Ακαδημαϊκό Διαδίκτυο
GUnet

Υποδομή Δημοσίου Κλειδιού
(Public Key Infrastructure)
των Ελληνικών Ακαδημαϊκών και Ερευνητικών Ιδρυμάτων

Hellenic Academic and Research Institutions Certification Authority (HARICA)

Πολιτική Πιστοποίησης και
Δήλωση Διαδικασιών Πιστοποίησης της Υποδομής Δημοσίου Κλειδιού των Ελληνικών Ακαδημαϊκών και Ερευνητικών Ιδρυμάτων

Έκδοση 3.2 (5 Ιουνίου 2015)

Υπεύθυνος εγγράφου: Δημήτρης Ζαχαρόπουλος

Ομάδα Εργασίας: Δημήτρης Ζαχαρόπουλος
Φώτης Λούκος
Απόστολος Παπαγιαννάκης
Ιωάννης Φενέρης

Πίνακας περιεχομένων

Έλεγχος Εκδόσεων

Version	Date	Comment
2.2	Μάρτιος 2011	• Προσαρμογές στην πολιτική του ETSI TS 101 456 "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates" • Προσαρμογή στην Ελληνικής νομοθεσίας όσον αφορά τις χρήσεις πιστοποιητικών • Αλλαγές σε θέματα φυσικής ασφάλειας και ασφάλειας προσωπικού, ασφάλειας κρυπτοσυσκευών που περιέχουν ιδιωτικά κλειδιά ΑΠ κατά τις προδιαγραφές FIPS 140-2 • Αλλαγές σε θέματα προστασίας ιδιωτικού κλειδιού • Κατάργηση MD5 αλγόριθμου κατακερματισμού • Προσθήκες για χρονοσήμανση • Προσθήκες για κλάσεις πιστοποιητικών για πιστοποίηση προσώπου • Αλλαγές στα περιγράμματα OCSP
2.3	Μάιος 2011	• Αλλαγή για ελάχιστο μέγεθος κλειδιού σε 2048bits • Αλλαγές σε χρόνους που αφορούν ΛΑΠ • Προσθήκες για απόδειξη ταυτότητας χρηστών
2.4, 2.5	Νοέμβριος, Δεκέμβριος 2011	• Προσθήκη και αλλαγές για περιορισμούς ονομάτων (nameConstraints)
2.6	Απρίλιος 2012	• Προσθήκη για πιστοποιητικά υπογραφής κώδικα, • Προσθήκη για λειτουργικότητα αποθήκης πιστοποιητικών
2.7	Απρίλιος 2013	• Προσαρμογές στην πολιτική CA/B Forum Baseline Requirements for the

		Issuance and Management of Publicly-Trusted Certificates v1.1, • Αλλαγές σε συχνότητα έκδοσης ΛΑΠ και χρόνους απόκρισης τεχνικών
3.0	Δεκέμβριος 2014	• Προσαρμογή στις πολιτικές CA/B Forum BR for Publicly-Trusted Certificates 1.1.9 • Προσαρμογή στο Microsoft Root Certificate Program –Technical Requirements 2.0 • Προσαρμογή στοMozilla Root CA program Policy 2.2 • Προσαρμογή στο ΠΔ 150/2001 • Αλλαγές σε περιγράμματα πιστοποιητικών και Policy OIDs
3.1	Φεβρουάριος 2015	• Προσθήκη επεκτάσεων αναγνωρισμένων πιστοποιητικών (qcStatements)
3.2	Ιούνιος 2015	• Αλλαγές στις επιτρεπτές τιμές του Υποκειμένου και της επέκτασης subjAltName • Αναφορά στα CAA records • Προσαρμογή στις πολιτικές CA/B Forum BR 1.2.5

1 Εισαγωγή

Η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure – PKI) για τα Ελληνικά Ακαδημαϊκά και Ερευνητικά Ιδρύματα υποστηρίζεται και διαχειρίζεται από το Ακαδημαϊκό Διαδίκτυο GUnet, ως υπηρεσία στα μέλη του – όλα τα ελληνικά Πανεπιστήμια και ΤΕΙ – για την εξυπηρέτηση της εκπαίδευσης και της έρευνας στη χώρα μας. Η υπηρεσία αυτή του GUnet, η οποία στη συνέχεια θα αναφέρεται ως Αρχή Πιστοποίησης των Ελληνικών Ακαδημαϊκών και Ερευνητικών Ιδρυμάτων (Hellenic Academic & Research Institutions Certification Authority – HARICA), δρα ως Πάροχος Υπηρεσιών Πιστοποίησης (Certification Services Provider – CSP). Η ανάπτυξη και η διαχείριση της υπηρεσίας ξεκίνησε στα πλαίσια των λειτουργιών του Ιδεατού Κέντρου Διαχείρισης Δικτύων (Virtual Network Operations Center – VNOC) του ΕΔΕΤ και συνεχίζεται στα πλαίσια του GUnet. Η διαχείριση της HARICA γίνεται από το Κέντρο Ηλεκτρονικής Διακυβέρνησης του Αριστοτελείου Πανεπιστήμιου Θεσσαλονίκης. Οι φορείς που συμμετέχουν σε αυτή την Υποδομή Δημοσίου Κλειδιού, αποδέχονται ανεπιφύλακτα την παρούσα Δήλωση Διαδικασιών Πιστοποίησης/Πολιτική Πιστοποίησης και συνυπογράφουν το σχετικό μνημόνιο.

1.1 Επισκόπηση

Η παρούσα Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης περιγράφει το σύνολο κανόνων το οποίο εφαρμόζεται για την έκδοση πιστοποιητικών από την Υποδομή Δημοσίου Κλειδιού της HARICA.

Η Αρχή Πιστοποίησης HARICA εκδίδει 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 εγκυρότητά του, θα πρέπει να λαμβάνουν γνώση και να συμμορφώνονται με το παρόν κείμενο.

Η HARICA ακολουθεί τα ακόλουθα πρότυπα για την Υποδομή Δημοσίου Κλειδιού της:

- ETSI TS 101 456 v1.4.3, που πιστοποιήθηκε από την εταιρία Deventum και την εταιρία QMSCERT. Ο εξωτερικός έλεγχος έγινε σύμφωνα με τις τεχνικές διαδικασίες που περιγράφονται στο πρότυπο Electronic Signatures and Infrastructures (ESI); “Policy requirements for certification authorities issuing qualified certificates” για συμμόρφωση σε έκδοση πιστοποιητικών που καλύπτουν προδιαγραφές τύπου “QCP” και “QCP+SSCD”.
- ETSI TS 102 042, που πιστοποιήθηκε από την εταιρία Deventum. Ο εξωτερικός έλεγχος έγινε σύμφωνα με τις τεχνικές διαδικασίες που περιγράφονται στο πρότυπο Electronic Signatures and Infrastructures (ESI); “Policy requirements for certification authorities issuing public key certificates” για συμμόρφωση σε έκδοση πιστοποιητικών που καλύπτουν προδιαγραφές τύπου “DVCP”, “OVCP”
- Αναγνωρισμένα Πιστοποιητικά, ακολουθώντας το ΠΔ 150/2001 και την Ευρωπαϊκή οδηγία 1999/93/ΕC του Ευρωπαϊκού Κοινοβουλίου “a Community framework for electronic signatures”

1.2 Ονομασία και αναγνώριση κειμένου

Το παρόν κείμενο ονομάζεται «Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης της Υποδομής Δημοσίου Κλειδιού της HARICA» και αποτελεί την τεκμηρίωση και τον κανονισμό λειτουργίας της Υποδομής Δημοσίου Κλειδιού της Αρχής Πιστοποίησης των Ελληνικών Ακαδημαϊκών και Ερευνητικών Ιδρυμάτων (Hellenic Academic & Research Institutions Certification Authority – HARICA). Σε σύντμηση πρέπει να αναφέρεται ως «ΠΠ-ΔΔΠ της HARICA» και στην αγγλική του έκδοση ως 'HARICA CP-CPS'.

Σκοπός της Πολιτικής Πιστοποίησης είναι να προσδιορίσει, να καταγράψει και να κοινοποιήσει προς κάθε ενδιαφερόμενο μέρος (π.χ. μέλη της ακαδημαϊκής και ερευνητικής κοινότητας, συνεργάτες, εγγραφόμενοι, τρίτα μέρη που βασίζονται στην εγκυρότητα των υπηρεσιών, άλλους οργανισμούς, Ιδρύματα και Αρχές) τις συνθήκες και τις λειτουργικές πρακτικές που εφαρμόζονται ή διέπουν την παροχή των Υπηρεσιών Πιστοποίησης της HARICA.

Η δομή του παρόντος κειμένου βασίζεται στο πρότυπο IETF RFC- 3647 με ελάχιστες διαφοροποιήσεις που είναι αναγκαίες για να περιγραφούν οι ιδιαίτερες ανάγκες του Ακαδημαϊκού χώρου. Επίσης, έχουν υιοθετηθεί απαιτήσεις και προδιαγραφές από το κείμενο του CA/Browser Forum, "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v1.2.5" http://www.cabforum.org.

