΥΔΚ ΕΣ δεν ευθύνεται για ζημία ή βλάβη, δεν αναλαμβάνει, ούτε μπορούν να τις αποδοθούν οικονομικές, αστικές ή άλλου είδους ευθύνες, παρά μόνο σε περιπτώσεις που αποδεικνύεται δόλος ή αμέλειά της.

9.9. Αποζημιώσεις

Η Υποδομή Δημοσίου Κλειδιού ΕΣ και οι υπηρεσίες Πιστοποίησης δεν αναλαμβάνουν ούτε μπορούν να τις αποδοθούν οικονομικές, αστικές ή άλλου είδους ευθύνες, παρά μόνο σε περιπτώσεις που αποδεικνύεται δόλος ή αμέλεια τους. Επίσης χρησιμοποιείται αποκλειστικά για Ακαδημαϊκούς και Ερευνητικούς σκοπούς και απαγορεύεται ρητά η εμπορική εκμετάλλευσή της. Συνεπώς, η ΥΔΚ απαλλάσσεται από κάθε ζημία, που δε συνδέεται αιτιωδώς με τη χρήση των υπηρεσιών πιστοποίησης για τους παραπάνω σκοπούς.

9.10. Χρονική περίοδος ισχύος της παρούσας ΠΠ/ΔΔΠ και τερματισμός της

Η παρούσα ΠΠ/ΔΔΠ ισχύει για το χρονικό διάστημα λειτουργίας της ΥΔΚ ΕΣ.

9.11. Ατομικές ειδοποιήσεις και επικοινωνία μεταξύ των αποτελούμενων μερών

Σε περίπτωση που κάποια συνεργαζόμενη Αρχή Καταχώρισης ή Αρχή Πιστοποίησης επιθυμεί να διακόψει τη συνεργασία με την ΥΔΚ ΕΣ, οφείλει να ενημερώσει εγγράφως την Κεντρική Υπηρεσία Πιστοποίησης. Ανάλογη επικοινωνία επιβάλλεται σε περιπτώσεις εκδήλωσης ενδιαφέροντος από μονάδες του ΕΣ που επιθυμούν να συμμετέχουν στην ΥΔΚ ΕΣ.

9.12. Τροποποιήσεις

9.12.1. Διαδικασία τροποποιήσεων

Συντακτικές αλλαγές μπορούν να γίνουν στην ΠΠ/ΔΔΠ χωρίς καμία ειδοποίηση και χωρίς ανάγκη αλλαγής του αναγνωριστικού του κειμένου (OID).

9.12.2. Μηχανισμοί ενημέρωσης και περίοδος ενημέρωσης

Οι συνδρομητές θα ενημερώνονται εκ των προτέρων σε περίπτωση σημαντικών αλλαγών στην ΠΠ/ΔΔΠ. Η ΥΔΚ ΕΣ, οφείλει σε περιπτώσεις αλλαγών να δημοσιεύει και τις προηγούμενες κύριες εκδόσεις των κειμένων ΠΠ/ΔΔΠ στον ιστοχώρο της υπηρεσίας. Η τρέχουσα ενεργή ΠΠ/ΔΔΠ είναι δημοσιευμένη στη διεύθυνση…….

9.12.3. Συνθήκες κάτω από τις οποίες το OID θα πρέπει να αλλάζει

Σε περίπτωση σημαντικών-ουσιαστικών αλλαγών που δύνανται να επηρεάσουν την δυνατότητα αποδοχής της ΥΔΚ ΕΣ, θα πρέπει να μεταβληθεί το όνομα και το αναγνωριστικό (OID) της πολιτικής πιστοποίησης.

9.13. Διαδικασίες επίλυσης διαφορών

Διαφορές που προκύπτουν από την ερμηνεία της ΠΠ/ΔΔΠ και τη λειτουργία της ΥΔΚ ΕΣ θα επιλύονται σύμφωνα με την Ακαδημαϊκή δεοντολογία και τον Ελληνικό Νόμο. Αρμόδια ορίζονται τα δικαστήρια της Θεσσαλονίκης.