Ο παγκόσμια μοναδικός Αριθμός Αναγνώρισης (OID) αυτού του εγγράφου είναι: 1.3.6.1.4.1.**26513.1.0.3.2** όπου:

1.3.6.1.4.1.26513	Αριθμός Αναγνώρισης (OID) της HARICA, καταχωρημένος από τον οργανισμό IANA (www.iana.org)
1	Υπηρεσία Πιστοποίησης
0	Δήλωση Διαδικασιών Πιστοποίησης
3.2	Πρώτο και δεύτερο ψηφίο του αριθμού έκδοσης (version) της Δήλωσης Διαδικασιών Πιστοποίησης

1.3 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 της HARICA.

1.3.1 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. Κορυφαίες Κεντρικές Αρχές Πιστοποίησης (Root Certification Authority, HARICA-ROOT-CA) οι οποίες εκδίδουν αποκλειστικά ψηφιακά πιστοποιητικά για υφιστάμενες Αρχές Πιστοποίησης για λογαριασμό άλλων ακαδημαϊκών ιδρυμάτων ή

σε άλλους οργανισμούς και δεν εκδίδει πιστοποιητικά για τελικές οντότητες. Κατ' εξαίρεση, επιτρέπεται η έκδοση πιστοποιητικού για τους OCSP responders σύμφωνα με το RFC2560 και το draft-cooper-pkix-rfc2560bis-00.txt (βλ. Figure 7 στο draft: "Designated OCSP Responder and CA with Two Keys Certified by Root CA"). Το πιστοποιητικό της HARICA-ROOT-CA έχει διάρκεια ισχύος **είκοσι (20)** έτη. Σε περίπτωση που το κλειδί της ROOT είναι 2048 bits, θα πρέπει να σταματήσει η χρήση της μέχρι το έτος 2030. Αναλυτικά η περιγραφή των πιστοποιητικών ROOT βρίσκεται στο ΠΑΡΑΡΤΗΜΑ Α (ΚΕΝΤΡΙΚΕΣ ΑΠ - ROOTS HARICA).

2. Υφιστάμενες Αρχές Πιστοποίησης, υπό τον έλεγχο των διαχειριστών των ROOT CAs για λογαριασμό ακαδημαϊκών και ερευνητικών ιδρυμάτων που συμμορφώνονται και υιοθετούν πλήρως την παρούσα Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης. Τα πιστοποιητικά των Υφιστάμενων Αρχών Πιστοποίησης έχουν διάρκεια ισχύος έως **δέκα (10)** έτη. Αρχικά λειτουργεί η υφιστάμενη Αρχή Πιστοποίησης για τις οντότητες που ανήκουν διαχειριστικά στην HARICA (HARICA-Administration-CA) η οποία εκδίδει πιστοποιητικά σε χρήστες και συσκευές της HARICA, αλλά όχι για τελικούς χρήστες άλλων φορέων. Εφόσον ζητηθεί η έκδοση ψηφιακών πιστοποιητικών από την HARICA για τελικές οντότητες άλλων Ιδρυμάτων, θα δημιουργούνται οι αντίστοιχες υφιστάμενες Κεντρικές Αρχές Πιστοποίησης (Central Certification Authorities) για κάθε Ίδρυμα. Υπάρχει η δυνατότητα δημιουργίας περισσότερων της μίας υφιστάμενης ΑΠ πχ να δημιουργηθούν οι ΑΠ (<ΙΔΡΥΜΑ>-SUBSCRIBERS-CA και <ΙΔΡΥΜΑ>-SERVERS-CA) οι οποίες θα εκδίδουν ανάλογα πιστοποιητικά τελικών χρηστών, εξυπηρετητών αντίστοιχα αλλά θα υπογράφονται από την αντίστοιχη Κεντρική Αρχή Πιστοποίησης του ιδρύματος. Όποιος φορέας το επιθυμεί, έχει τη δυνατότητα να αναλάβει τη διαχείριση της Αρχής Πιστοποίησής του με ίδια μέσα. Στην περίπτωση αυτή, η ΑΠ χαρακτηρίζεται ως «ΑΠ εξωτερικής διαχείρισης» και θα πρέπει υποχρεωτικά να έχει τεχνικούς περιορισμούς (nameConstraints σύμφωνα με το RFC5280), να πιστοποιηθεί με εξωτερική πιστοποίηση (external audit) από ειδικά διαπιστευμένο επιθεωρητή ως προς τα πρότυπα των προγραμμάτων Microsoft/Mozilla/Apple και να καλύπτει τις απαιτήσεις του ΠΔ 150/2001. Σε περίπτωση που κάποια ενδιάμεση ΑΠ έχει διαφορετικές πολιτικές και διαδικασίες πιστοποίησης καθώς και στις περιπτώσεις ΑΠ εξωτερικής διαχείρισης, είναι υποχρεωτική η δημιουργία ξεχωριστού κειμένου ΠΠ/ΔΔΠ, με μοναδικό αναγνωριστικό OID το οποίο θα εμφανίζεται στην κατάλληλη επέκταση πιστοποιητικών (Πολιτικές Πιστοποίησης – Policy extension field) στο πιστοποιητικό της συγκεκριμένης ενδιάμεσης ΑΠ.

3. Η HARICA επιτρέπεται να εκδώσει πιστοποιητικά δια-πιστοποίησης (cross-certificates) κατά τη διαδικασία αλλαγής της κορυφαίας Αρχής Πιστοποίησης (ROOT) και μόνο για ΑΠ που βρίσκονται κάτω από τον άμεσο έλεγχό της. Όλα τα πιστοποιητικά δια-πιστοποίησης πρέπει να δημοσιεύονται.

1.3.2 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. Το GUnet λειτουργεί ως κεντρική Αρχή Καταχώρισης της ΥΔΚ HARICA και εφαρμόζει αυστηρές διαδικασίες πιστοποίησης ταυτότητας των χρηστών της υπηρεσίας πιστοποίησης.

1.3.3 Συνδρομητές (Subscribers)

Συνδρομητές στην Υποδομή Δημοσίου Κλειδιού είναι όσοι αιτούνται και αποκτούν ψηφιακό πιστοποιητικό υπογεγραμμένο από Αρχή Πιστοποίησης της HARICA ή από άλλη υφιστάμενη ΑΠ. Συνδρομητές στην Υπηρεσία μπορούν να είναι οντότητες (φυσικά πρόσωπα και συσκευές) που ανήκουν στους φορείς – συνδρομητές της ελληνικής ακαδημαϊκής, ερευνητικής και εκπαιδευτικής κοινότητας.

Η εγγραφή μη φυσικών προσώπων ή ρόλων (π.χ. ‘Πρύτανης’) στην Υπηρεσία, εκτός από την περίπτωση των δικτυακών συσκευών, δεν προβλέπεται στο παρόν κείμενο αλλά δεν απαγορεύεται. Η έκδοση ψηφιακών πιστοποιητικών ρόλων από μία υφιστάμενη ΑΠ κάποιου Ιδρύματος είναι δυνατή, εφόσον έχει προβλεφθεί και περιγραφεί η σχετική διαδικασία στην ΠΠ-ΔΔΠ και εφόσον η διαδικασία αυτή δεν συγκρούεται με κάποιον από τους όρους του παρόντος κειμένου.

1.3.4 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 της ελληνικής ακαδημαϊκής κοινότητας, 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 της HARICA 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

1.3.5 Άλλοι συμμετέχοντες

Δεν ορίζεται.

1.4 Χρήση των πιστοποιητικών

Τα πιστοποιητικά μπορούν να χρησιμοποιηθούν από τα μέλη της ευρύτερης ακαδημαϊκής και ερευνητικής κοινότητας, αλλά και από άλλους χρήστες, όπως περιγράφονται στη παράγραφο 1.3.

1.4.1 Κατάλληλες χρήσεις των πιστοποιητικών

Τα πιστοποιητικά μπορούν να χρησιμοποιηθούν μόνο για ακαδημαϊκούς, διοικητικούς και ερευνητικούς 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 εξής (η λίστα δεν είναι περιοριστική):

α) 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», με την έννοια του αναφέρεται σε συσκευές που ακολουθούν τις προδιαγραφές της παραγράφου 6.2.1 (π.χ. smart card ή e-token), ώστε να εξασφαλίζονται τουλάχιστον 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).

β) 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).

γ) 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.

δ) 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.

ε) 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.

στ) Στην υλοποίηση ασφαλών δικτυακών πρωτοκόλλων, όπως τα SSL, IPSec κλπ.

1.4.2 Απαγορευμένες χρήσεις των πιστοποιητικών

Τα πιστοποιητικά δεν μπορούν να χρησιμοποιηθούν για πράξεις πληρωμών (πχ πληρωμές μέσω πιστωτικών καρτών σε e-shop) ή για χρήσεις που δεν περιλαμβάνονται σε αυτές της 1ης παραγράφου της ενότητας 1.4.1.

1.5 Διαχείριση της πολιτικής

1.5.1 Οργανισμός που διαχειρίζεται την πολιτική

Το παρόν κείμενο καθώς και όλα τα κείμενα όρων χρήσης, συμφωνιών, μελέτες ασφάλειας και διαδικαστικά κείμενα, βρίσκονται υπό την εποπτεία και τον έλεγχο της Επιτροπής Διαχείρισης Πολιτικής Πιστοποίησης και Διαδικασιών HARICA (Policy Management Committee – PMC) που έχει οριστεί από το Διοικητικό Συμβούλιο της GUnet.

ca-admin@harica.gr
ΑΚΑΔΗΜΑΙΚΟ ΔΙΑΔΙΚΤΥΟ GUnet
Ε.Κ.Π.Α. - ΚΕΝΤΡΟ ΛΕΙΤΟΥΡΓΙΑΣ & ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΟΥ
ΠΑΝΕΠΙΣΤΗΜΙΟΥΠΟΛΗ 157 84
Τηλ: 210 7275611
Fax: 210 7275601

1.5.2 Πρόσωπο επικοινωνίας

ca@harica.gr
Δημήτρης Ζαχαρόπουλος [d.zacharopoulos@auth.gr]
Τηλ: 2310 998483
Fax: 2310 999100

Γιάννης Σαλματζίδης [jsal@it.auth.gr]
Τηλ: 2310 998498
Fax: 2310 999100

Σπύρος Μπόλης [sbol@noc.uoa.gr]
Τηλ: 210 7275611
Fax: 210 7275601

Αρχή Πιστοποίησης HARICA
ΑΚΑΔΗΜΑΙΚΟ ΔΙΑΔΙΚΤΥΟ GUnet
Ε.Κ.Π.Α. - ΚΕΝΤΡΟ ΛΕΙΤΟΥΡΓΙΑΣ & ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΟΥ
ΠΑΝΕΠΙΣΤΗΜΙΟΥΠΟΛΗ 157 84
Τηλ: 210 7275611
Fax: 210 7275601

1.5.3 Πρόσωπο που κρίνει τη συμμόρφωση στην πολιτική

cp@harica.gr
Δημήτρης Ζαχαρόπουλος [jimmy@it.auth.gr]
Τηλ: 2310 998483
Fax: 2310 999100

Γιάννης Σαλματζίδης [jsal@it.auth.gr]
Τηλ: 2310 998498
Fax: 2310 999100

Σπύρος Μπόλης [sbol@noc.uoa.gr]
Τηλ: 210 7275611
Fax: 210 7275601

Αρχή Πιστοποίησης HARICA
ΑΚΑΔΗΜΑΙΚΟ ΔΙΑΔΙΚΤΥΟ GUnet
Ε.Κ.Π.Α. - ΚΕΝΤΡΟ ΛΕΙΤΟΥΡΓΙΑΣ & ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΟΥ
ΠΑΝΕΠΙΣΤΗΜΙΟΥΠΟΛΗ 157 84
Τηλ: 210 7275611
Fax: 210 7275601

1.5.4 Διαδικασίες έγκρισης ΠΠ/ΔΔΠ

Η ΠΠ/ΔΔΠ εγκρίνεται από την ειδική επιτροπή Διαχείρισης Πολιτικής Πιστοποίησης και Διαδικασιών HARICA Όλες οι διορθώσεις και αλλαγές στα κείμενα πολιτικής και διαδικασιών από τις 13/5/2011 και έπειτα, θα δημοσιεύονται στον κεντρικό ιστοχώρο της HARICA.

Σημαντικές αλλαγές της ΠΠ/ΔΔΠ θα ανακοινώνονται σε εύλογο χρονικό διάστημα στους συνδρομητές και βασιζόμενα μέρη, πριν τεθούν σε εφαρμογή.

Η HARICA συμμορφώνεται με την τρέχουσα έκδοση των προδιαγραφών που ορίζονται στο κείμενο “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published” (BR) το οποίο είναι διαθέσιμο (στην Αγγλική γλώσσα) στον ιστοχώρο http://www.cabforum.org. Σε περίπτωση που υπάρχει ασυνέπεια μεταξύ του παρόντος κειμένου και συγκεκριμένων προδιαγραφών του “Baseline Requirements” κειμένου, ισχύουν οι προδιαγραφές του τελευταίου. Διευκρινίζεται ότι η HARICA δηλώνει ότι προτίθεται να παρακολουθεί διαρκώς τις όποιες αλλαγές δημοσιεύονται στο CA/B Forum BR, να υιοθετεί αυτές τις αλλαγές πριν τις καταληκτικές τους ημερομηνίες και να ενημερώνει κατάλληλα την παρούσα ΠΠ/ΔΔΠ.

Ακόμα κι αν δεν υπάρχει απαίτηση αλλαγής της ΠΠ/ΔΔΠ, η PMC θα συνεδριάζει σε ετήσια βάση προκειμένου να πραγματοποιεί επισκόπηση πολιτικής και διαδικασιών, και να εξετάζει θέματα βελτίωσης αυτών.

1.6 Ορισμοί και ακρωνύμια

Ελληνικός όρος	Συντόμευση	Αγγλικός όρος	Συντόμευση
Ασφαλής Διάταξη Δημιουργίας Υπογραφής	ΑΔΔΥ	Secure Signature Creation Device	SSCD
Αναγνωριστικό Αντικειμένου	ΑΑ	Object Identifier	OID
Αναγνωρισμένο Πιστοποιητικό		Qualified Certificate	QCP
Αναγνωρισμένο Πιστοποιητικό σε Ασφαλή Διάταξη		Qualified Certificate with SSCD	QCP+SSCD ή QCP+
Επιβεβαίωση κατοχής Domain		Domain Validation Cert. Policy	DVCP

Επιβεβαίωση Οργανισμού		Organizational Validation Cert. Policy	OVCP
Αρχή Καταχώρισης	ΑΚ	Registration Authority	RA
Αρχή Πιστοποίησης Πολιτικής	ΑΠΠ	Policy Certification Authority	PCA
Αρχή Πιστοποίησης	ΑΠ	Certification Authority	CA
Δήλωση Διαδικασιών Πιστοποίησης	ΔΔΠ	Certification Practice Statement	CPS
Δημόσιο Κλειδί		Public Key	
Διαδρομή Πιστοποίησης	ΔΠ	Certification Path	
Διακεκριμένο Όνομα	ΔΟ	Distinguished Name	DN
Έμπιστη Τρίτη Οντότητα	ΕΤΟ	Trusted Third Party	TTP
Ιδιωτικό Κλειδί		Private Key	
Ιεραρχική Δομή Πιστοποίησης	ΙΔΠ	Hierarchic Certification Structure	HCS
Κοινό Όνομα	ΚΟ	CommonName	CN
Λίστα Ανάκλησης Πιστοποιητικών	ΛΑΠ	Certificate Revocation List	CRL
Λίστα Έμπιστων Πιστοποιητικών	ΛΕΠ	Certification Trust List	CTL
Όνομα Οργανισμού	Ο	OrganizationName	O
Οργανωτική Μονάδα	ΟΜ	Organizational Unit	OU
Όνομα Χώρας	Χ	CountryName	C
Πιστοποιητικό		Certificate	
Πολιτική Πιστοποίησης	ΠΠ	Certification Policy	CP
Υποδομή Δημοσίου Κλειδιού	ΥΔΚ	Public Key Infrastructure	PKI
Επιτροπή Διαχείρισης Πολιτικής Πιστοποίησης και Διαδικασιών		Policy Management Committee	PMC
Υποκείμενο Πιστοποιητικού		Certificate Subject	
Ψηφιακά Πιστοποιητικά για Αρχή Πιστοποίησης		Certification Authority Digital Certificates	
Ψηφιακά Πιστοποιητικά για Εξυπηρετητές		Server Digital Certificates	
Ψηφιακά Πιστοποιητικά Ταυτότητας		Personal Identity Digital Certificates	
Ψηφιακά Πιστοποιητικά για Υπογραφή Αντικειμένων		Object-Signing Digital Certificates	
		Public-Key Cryptography Standards	PKCS
Εγγραφόμενος		Subscriber	
Οντότητα που εμπιστεύεται τα πιστοποιητικά		Relying Party	
Αποθήκη Δεδομένων		Data Repository	
Αυθυπόγραφα πιστοποιητικά		Self signed certificates	
Αναγνώριση		Identification	

Απόδειξη ταυτότητας		Authentication	
Συνοδεία ιδιωτικού κλειδιού		Private Key Escrow	
Χαρακτηριστικό πολιτικής		Policy Qualifier	
		Secure Socket Layer	SSL
		Uniform Resource Identifier	URI

2 Δημοσιοποίηση και αποθήκες

2.1 Αποθήκες

Η ΥΔΚ HARICA διαθέτει κεντρική αποθήκη δεδομένων όπου δημοσιεύονται κείμενα πολιτικής, πιστοποιητικά Αρχών Πιστοποίησης και τελικά πιστοποιητικά συνδρομητών/συσκευών στη διεύθυνση http://www.harica.gr. 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 ΥΔΚ HARICA διαθέτει κεντρική αποθήκη δεδομένων διαθέσιμη από το διαδίκτυο στην οποία δημοσιεύει το Ψηφιακό Πιστοποιητικό της (τύπου X.509.v3), τα Ψηφιακά Πιστοποιητικά που εκδίδονται σύμφωνα με τη Δήλωση Διαδικασιών Πιστοποίησης, την τρέχουσα ΛΑΠ, το κείμενο της Πολιτικής Πιστοποίησης / Δήλωση Διαδικασιών Πιστοποίησης και άλλα κείμενα σχετικά με τη λειτουργία της (πχ μνημόνιο συνεργασίας και συναντίληψης - MoU).

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

Η ηλεκτρονική διεύθυνση της αποθήκης της Υποδομής Δημοσίου Κλειδιού HARICA είναι http://www.harica.gr/rep_dyn.

Επιπλέον, είναι δυνατή η αποθήκευση και αναζήτηση πιστοποιητικών και ΛΑΠ σε υπηρεσίες καταλόγου της HARICA ή των συνεργαζόμενων ιδρυμάτων.