9.14. Ισχύουσα νομοθεσία

Η ΥΔΚ ΕΣ δημιουργήθηκε για να υπηρετήσει την Ακαδημαϊκή κοινότητα του ΕΣ. Κάθε πιστοποιητικό που εκδίδεται, αναφέρει ρητά στο πεδίο Certificate Policy Notice, το εξής κείμενο: “This certificate is subject to Greek laws and our CPS. This Certificate must only be used for academic, research or educational purposes” το οποίο μεταφράζεται στο εξής κείμενο: «Το συγκεκριμένο πιστοποιητικό υπόκειται στην Ελληνική νομοθεσία και τη Δήλωση Διαδικασιών Πιστοποίησης. Το πιστοποιητικό αυτό πρέπει να χρησιμοποιείται αποκλειστικά για ακαδημαϊκή, ερευνητική ή εκπαιδευτική χρήση». Η ΥΔΚ ΕΣ δεν θα εκτελεί οικονομικές συναλλαγές εκτός αν οριστεί διαφορετικά σε κάποια ενδιάμεση Αρχή Πιστοποίησης,

μέσω ξεχωριστού κειμένου Πολιτικής Πιστοποίησης. Η λειτουργία της ΥΔΚ ΕΣ καθώς και η ερμηνεία της Πολιτικής Πιστοποίησης/Δήλωσης Διαδικασιών Πιστοποίησης υπόκεινται κύρια στα Ακαδημαϊκά ήθη και στην Ελληνική Νομοθεσία. Ιδιαίτερα όσον αφορά το Προεδρικό Διάταγμα 150/2001 «Προσαρμογή στην οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές», τα πιστοποιητικά που εκδίδονται ΔΕΝ θεωρούνται γενικά ως «Αναγνωρισμένα Πιστοποιητικά», αν και όλες οι Αρχές Πιστοποίησης και τα εκδιδόμενα πιστοποιητικά ΚΑΛΥΠΤΟΥΝ τις τεχνικές προδιαγραφές των «Αναγνωρισμένων Πιστοποιητικών».

Κάτω από συγκεκριμένες προϋποθέσεις και συνθήκες, μπορούν τα πιστοποιητικά που εκδίδονται να χρησιμοποιηθούν ως «αναγνωρισμένα»-όπως αυτά ορίζονται στο ΠΔ 150/2001- πιστοποιητικά σε κλειστές ομάδες οντοτήτων, όπως για παράδειγμα σε κάποια διοικητική υπηρεσία του Ιδρύματος. Οι αντίστοιχες διαδικασίες θα πρέπει να περιγράφονται σε κείμενο Πολιτικής Πιστοποίησης/Δήλωση Διαδικασιών Πιστοποίησης (CP/CPS) της υφιστάμενης αυτής Αρχής Πιστοποίησης, λαμβάνοντας υπ' όψιν τις κείμενες διατάξεις και όλους τους όρους του ΠΔ 150/2001 (συμπεριλαμβανομένων των όρων για την Οικονομική ευθύνη). Το κείμενο CP/CPS κάθε υφιστάμενης αρχής δεν πρέπει να έρχεται σε αντίθεση με τους όρους του παρόντος κειμένου. Βασικές προϋποθέσεις για αυτή την αναγνώριση και κατά συνέπεια της αναγνώρισης της σχετικής παραγόμενης ψηφιακής υπογραφής ως ισότιμης με τη χειρόγραφη, είναι

α) η χρήση «ασφαλούς διάταξης δημιουργίας υπογραφής» στην πλευρά του πελάτη (π.χ. έξυπνη κάρτα όπου δημιουργείται, αποθηκεύεται και χρησιμοποιείται αποκλειστικά το ιδιωτικό κλειδί του πελάτη) και

β) η έγκριση του αρμόδιου οργάνου (π.χ. σύγκλητος).

9.15. Συμμόρφωση με την κείμενη νομοθεσία

Η ΥΔΚ ΕΣ συμμορφώνεται πλήρως με την κείμενη Ελληνική νομοθεσία.

9.16. Διάφορες Παροχές – Δεσμεύσεις

9.16.1. Υποχρεώσεις των Αρχών Πιστοποίησης

Μια Αρχή Πιστοποίησης είναι υπεύθυνη για την έκδοση και τη διαχείριση των πιστοποιητικών. Συγκεκριμένα, οι Αρχές Πιστοποίησης του ΕΣ δεσμεύονται:

- Να παρέχουν και να συντηρούν την υποδομή που απαιτείται για την σύσταση μιας ιεραρχίας πιστοποίησης για το Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, σύμφωνα με την Πολιτική και τις Διαδικασίες Πιστοποίησης που περιγράφονται στο έγγραφο αυτό.
- Να υλοποιούν και να συντηρούν τις απαιτήσεις ασφαλείας σύμφωνα με τα όσα ορίζονται στις σχετικές παραγράφους του παρόντος εγγράφου.
- Να αποδέχονται ή να απορρίπτουν αιτήσεις για έκδοση πιστοποιητικών σύμφωνα με τα όσα ορίζονται στις σχετικές παραγράφους του παρόντος εγγράφου.
- Να συντηρούν ένα χώρο αποθήκευσης ευρείας πρόσβασης για την αποθήκευση των πιστοποιητικών και των Λιστών Ανάκλησης Πιστοποιητικών. Οι πληροφορίες αυτές θα πρέπει να δημοσιοποιούνται μέσω ευρέως χρησιμοποιούμενων πρωτοκόλλων του παγκόσμιου ιστού, όπως HTTP, FTP και LDAP.
- Να ανακαλούν πιστοποιητικά όταν συντρέχουν λόγοι ή μετά από αίτημα του υποκειμένου ενός πιστοποιητικού.
- Να διατηρούν τις Λίστες Ανάκλησης Πιστοποιητικών πρόσφατα ενημερωμένες.