2.3 Συχνότητα δημοσιοποίησης

Η Λίστα Ανάκλησης Πιστοποιητικών ενημερώνεται σύμφωνα με τη παράγραφο 4.9.7.

Τα πιστοποιητικά που εκδίδονται από κάποια 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 με τη μορφή αναζήτησης. Η αναζήτηση γίνεται είτε με το σειριακό αριθμό του πιστοποιητικού, οπότε προβάλλεται μία εγγραφή, ή με τμήμα του διακεκριμένου ονόματος του αντικειμένου του πιστοποιητικού, οπότε είναι πιθανό να επιστραφεί λίστα πιστοποιητικών.

Ενδέχεται να επιβάλλεται περιορισμός στην πρόσβαση της αποθήκης 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

Όλες οι πληροφορίες που περιλαμβάνονται στα τελικά πιστοποιητικά πρέπει να επαληθεύονται κατά τη χρονική στιγμή έκδοσής τους.

3.1.1.1 Πιστοποιητικά χρηστών

Τα πιστοποιητικά χρήστη πρέπει να περιλαμβάνουν το ονοματεπώνυμο του χρήστη, την ηλεκτρονική του διεύθυνση (σύμφωνα με το rfc822), το όνομα του φορέα στον οποίον ανήκει, και τη συντομογραφία της χώρας.

Επίσης μπορούν να περιλαμβάνονται (προαιρετικά), συμπληρωματικά στοιχεία όπως οργανωτική μονάδα του φορέα στον οποίο ανήκει ο χρήστης και τοποθεσία στην οποία βρίσκεται και κατηγορία πιστοποιητικού.

3.1.1.2 Πιστοποιητικά συσκευών/υπηρεσιών

Τα πιστοποιητικά συσκευής (διακομιστή, δρομολογητή ή άλλης δικτυακής συσκευής) πρέπει να περιλαμβάνουν το πλήρες διακεκριμένο όνομα της συσκευής κατά την υπηρεσία ονοματολογίας (FQDN DNS), το όνομα του φορέα στον οποίον ανήκει, και τη συντομογραφία της χώρας. Δεν επιτρέπεται η πιστοποίηση διευθύνσεων IP ή γενικών ονομάτων συσκευών (hostnames).

Επίσης μπορούν να περιλαμβάνονται (προαιρετικά) συμπληρωματικά στοιχεία όπως η οργανωτική μονάδα του φορέα στον οποίο ανήκει η συσκευή και η τοποθεσία στην οποία βρίσκεται.

3.1.1.3 Πιστοποιητικά υπογραφής κώδικα (code signing)

Τα πιστοποιητικά υπογραφής κώδικα (code signing certificates), παρέχονται μέσω των πιστοποιητικών χρηστών που περιγράφονται στην παράγραφο 3.1.1.1. 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.

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

Παράβαση των όρων, μπορεί να οδηγήσει σε αυτεπάγγελτη ανάκληση του πιστοποιητικού που υπέγραψε τον κώδικα.

3.1.2 Υποχρέωση τα ονόματα να έχουν συγκεκριμένο νόημα

Τα ονόματα που περιλαμβάνονται στα πιστοποιητικά χρηστών, πρέπει με κάποιο τρόπο να συσχετίζονται με τον συνδρομητή/δικαιούχο του πιστοποιητικού.

3.1.3 Δυνατότητα έκδοσης ανώνυμων πιστοποιητικών ή πιστοποιητικών με ψευδώνυμα

Η ΥΔΚ HARICA δεν επιτρέπει έκδοση πιστοποιητικών σε ανώνυμους χρήστες. Η έκδοση πιστοποιητικών με την ύπαρξη ψευδωνύμων στο διακεκριμένο όνομα π.χ. «Πρύτανης», δεν προβλέπεται στην παρούσα δήλωση διαδικασιών πιστοποίησης αλλά και δεν απαγορεύεται. Τα «ψευδώνυμα» θα πρέπει να περιλαμβάνονται σε ξεχωριστό διακριτικό εντός του πιστοποιητικού, μετά από κατάλληλο έλεγχο/πιστοποίηση ότι το φυσικό πρόσωπο που συνδέεται με το συγκεκριμένο πιστοποιητικό έχει δικαίωμα χρήσης του ψευδώνυμου. Για παράδειγμα, στο ρόλο «Προϊστάμενος», θα πρέπει να υπάρχει ανάλογη πιστοποίηση ότι ο συνδρομητής κατέχει τον συγκεκριμένο ρόλο.

3.1.4 Κανόνες σύνταξης των ονομάτων

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

3.1.4.1 Πιστοποιητικά χρηστών

Στα πιστοποιητικά χρήστη, το όνομα χρήστη αντιστοιχίζεται στο χαρακτηριστικό «CN», η ηλεκτρονική διεύθυνση στο χαρακτηριστικό «E», το όνομα του φορέα στον οποίο ανήκει στο χαρακτηριστικό «O» ή/και «OU», η χώρα στο χαρακτηριστικό «C», και προαιρετικά, η τοποθεσία στην οποία βρίσκεται στο χαρακτηριστικό «L». Είναι επιθυμητό, σε κάθε περίπτωση, να ακολουθείται η ονοματολογία που χρησιμοποιείται από την Εθνική υπηρεσία καταλόγου (σήμερα στεγάζεται στο ds.grnet.gr). Τα πιστοποιητικά χρηστών της ΥΔΚ HARICA πρέπει στο Διακεκριμένο Όνομα να περιλαμβάνουν το χαρακτηριστικό “C=GR”.

3.1.4.2 Πιστοποιητικά συσκευών

Στα πιστοποιητικά συσκευής, το όνομα της (FQDN DNS) αντιστοιχίζεται υποχρεωτικά στο χαρακτηριστικό “Subject Alternative Name – SAN”, το όνομα του φορέα στον οποίο ανήκει στο χαρακτηριστικό ”O” ή/και“OU”, η χώρα στο χαρακτηριστικό ”C” και προαιρετικά, η τοποθεσία στην οποία βρίσκεται στο χαρακτηριστικό ”L”. Το χαρακτηριστικό “CN” είναι προαιρετικό αλλά σε περίπτωση που υπάρχει, πρέπει να περιλαμβάνει ένα από τα FQDN ονόματα από την επέκταση subjectAltName. Τα πιστοποιητικά συσκευών της ΥΔΚ HARICA πρέπει στο Διακεκριμένο Όνομα να περιλαμβάνουν το χαρακτηριστικό “C=GR”. Δεν επιτρέπεται η πιστοποίηση διευθύνσεων IP ή γενικών ονομάτων συσκευών (hostnames).

3.1.5 Μοναδικότητα ονομάτων

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

3.1.6 Διαδικασία επίλυσης διαφορών σχετικά με την κυριότητα ονόματος και ο ρόλος των εμπορικών σημάτων

Αρμόδιο όργανο για θέματα επίλυσης διαφορών σχετικά με την κυριότητα ονομάτων στην ΥΔΚ HARICA είναι η Γενική Συνέλευση των μελών της HARICA.

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.

Για Αναγνωρισμένα Πιστοποιητικά σε ασφαλείς διατάξεις (ΑΔΔΥ), σύμφωνα με το ΠΔ 150/2001 και τη σχετική Ευρωπαϊκή νομοθεσία (QCP+), τα ιδιωτικά κλειδιά δημιουργούνται απευθείας στις ασφαλείς διατάξεις δημιουργίας υπογραφής παρουσία του δικαιούχου του πιστοποιητικού και εξουσιοδοτημένου προσωπικού της ΑΚ που πιστοποιεί ότι το ιδιωτικό κλειδί δημιουργήθηκε στην ΑΔΔΥ. Η παρουσία εξουσιοδοτημένου προσωπικού μπορεί αποφευχθεί αν υπάρχει αξιόπιστη διαδικασία εξασφάλισης με τεχνικά μέσα, ότι το ιδιωτικό κλειδί δημιουργείται μόνο εντός της ΑΔΔΥ. Ο δικαιούχος είναι υπεύθυνος για την ασφάλεια της ΑΔΔΥ μέσω του Προσωπικού Αναγνωριστικού (Personal Identification Number - PIN) που την προστατεύει.

3.2.2 Απόδειξη ταυτότητας οργανισμού

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

Ο συνδρομητής πρέπει:

α) να είναι εγγεγραμμένος σε επίσημη υπηρεσία καταλόγου του φορέα του και να φαίνεται στην εγγραφή του ο φορέας στον οποίον ανήκει

β) ή να κατέχει διεύθυνση ηλεκτρονικού ταχυδρομείου σε επίσημη υπηρεσία του φορέα και η διοίκηση του φορέα 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 στην ΥΔΚ HARICA 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 ασφαλούς διάταξης (ΑΔΔΥ) και πιστοποιούνται παρουσία εξουσιοδοτημένου προσωπικού της Αρχής Καταχώρισης που ελέγχει ότι το κλειδί δημιουργήθηκε στην ασφαλή διάταξη. 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 ιδρύματος μπορεί να εκχωρήσει τον έλεγχο της ταυτότητας σε υπηρεσίες των μονάδων όπου ανήκουν οι συνδρομητές (πχ γραμματείες Σχολών/Τμημάτων) και στη συνέχεια να χρησιμοποιεί ηλεκτρονικούς τρόπους πιστοποίησης της ταυτότητας του συνδρομητή. 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, φοιτητική ταυτότητα) και το οποίο θεωρείται αξιόπιστο από την οικεία μονάδα. Εναλλακτικά, η ίδια η ΑΚ κάθε ιδρύματος 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 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.