- Να διαχειρίζονται εμπιστευτικά όλες τις προσωπικές πληροφορίες που παρέχονται από τους εγγραφόμενους στην Υπηρεσία Πιστοποίησης.
- Να ενημερώνουν άμεσα το τεχνικό προσωπικό των υφιστάμενων ΑΠ, για έκθεση, απώλεια, δημοσιοποίηση, τροποποίηση, ή μη εγκεκριμένη χρήση του μυστικού κλειδιού των ΑΠ.
- Να διασφαλίζουν ότι όλα τα θέματα αναφορικά με τις υπηρεσίες που παρέχουν, όλες οι λειτουργίες που εκτελούνται και το σύνολο της υποδομής συμμορφώνονται με την παρούσα Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης.

9.16.2. Υποχρεώσεις υφιστάμενων ΑΠ

Κάθε υφιστάμενη Αρχή Πιστοποίησης εγκεκριμένη από την Υποδομή Δημοσίου Κλειδιού του ΕΣ δεσμεύεται:

- Να μην χορηγεί πιστοποιητικά με περίοδο εγκυρότητας μεγαλύτερη από την περίοδο ισχύος της εργασιακής ή άλλου είδους σχέσης, μεταξύ του αιτούντος και του φορέα με τον οποίο αυτός σχετίζεται, με την ιδιότητα που κατέχει κατά τη στιγμή της έκδοσης του πιστοποιητικού.
- Να ενημερώνει άμεσα την σχετική Κεντρική Αρχή Πιστοποίησης του ΕΣ σε περιπτώσεις έκθεσης του μυστικού κλειδιού.
- Να προστατεύει το μυστικό ισχυρό κωδικό που χρησιμοποιείται για την υπογραφή πιστοποιητικών τουλάχιστον στο επίπεδο ασφαλείας που ορίζεται στο παρόν κείμενο.
- Να αναπτύξει –αν το επιθυμεί- τις δικές της Διαδικασίες Πιστοποίησης, οι οποίες θα πρέπει να είναι τουλάχιστον τόσο αυστηρές και δεσμευτικές όσο είναι αυτή που περιγράφεται σε αυτό το έγγραφο.

9.16.3. Υποχρεώσεις των Αρχών Καταχώρισης

Κάθε Αρχή Καταχώρισης διεκπεραιώνει τις αιτήσεις εγγραφών των συνδρομητών.

- Κάθε ΑΚ είναι υπεύθυνη για τη λήψη των αιτήσεων πιστοποίησης, την πιστοποίηση της ταυτότητας του συνδρομητή, την επιβεβαίωση ότι το δημόσιο κλειδί που υποβάλλεται ανήκει σε αυτόν και για τη μεταβίβαση της αίτηση με ασφαλή τρόπο στην αντίστοιχη ΑΠ.
- Η λήψη των αιτήσεων μπορεί να πραγματοποιηθεί – ανάλογα με την κλάση του πιστοποιητικού που πρόκειται να εκδοθεί - είτε με την αυτοπρόσωπη υποβολή από τον ενδιαφερόμενο, είτε μέσω ηλεκτρονικού ταχυδρομείου είτε μέσω ειδικής φόρμας σε ιστοσελίδα, όπου υπάρχει μηχανισμός ασφαλούς αυθεντικοποίησης του χρήστη. Η αίτηση θα πρέπει να περιλαμβάνει τα προσωπικά στοιχεία ταυτότητας του εγγραφόμενου και το δημόσιο κλειδί που ο ίδιος έχει δημιουργήσει.
- Είναι δυνατή η μαζική υποβολή αιτήσεων από μία συγκεκριμένη υπηρεσία, για λογαριασμό των φυσικών προσώπων που ανήκουν σε αυτή.
- Κάθε ΑΚ πρέπει να ελέγχει αν το πρόσωπο που αιτείται προσωπικό πιστοποιητικό χρήστη, είναι ο δικαιούχος της πιστοποιημένης διεύθυνσης e-mail.
- Κάθε ΑΚ πρέπει να ελέγχει αν το πρόσωπο που αιτείται πιστοποιητικό συσκευής είναι ο κάτοχος του ονόματος FQDN και ο διαχειριστής της συσκευής.