Η Κεντρική Αρχή Καταχώρησης της HARICA χρησιμοποιεί τρεις μεθόδους ελέγχου της κυριότητας μιας διεύθυνσης e-mail:

- Η πρώτη μέθοδος χρησιμοποιεί απλή επιβεβαίωση μέσω e-mail. Ο χρήστης εισάγει τη διεύθυνση e-mail σε ιστοσελίδα της ΑΚ και ένα μήνυμα επιβεβαίωσης αποστέλλεται στην διεύθυνση αυτή για επιβεβαίωση. Στη συνέχεια, εφόσον επιβεβαιωθεί η δ/νση από τον χρήστη, αποστέλλεται μήνυμα προς τον διαχειριστή e-mail του Ιδρύματος στο οποίο ανήκει ο χρήστης το οποίο περιλαμβάνει τη διεύθυνση e-mail του χρήστη και το πλήρες ονοματεπώνυμό του. Στη συνέχεια, ο διαχειριστής ελέγχει αν τα στοιχεία είναι έγκυρα και δίνει τη συγκατάθεσή του στην ΑΚ για την έκδοση του πιστοποιητικού. Η έγκριση αυτή απαιτεί την αναγνώριση του χρήστη με έλεγχο ταυτοπροσωπίας. Σε περίπτωση που η διαδικασία ελέγχου ταυτότητας προηγήθηκε (πχ κατά την δημιουργία του λογαριασμού e-mail), δεν υπάρχει λόγος να επαναληφθεί.

- Η δεύτερη μέθοδος χρησιμοποιεί κάποιον κεντρικό εξυπηρετητή LDAP. Ο χρήστης εισάγει την ιδρυματική διεύθυνση e-mail στην αίτηση πιστοποιητικού και το ιδρυματικό κωδικό. Η πληροφορία αυτή επαληθεύεται μέσω του ιδρυματικού εξυπηρετητή LDAP και της υπηρεσία καταλόγου. Σε περίπτωση επιτυχίας, η ΑΚ αντλεί συμπληρωματικά στοιχεία από τον κατάλογο (το πλήρες ονοματεπώνυμο, Τμήμα κ.α.) τα οποία στη συνέχεια συνθέτουν το πιστοποιητικό. Προκειμένου να βρίσκεται ένας χρήστης στην Ιδρυματική Υπηρεσία Καταλόγου, το ίδρυμα θα πρέπει να έχει επαληθεύσει τα στοιχεία του χρήστη με έλεγχο ταυτοπροσωπίας μέσω επίσημου εγγράφου που φέρει την φωτογραφία του κατόχου.

- Η Τρίτη μέθοδος χρησιμοποιεί αρχιτεκτονική Single Sign On (SSO) που βασίζεται στο πρότυπο SAML. Ο συνδρομητής δίνει το Ιδρυματικό e-mail

του σε ειδική ιστοσελίδα και στη συνέχεια ανακατευθύνεται στην ιστοσελίδα του Παρόχου Ταυτοποίησης του οικείου Ιδρύματος του συνδρομητή. Ο συνδρομητής παρέχει τα ιδρυματικά του αναγνωριστικά στοιχεία και στη συνέχεια επιστρέφονται με ασφάλεια τα στοιχεία του συνδρομητή (το πλήρες ονοματεπώνυμο, Τμήμα, κ.α.) τα οποία στη συνέχεια συνθέτουν το πιστοποιητικό. Προκειμένου να πιστοποιηθεί ένας χρήστης σε Ιδρυματικό Πάροχο Πιστοποίησης, το ίδρυμα θα πρέπει να έχει επαληθεύσει τα στοιχεία του χρήστη με έλεγχο ταυτοπροσωπίας μέσω επίσημου εγγράφου που φέρει την φωτογραφία του κατόχου.

Τα πιστοποιητικά της κλάσης Α συνιστάται να περιέχουν ένα επιπλέον πεδίο οργανωτικής μονάδας (OU) στο πεδίο του αντικειμένου με τιμή ”Class A – Private Key created and stored in hardware CSP”. Επιπλέον, ΠΡΕΠΕΙ να περιέχουν το αναγνωριστικό id-etsi-qcs-QcSSCD στην επέκταση qcStatements. Τα πιστοποιητικά κλάσης Α, πληρούν τους όρους και προϋποθέσεις του ΠΔ 150/2001 σε ό,τι αφορά τις ασφαλείς διατάξεις δημιουργίας υπογραφής (ΑΔΔΥ). Τα πιστοποιητικά της κλάσης Β συνιστάται 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 υπεύθυνος για τη λειτουργία και τη συμμόρφωση της συσκευής στην πολιτική πιστοποίησης, συνιστάται να είναι ο ίδιος συνδρομητής πιστοποιητικού που έχει εκδοθεί από ΑΠ η οποία συμμορφώνεται με τη Δήλωση Διαδικασιών Πιστοποίησης/Πολιτική Πιστοποίησης της HARICA.

Ο συνδρομητής συνιστάται να συμπληρώνει αίτηση για έκδοση πιστοποιητικού σε ιστοσελίδα όπου πρέπει να πιστοποιηθεί παρουσιάζοντας το προσωπικό πιστοποιητικό του. Δεν επιτρέπεται η έκδοση πιστοποιητικού για συσκευή φορέα διαφορετικού από τον φορέα στον οποίο ανήκει ο υπεύθυνός του.

Η Κεντρική Αρχή Καταχώρησης της HARICA χρησιμοποιεί συγκεκριμένες μεθόδους για έλεγχο κυριότητας της πιστοποιούμενης συσκευής. Πρώτα απ’ όλα, η έκδοση πιστοποιητικού SSL/TLS για συσκευή επιτρέπεται μόνο για ζώνη DNS (domain) που ανήκει στο Ίδρυμα. Στη συνέχεια, προκειμένου ένας χρήστης να μπορεί να αιτηθεί πιστοποιητικό συσκευής (SSL/TLS), πρέπει να είναι κάτοχος πιστοποιητικού χρήστη το οποίο χρησιμοποιεί για να πιστοποιήσει την ταυτότητά του. Έπειτα, αποστέλλεται ένα μήνυμα e-mail σε εξουσιοδοτημένο Διαχειριστή της ΥΔΚ του Ιδρύματος 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 ίδρυμα.

Συμπληρωματικά με τις παραπάνω διαδικασίες, ένας συνδρομητής που ζητά την έκδοση πιστοποιητικού συσκευής για συγκεκριμένο ή περισσότερα FQDN, μπορεί να πιστοποιηθεί από τον Καταχωρητή Ονομάτων DNS (Domain Name Registrant), με τη διαδικασία που περιγράφεται στην ενότητα 11.1.1 του CA/B Forum BR. Για κάθε FQDN που θα περιλαμβάνεται σε ψηφιακό πιστοποιητικό συσκευής, η ΑΠ ΠΡΕΠΕΙ να επιβεβαιώσει ότι, κατά την ημερομηνία έκδοσης του πιστοποιητικού, ο αιτούμενος είτε είναι ο υπεύθυνος της Καταχώρησης του ονόματος σε επίσημο καταχωρητή ονομάτων

(Domain Name Registrant) ή έχει διαχειριστικό έλεγχο στο FQDN, το οποίο αποδεικνύεται με τις εξής μεθόδους:

- Απευθείας επιβεβαίωση από τον καταχωρητή μητρώου ονομάτων DNS
- Απευθείας επικοινωνία με τον αιτούντα, χρησιμοποιώντας διεύθυνση e-mail ή τηλέφωνο που βρίσκεται καταχωρημένο σε κεντρικό καταχωρητή μητρώου ονομάτων
- Απευθείας επικοινωνία με τον αιτούντα χρησιμοποιώντας πληροφορίες που βρίσκονται καταχωρημένες στις εγγραφές WHOIS, στα πεδία “registrant”, “technical” ή “administrative” field
- Επικοινωνία με τον διαχειριστή του Domain χρησιμοποιώντας ειδικές διευθύνσεις e-mail με συγκεκριμένα προθέματα ‘admin’, ‘administrator’, ‘webmaster’, ‘hostmaster’, ή ‘postmaster’ στο αριστερό μέρος της διεύθυνσης, στη συνέχεια το σύμβολο (“@”), και στη συνέχεια το Domain Name, από το αιτούμενο FQDN
- Βάσει πιστοποιητικού κατοχής Domain από επίσημο καταχωρητή ονομάτων DNS
- Ζητώντας από τον αιτούντα να αποδείξει έλεγχο του FQDN με τεχνικά μέσα, πραγματοποιώντας μια προ-συμφωνημένη αλλαγή σε πληροφορία που βρίσκεται σε δημόσια προσβάσιμο web server, σε URI που περιλαμβάνει το FQDN ή
- Χρησιμοποιώντας όποια άλλη μέθοδο επιβεβαίωσης, εξασφαλίζοντας ότι η CA τηρεί έγγραφα αποδεικτικά της μεθόδου επιβεβαίωσης ότι ο αιτούμενος είναι και κάτοχος του FQDN με το ίδιο επίπεδο βεβαιότητας όπως οι μέθοδοι που περιγράφονται ανωτέρω.