9.16.4. Υποχρεώσεις των συνδρομητών

- Οι συνδρομητές στην Υπηρεσία είναι υποχρεωμένοι να διαβάσουν, να αποδεχθούν και να τηρούν την ΠΠ/ΔΔΠ. Οι συνδρομητές είναι υποχρεωμένοι να χρησιμοποιούν το πιστοποιητικό μόνο σε χρήσεις σύμφωνες με την ΠΠ/ΔΔΠ και το ισχύον νομοθετικό πλαίσιο.
- Οι συνδρομητές πρέπει να δημιουργήσουν ένα ζεύγος κλειδιών χρησιμοποιώντας ένα αξιόπιστο σύστημα και να λάβουν προφυλάξεις για την προστασία του ιδιωτικού κλειδιού τους από τυχαία καταστροφή, απώλεια ή κλοπή.
- Οι συνδρομητές με την παραλαβή του πιστοποιητικού, αποδέχονται ότι οι πληροφορίες που περιέχονται σε αυτό είναι αληθινές και σωστές.
- Οι συνδρομητές είναι υποχρεωμένοι να ζητούν από την ΑΠ την ανάκληση του πιστοποιητικού τους όταν αυτό δεν χρησιμοποιείται πλέον, όταν τα στοιχεία που περιέχει έχουν αλλάξει και όταν έχει εκτεθεί ή χαθεί ή υποπτευθεί ότι έχει εκτεθεί ή χαθεί το ιδιωτικό τους κλειδί.
- Ειδικά για την περίπτωση ψηφιακής υπογραφής κώδικα (code signing), οι συνδρομητές δεσμεύονται από την ΑΚ να παρέχουν πλήρεις, ακριβείς και αληθείς πληροφορίες (πχ όνομα εφαρμογής, URL με πληροφορίες της εφαρμογής, περιγραφή εφαρμογής, κ.α.) στον κώδικα που υπογράφουν.

9.16.5. Υποχρεώσεις των οντοτήτων που εμπιστεύονται τα πιστοποιητικά

- Οι οντότητες που εμπιστεύονται τα πιστοποιητικά είναι υποχρεωμένες να διαβάσουν και να αποδεχθούν την ΠΠ/ΔΔΠ και να χρησιμοποιούν το πιστοποιητικό μόνο σε χρήσεις σύμφωνες με την ΠΠ/ΔΔΠ και το ισχύον εθνικό νομικό πλαίσιο.
- Οι οντότητες που εμπιστεύονται τα πιστοποιητικά πρέπει να ελέγχουν την εγκυρότητα της υπογραφής του ψηφιακού πιστοποιητικού, να εμπιστεύονται το πιστοποιητικό της ΑΠ που το έχει εκδώσει, να ελέγχουν την περίοδο ισχύος του πιστοποιητικού και να ελέγχουν περιοδικά την ΛΑΠ για τυχόν ανάκληση της ισχύος του.

9.16.6. Υποχρεώσεις αποθήκης

Κάθε ΑΠ (κεντρική ή ενδιάμεση) είναι υποχρεωμένη να τηρεί δημόσια προσβάσιμη αποθήκη δεδομένων στην οποία να καταχωρεί:

- το ψηφιακό πιστοποιητικό της,
- την ΠΠ/ΔΔΠ,
- τις επιμέρους Δηλώσεις Διαδικασιών Πιστοποίησης,
- τα εκδοθέντα πιστοποιητικά
- τη ΛΑΠ.

Βιβλιογραφικές πηγές

1. Υποδομή Δημοσίου Κλειδιού (Public Key Infrastructure) στο Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Έκδοση 3.4, Δημήτρης Ζαχαρόπουλος, 23 Απριλίου 2012
2. Visa Public Key Infrastructure Certificate Policy (CP), Version 3.1, 31 March 2017
3. http://www.harica.gr/index.php.el
4. https://www.eugdpr.org/
5. https://ec.europa.eu/digital-single-market/en/trust-services-and-eid
6. "An Overview of Public Key Infrastructures (PKI)". Techotopia. Retrieved 26 March 2015, http://www.techotopia.com/index.php/An_Overview_of_Public_Key_Infrastructures_(PKI)#What_is_a_Public_Key_Infrastructure.3F
7. Κανονισμός (ΕΕ) 2016/679 ΤΟΥ Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 - http://eur-lex.europa.eu/legal-content/EL/TXT/?uri=celex%3A32016R0679