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 το ίδρυμα. Αυτό γίνεται είτε με ηλεκτρονικές λίστες που συγκεντρώνει η κάθε ΑΚ από τις αρμόδιες -για κάθε κατηγορία- πηγές (πχ γραμματείες τμημάτων/σχολών, δ/νση μηχανοργάνωσης διοίκησης κ.α.), είτε με προσκόμιση επικυρωμένων έγγραφων βεβαιώσεων των συνδρομητών όπου πιστοποιείται η σχέση του ενδιαφερόμενου με το ίδρυμα.

3.2.6 Κριτήρια για διαλειτουργικότητα

Δεν ορίζεται.

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)** ημέρες 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.

3.4 Επαλήθευση ταυτότητας για αιτήματα ανάκλησης

Ισχύουν όσα περιγράφονται στην παράγραφο 3.2.3. Επιπλέον, συνιστάται ο συνδρομητής, κατά την παραλαβή του πιστοποιητικού, να μαθαίνει έναν μυστικό κωδικό ανάκλησης του πιστοποιητικού (είτε πρόκειται για πιστοποιητικό χρήστη είτε για πιστοποιητικό συσκευής).

3.4.1 Αρχή Πιστοποίησης

Η ΑΠ μπορεί να ανακαλέσει πιστοποιητικά εφόσον έχει ισχυρές ενδείξεις και αποδείξεις ότι το ιδιωτικό κλειδί κάποιου συνδρομητή έχει διαρρεύσει ή έχει γίνει κακή χρήση του πιστοποιητικού. Μπορεί επίσης, να ανακαλέσει ένα πιστοποιητικό το οποίο έχει λάθος παραμέτρους/πληροφορίες. Κατ' εξαίρεση, ένα «αναγνωρισμένο πιστοποιητικό» μπορεί να ανακληθεί εφόσον:

- ζητηθεί επισήμως από Κρατική Αρχή ή την Εποπτεύουσα Αρχή για «Αναγνωρισμένα Πιστοποιητικά»
- κατά τη διάρκεια ελέγχου, διαπιστωθεί ότι το πιστοποιητικό περιέχει ψευδείς ή ανακριβείς πληροφορίες
- υπάρχει σχετική δικαστική απόφαση
- συντρέχουν κατάλληλες προϋποθέσεις σύμφωνα με την Εθνική και Ευρωπαϊκή Νομοθεσία (άρθρο 5 του Κανονισμού Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής (ΦΕΚ 603/Β/16-2-2002).

3.4.2 Συνδρομητής

Ο συνδρομητής μπορεί να αιτηθεί την ανάκληση του πιστοποιητικού μέσω κατάλληλης ιστοσελίδας, με τη χρήση του μυστικού κωδικού ανάκλησης. Εναλλακτικά, μπορεί να ζητηθεί ανάκληση πιστοποιητικού με τηλεφωνική επικοινωνία ή επιτόπου επίσκεψη του συνδρομητή στην αρμόδια Αρχή Καταχώρησης, οπότε και θα πρέπει να ακολουθήσει επιβεβαίωση της ταυτότητάς του βάσει πληροφοριών που είναι γνωστές μεταξύ Αρχής Καταχώρισης και συνδρομητή.

4 Απαιτήσεις λειτουργίας

4.1 Αιτήσεις για πιστοποιητικά

4.1.1 Ποιος δικαιούται να καταθέσει αίτημα για έκδοση πιστοποιητικού

Αιτήσεις για έκδοση πιστοποιητικού μπορούν να καταθέσουν μόνο οι συνδρομητές που περιγράφονται στην παράγραφο 1.3.3.

4.1.2 Ποια είναι η διαδικασία κατάθεσης αιτήματος για έκδοση πιστοποιητικού και ευθύνες

Το Διακεκριμένο Όνομα του πιστοποιητικού του αιτούντος πρέπει να είναι σύμφωνο με όσα αναφέρονται στην παράγραφο 3.2. Η πιστοποίηση της ταυτότητας του χρήστη πρέπει να έχει γίνει σύμφωνα με όσα ορίζονται στο κεφάλαιο 3.

Ο συνδρομητής μπορεί να υποβάλει την αίτηση για έκδοση του πιστοποιητικού στην ιστοσελίδα της Κεντρικής Αρχής Καταχώρισης, http://www.harica.gr/, ή στην Αρχή Καταχώρισης του ιδρύματός του.

4.2 Επεξεργασία των αιτήσεων πιστοποιητικών

4.2.1 Διαδικασίες ελέγχου ταυτότητας και ιδιότητας συνδρομητή

Η επεξεργασία των αιτήσεων βασίζεται σε όσα αναγράφονται στην παράγραφο 3.2. Όλα τα αιτήματα πρέπει να 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 οικείο φορέα.

4.2.2 Έγκριση ή απόρριψη αιτήσεων πιστοποιητικών

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

4.2.3 Χρόνος επεξεργασίας αιτήσεων πιστοποιητικών

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

4.2.4 Certificate Authority Authorization (CAA)

Η HARICA δεν ελέγχει επί του παρόντος τις εγγραφές τύπου CAA, όπως περιγράφονται στο IETF RFC 6844.

4.3 Έκδοση πιστοποιητικών

4.3.1 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.

4.3.2 Ενημέρωση του συνδρομητή από την ΑΠ σχετικά με την έκδοση του πιστοποιητικού

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

4.4 Αποδοχή των πιστοποιητικών

4.4.1 Συμπεριφορά που αποτελεί την παραλαβή πιστοποιητικών

Οι συνδρομητές της ΥΔΚ HARICA, συνιστάται να πρέπει να παραλάβουν (να ανακτήσουν και να εγκαταστήσουν) το νέο πιστοποιητικό μέσα σε **τριάντα (30) ημέρες,** διαφορετικά, συνιστάται το Πιστοποιητικό να ακυρώνεται και ο συνδρομητής να πρέπει να κάνει εκ νέου αίτηση. Προκειμένου να ανακτήσουν το πιστοποιητικό τους, συνιστάται να δηλώνουν σε συγκεκριμένη ιστοσελίδα ότι έχουν ελέγξει όλα τα στοιχεία του πιστοποιητικού, ότι αυτά είναι σωστά και αληθή. Τέλος, ότι αποδέχονται τους όρους και προϋποθέσεις της παρούσας ΔΠ/ΔΔΠ, και κατόπιν παραλαμβάνουν το πιστοποιητικό.

4.4.2 Δημοσίευση πιστοποιητικών από τις ΑΠ

Οι ΑΠ δημοσιεύουν τα πιστοποιητικά μόνο εφόσον έχει γίνει παραλαβή τους από τους δικαιούχους σύμφωνα με την παράγραφο 4.4.1.

4.4.3 Ενημέρωση άλλων οντοτήτων για την έκδοση πιστοποιητικών

Δεν προβλέπεται ενημέρωση άλλων οντοτήτων για τα νέα πιστοποιητικά πέραν των όσων περιγράφονται στην παράγραφο 9.16.

4.5 Ζεύγος κλειδιών και χρήσεις των πιστοποιητικών

4.5.1 Υποχρεώσεις συνδρομητών σχετικά με τη χρήση ιδιωτικών κλειδιών και πιστοποιητικών

Οι συνδρομητές της ΥΔΚ HARICA επιτρέπεται να χρησιμοποιούν τα ιδιωτικά κλειδιά και τα πιστοποιητικά τους σε χρήσεις για τις οποίες αυτά έχουν εκδοθεί. Τέτοιες χρήσεις περιγράφονται στην παράγραφο 6.1.7.

4.5.2 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 HARICA ακολουθώντας τα όσα αναγράφονται στην παράγραφο 1.3.4. 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)

4.6 Ανανέωση πιστοποιητικών

4.6.1 Συνθήκες κατά τις οποίες μπορεί να γίνει ανανέωση πιστοποιητικών

Ανανεώσεις πιστοποιητικών επιτρέπονται όταν πλησιάζει η λήξη ισχύοντος πιστοποιητικού. Ορισμένα πιστοποιητικά μπορούν να ανανεωθούν εφόσον δεν έχει ξεπεραστεί το χρονικό όριο ισχύος των κλειδιών που συνοδεύουν τα πιστοποιητικά. Θα πρέπει να ισχύουν όλα όσα αναγράφονται στην παράγραφο 1.3.3. Τα χρονικά όρια περιγράφονται στην παράγραφο 6.3.2. Συνιστάται όλα τα πιστοποιητικά που ανανεώνονται, να έχουν νέα ζεύγη κλειδιών.

4.6.2 Ποιος μπορεί να καταθέσει αίτημα ανανέωσης πιστοποιητικού

Το αίτημα ανανέωσης κατατίθεται από τον ίδιο τον δικαιούχο συνδρομητή. Συνιστάται να γίνεται μέσω πιστοποιημένης ιστοσελίδας μετά από διαδικασία ελέγχου ταυτότητας (authentication) στην οποία επιλέγει την ανανέωση. Οι δικαιούχοι συνδρομητές, συνιστάται να λαμβάνουν μήνυμα ηλεκτρονικού ταχυδρομείου από την Αρχή Καταχώρισης **δεκαπέντε (15) μέρες** πριν τη λήξη του πιστοποιητικού τους και να ενημερώνονται για την επικείμενη λήξη του. Οι δικαιούχοι στη συνέχεια έχουν τη δυνατότητα να καταθέτουν αίτημα επανέκδοσης. Συνιστάται να γίνεται μέσω πιστοποιημένης ιστοσελίδας μετά από διαδικασία ελέγχου ταυτότητας (authentication) στην οποία επιλέγουν έκδοση νέου πιστοποιητικού.

4.6.3 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 και ότι το κλειδί ικανοποιεί τις απαιτήσεις ασφαλούς κρυπτογράφησης
- Συμπληρωματικά, σε περίπτωση που στοιχεία του χρήστη όπως για παράδειγμα το ονοματεπώνυμο ή το e-mail, αλλάξουν, ακολουθούνται διαδικασίες έκδοσης νέου πιστοποιητικού.
- 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 **πέντε (5) χρόνια**. Τα ιδιωτικά κλειδιά για πιστοποιητικά εξυπηρετητών/συσκευών είναι **τρία (3) χρόνια**

4.6.4 Ενημέρωση συνδρομητών για τα ανανεωμένα πιστοποιητικά

Ακολουθείται η ίδια διαδικασία με την έκδοση νέου πιστοποιητικού, όπως περιγράφεται στην παράγραφο 4.3.2.

4.6.5 Αποδοχή ανανεωμένων πιστοποιητικών

Ο χρήστης/συνδρομητής πρέπει να παραλάβει το ανανεωμένο πιστοποιητικό ακολουθώντας την ίδια διαδικασία με την αποδοχή και παραλαβή νέου πιστοποιητικού, όπως περιγράφεται στην παράγραφο 4.4.1.

4.6.6 Δημοσίευση ανανεωμένων πιστοποιητικών

Το ανανεωμένο πιστοποιητικό δημοσιεύεται, σύμφωνα με τις διαδικασίες που περιγράφονται στην παράγραφο 4.4.2.

4.6.7 Ενημέρωση άλλων οντοτήτων για την ανανέωση πιστοποιητικών

Δεν προβλέπεται ενημέρωση άλλων οντοτήτων για τα ανανεωμένα πιστοποιητικά πέραν των όσων περιγράφονται στην παράγραφο 9.16.

4.7 Αλλαγή κλειδιών Πιστοποιητικών

4.7.1 Συνθήκες κατά τις οποίες μπορεί να γίνει αλλαγή κλειδιών

Αλλαγή κλειδιών σε πιστοποιητικά είναι η διαδικασία που οδηγεί σε επανέκδοση πιστοποιητικού με τα ίδια ακριβώς στοιχεία του υποκειμένου, την ίδια ημερομηνία λήξης (“validTo” πεδίο) αλλά με νέο ζεύγος κλειδιών. Η αλλαγή κλειδιών πιστοποιητικών επιτρέπεται εφόσον ισχύουν όλα όσα αναφέρονται στην ενότητα 1.3.3.

4.7.2 Πώς μπορεί να γίνει αίτημα αλλαγής κλειδιών πιστοποιητικών

Οι δικαιούχοι συνδρομητές, επικοινωνούν με την ΑΠ προκειμένου να ανακληθεί το ισχύον πιστοποιητικό. Οι δικαιούχοι στη συνέχεια έχουν τη δυνατότητα να καταθέτουν αίτημα αλλαγής κλειδιών πιστοποιητικού. Συνιστάται να γίνεται μέσω πιστοποιημένης ιστοσελίδας μετά από διαδικασία ελέγχου ταυτότητας (authentication).

4.7.3 Διαδικασίες των ΑΚ, ΑΠ για αιτήματα αλλαγής κλειδιών

Ακολουθείται η διαδικασία που προβλέπεται για έκδοση νέων πιστοποιητικών όπως περιγράφεται στην παράγραφο 4.3.

4.7.4 Ενημέρωση συνδρομητών για τα πιστοποιητικά όπου πραγματοποιήθηκε αλλαγή κλειδιού

Ακολουθείται η ίδια διαδικασία με την έκδοση νέων πιστοποιητικών όπως περιγράφεται στην παράγραφο 4.3.2.

4.7.5 Αποδοχή πιστοποιητικών στα οποία έγινε αλλαγή κλειδιού

Ο χρήστης/συνδρομητής πρέπει να παραλάβει το πιστοποιητικό με το νέο κλειδί, ακολουθώντας την ίδια διαδικασία με την αποδοχή νέου πιστοποιητικού, όπως περιγράφεται στην παράγραφο 4.4.1.

4.7.6 Δημοσίευση πιστοποιητικών στα οποία έγινε αλλαγή κλειδιού

Το πιστοποιητικό με το νέο κλειδί δημοσιεύεται, σύμφωνα με τις διαδικασίες της αποθήκης όπως περιγράφονται στην παράγραφο 4.4.2.

4.7.7 Ενημέρωση άλλων οντοτήτων για την έκδοση πιστοποιητικών με νέο κλειδί

Δεν προβλέπεται ενημέρωση άλλων οντοτήτων για τα πιστοποιητικά στα οποία το κλειδί επανεκδόθηκε πέραν των όσων περιγράφονται στην παράγραφο 9.16.

4.8 Μεταβολή Πιστοποιητικών

4.8.1 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, όπως περιγράφεται στην παράγραφο 4.3

4.8.2 Πώς μπορεί να γίνει αίτημα μεταβολής πιστοποιητικών

Μεταβολή στοιχείων πιστοποιητικών δεν επιτρέπονται.

4.8.3 Διαδικασίες των ΑΚ, ΑΠ για αιτήματα μεταβολής πιστοποιητικών

Μεταβολή στοιχείων πιστοποιητικών δεν επιτρέπεται.

4.8.4 Ενημέρωση συνδρομητών για τα πιστοποιητικά που μεταβλήθηκαν

Μεταβολή στοιχείων πιστοποιητικών δεν επιτρέπεται.

4.8.5 Αποδοχή πιστοποιητικών που μεταβλήθηκαν

Μεταβολή στοιχείων πιστοποιητικών δεν επιτρέπεται.

4.8.6 Δημοσίευση πιστοποιητικών που μεταβλήθηκαν

Μεταβολή στοιχείων πιστοποιητικών δεν επιτρέπεται.

4.8.7 Ενημέρωση άλλων οντοτήτων για την έκδοση πιστοποιητικών που μεταβλήθηκαν

Μεταβολή στοιχείων πιστοποιητικών δεν επιτρέπεται.

4.9 Αναστολή και ανάκληση πιστοποιητικών

4.9.1 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 συνιστάται να ανακαλείται όταν δεν το παραλάβει ο συνδρομητής μέσα στο χρονικό διάστημα που ορίζεται στη παράγραφο 4.4.1 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 αιτούντα με τον φορέα στον οποίο ανήκε όταν πιστοποιήθηκε (π.χ., αποφοίτηση, απόλυση, διακοπή σχέσης εργασίας).

4.9.2 Ποιος μπορεί να αιτηθεί ανάκληση

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

Επίσης, οι γραμματείες ή οι υπηρεσίες προσωπικού των φορέων, υποχρεούνται να αιτούνται ανάκληση για τα άτομα που χάνουν την ιδιότητα υπό την οποία πιστοποιήθηκαν.

Κατ' εξαίρεση, ένα «αναγνωρισμένο πιστοποιητικό» μπορεί να ανακληθεί εφόσον ζητηθεί επισήμως από Κρατική Αρχή ή την Εποπτεύουσα Αρχή για «Αναγνωρισμένα Πιστοποιητικά» ή υπάρχει σχετική δικαστική απόφαση.

4.9.3 Διαδικασία αιτήματος ανάκλησης

4.9.3.1 Ανάκληση του πιστοποιητικού από το συνδρομητή

Απαιτείται η πιστοποίηση της ταυτότητας του συνδρομητή σύμφωνα με τη παράγραφο 3.4. Μετά την ανάκληση, ο συνδρομητής του εν λόγω πιστοποιητικού θα ειδοποιείται για την αλλαγή της κατάστασης του Πιστοποιητικού και ότι το πιστοποιητικό δεν θα μπορεί να επανέλθει σε κανονική κατάσταση.

4.9.3.2 Ανάκληση του πιστοποιητικού από άλλη οντότητα

Απαιτείται 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 τον φορέα του. Μετά την ανάκληση, ο συνδρομητής του εν λόγω πιστοποιητικού θα ειδοποιείται για την αλλαγή της κατάστασης του Πιστοποιητικού και ότι το πιστοποιητικό δεν θα μπορεί να επανέλθει σε κανονική κατάσταση.

4.9.4 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.

4.9.5 Χρόνος απόκρισης της Υπηρεσίας Πιστοποίησης για ανακλήσεις πιστοποιητικών

Οι Αρχές Πιστοποίησης οφείλουν να ξεκινούν τη διερεύνηση του αιτήματος ανάκλησης εντός **μίας (1)** εργάσιμης ημέρας εκτός περιπτώσεων ανωτέρας βίας. Θα καταβάλλεται προσπάθεια ώστε τεκμηριωμένα αιτήματα ανάκλησης πιστοποιητικών να εξυπηρετούνται άμεσα.

4.9.6 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 προτού βασιστούν σε κάποιο πιστοποιητικό να ακολουθούν τις διαδικασίες της παραγράφου 1.3.4. Επίσης, θα πρέπει κάθε φορά πριν εμπιστευθούν οποιοδήποτε πιστοποιητικό της ΥΔΚ HARICA, να μεταφορτώνουν τις Λίστες Ανάκλησης Πιστοποιητικών (ΛΑΠ) όλων των ενδιάμεσων Αρχών Πιστοποίησης που μεσολαβούν μέχρι την εκδότρια αρχή του τελικού πιστοποιητικού. Οι λίστες ανάκλησης βρίσκονται πάντα δημοσιευμένες στην Αποθήκη. Οι Λίστες Ανάκλησης Πιστοποιητικών θα περιλαμβάνουν την κατάσταση των ανακλημένων πιστοποιητικών το τουλάχιστον μέχρι την ημερομηνία λήξης τους.

Οι πάροχοι λογισμικού που επιθυμούν να δοκιμάσουν τη συμπεριφορά πιστοποιητικών της ΥΔΚ HARICA, μπορούν να χρησιμοποιήσουν τους ιστοχώρους:

- https://www.harica.gr που διαθέτει «έγκυρο» πιστοποιητικό
- https://revoked.harica.gr που διαθέτει «ανακλημένο» πιστοποιητικό
- https://expired.harica.gr που διαθέτει «ληγμένο» πιστοποιητικό.

4.9.7 Συχνότητα έκδοσης ΛΑΠ

Η ΛΑΠ θα εκδίδεται:

- για Πιστοποιητικά τελικών χρηστών/συσκευών, τουλάχιστον κάθε **μία (1) ημέρα**. Η ΛΑΠ θα ισχύει για μέγιστο χρονικό διάστημα ίσο με **δέκα (10) ημέρες**
- για Πιστοποιητικά Αρχών Πιστοποίησης, τουλάχιστον κάθε **δώδεκα (12) μήνες**. Η ΛΑΠ θα ισχύει για μέγιστο χρονικό διάστημα ίσο με **δώδεκα (12) μήνες**

Σε περίπτωση έκθεσης μυστικού κλειδιού συνδρομητή ή άλλου σημαντικού συμβάντος όπως για παράδειγμα ανάκληση Αρχής Πιστοποίησης, θα εκδίδεται ενημερωμένη ΛΑΠ εντός 24 ωρών από την ανάκληση.

Οι ΛΑΠ θα βρίσκονται αποθηκευμένες σε προστατευμένο περιβάλλον προκειμένου να εξασφαλίζεται η ακεραιότητα και αυθεντικότητά τους.

4.9.8 Χρόνος δημοσίευσης ΛΑΠ στην αποθήκη

Μετά από την ανάκληση κάποιου πιστοποιητικού δημιουργείται 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 πρέπει να ειδοποιείται ο συνδρομητής και ο υπεύθυνος ασφαλείας της ΑΠ σε περίπτωση έκθεσης ιδιωτικού κλειδιού.

Οι ΑΠ πρέπει να λειτουργούν και να παρέχουν τις ΛΑΠ και τις δυνατότητες OCSP με ικανά συστήματα, προκειμένου να εξασφαλίζεται μέγιστος χρόνος απόκρισης τα δέκα (10) δευτερόλεπτα, υπό φυσιολογικές συνθήκες.

4.9.9 Διαθεσιμότητα υπηρεσίας ελέγχου κατάστασης πιστοποιητικών σε πραγματικό χρόνο (OCSP)

Στην ΥΔΚ HARICA λειτουργεί υπηρεσία ελέγχου καταστάσεις πιστοποιητικών σε πραγματικό χρόνο (On-line Certificate Status Protocol – OCSP). Η διεύθυνση της υπηρεσίας είναι ενσωματωμένη στα πιστοποιητικά που εκδίδονται. Η λειτουργία της υπηρεσίας OCSP είναι υποχρεωτική μόνο για υφιστάμενες Αρχές Πιστοποίησης που βρίσκονται υπό τη διαχείριση των φορέων της HARICA και εκδίδουν δημόσια αναγνωρισμένα πιστοποιητικά.

4.9.10 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 προτού βασιστούν σε κάποιο πιστοποιητικό να ακολουθούν τις διαδικασίες της παραγράφου 1.3.4. Επίσης, θα πρέπει κάθε φορά πριν εμπιστευθούν οποιοδήποτε πιστοποιητικό της ΥΔΚ HARICA, να ελέγχουν την υπηρεσία OCSP της ΥΔΚ HARICA 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. Η λειτουργία της υπηρεσίας OCSP είναι υποχρεωτική μόνο για υφιστάμενες Αρχές Πιστοποίησης που βρίσκονται υπό τη διαχείριση των φορέων της HARICA και εκδίδουν δημόσια αναγνωρισμένα πιστοποιητικά.

4.9.11 Άλλες μορφές ανακοίνωσης ανάκλησης πιστοποιητικών

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

4.9.12 Παραλλαγές των παραπάνω για την περίπτωση έκθεσης του ιδιωτικού κλειδιού

Ισχύει ότι ορίζεται στη παράγραφο 4.9.3.2.

4.9.13 Περιπτώσεις αναστολής πιστοποιητικών

Δεν προβλέπεται αναστολή των πιστοποιητικών.

4.9.14 Ποιος μπορεί να αιτηθεί αναστολή πιστοποιητικών

Δεν προβλέπεται αναστολή των πιστοποιητικών..

4.9.15 Διαδικασία αιτήματος αναστολής πιστοποιητικού

Δεν προβλέπεται αναστολή των πιστοποιητικών.

4.9.16 Χρονική περίοδος αναστολής πιστοποιητικού

Δεν προβλέπεται αναστολή των πιστοποιητικών.

4.10 Υπηρεσίες ελέγχου κατάστασης πιστοποιητικών

4.10.1 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.

4.10.1.1 Υπηρεσία ελέγχου κατάστασης πιστοποιητικών πραγματικού χρόνου OCSP

Ισχύουν όσα περιγράφονται στην παράγραφο 4.9.10

4.10.1.2 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 HARICA.

4.10.1.3 Χρήση των Λιστών Ανάκλησης Πιστοποιητικών (ΛΑΠ)

Ισχύουν όσα περιγράφονται στην παράγραφο 4.9.6.

4.10.2 Διαθεσιμότητα υπηρεσίας ελέγχου κατάστασης πιστοποιητικών

Θα καταβάλλεται προσπάθεια για πολύ υψηλή διαθεσιμότητα των υπηρεσιών ελέγχου κατάστασης πιστοποιητικών.

4.10.3 Προαιρετικά χαρακτηριστικά

Δεν ορίζεται.

4.11 Λήξη συνδρομής

Μετά τη λήξη της χρονικής ισχύος των πιστοποιητικών της ΥΔΚ HARICA, δεν είναι απαραίτητη η ανάκλησή τους, παρά μόνο αν συντρέχει κάποιος από τους λόγους που αναφέρονται στην παράγραφο 4.9.1.

4.12 Συνοδεία ιδιωτικού κλειδιού (key escrow) και επαναφορά κλειδιού

4.12.1 Διαδικασίες και πρακτικές συνοδείας ιδιωτικού κλειδιού και επαναφοράς

Δεν ορίζεται.

4.12.2 Ενθυλάκωση κλειδιού συνόδου (session key) και διαδικασίες και πρακτικές επαναφοράς

Δεν ορίζεται.

5 Διοικητικοί, τεχνικοί και λειτουργικοί έλεγχοι

5.1 Φυσική ασφάλεια και έλεγχος πρόσβασης

5.1.1 Τοποθεσία εγκαταστάσεων

Η Κεντρική Αρχή Πιστοποίησης της HARICA βρίσκεται σήμερα εγκατεστημένη στο Κέντρο Ηλεκτρονικής Διακυβέρνησης (ΚΗΔ) του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης. Άλλες ενδιάμεσες Αρχές Πιστοποίησης μπορεί να βρίσκονται εντός και εκτός του ΚΗΔ ΑΠΘ.

Απαγορεύεται η απομάκρυνση/μετακίνηση εξοπλισμού, πληροφορίες και λογισμικό που σχετίζεται με τη λειτουργία των Αρχών Πιστοποίησης και Καταχώρισης της HARICA, σε άλλο φυσικό χώρο χωρίς έγκριση από τη διοίκηση της HARICA.

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.

Σε περίπτωση που μη εξουσιοδοτημένο προσωπικό πρέπει να εισέλθει στους χώρους των ΑΠ και ΑΚ, είναι απαραίτητο να συνοδεύονται από κάποιο μέλος του εξουσιοδοτημένου προσωπικού.

5.1.3 Κλιματισμός και ρύθμιση τροφοδοσίας με ρεύμα

Όλος ο εξοπλισμός της Υποδομής Δημοσίου Κλειδιού HARICA που σήμερα φιλοξενείται στο ΚΗΔ ΑΠΘ, 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 HARICA που σήμερα φιλοξενείται στο ΚΗΔ ΑΠΘ βρίσκεται σε χώρο που δεν κινδυνεύει σε μεγάλο βαθμό από πλημμύρες.

5.1.5 Πρόληψη και προστασία από φωτιά

Ο εξοπλισμός της ΥΔΚ HARICA που σήμερα φιλοξενείται στο ΚΗΔ ΑΠΘ υπόκειται 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 της HARICA, πρέπει να βρίσκονται σε αποσπώμενα αποθηκευτικά μέσα (CD Roms) ή άλλο αφαιρούμενο μέσο σε κρυπτογραφημένη μορφή, με κωδικό (passphrase) που γνωρίζει μόνο εξουσιοδοτημένο προσωπικό 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 της HARICA, βρίσκονται σε μαγνητικές ταινίες ή memory flash disks που κατέχουν εξουσιοδοτημένα στελέχη.

Και τα δύο παραπάνω αποθηκευτικά μέσα βρίσκονται σε φυσικές τοποθεσίες διαφορετικές από τους κεντρικούς εξυπηρετητές της HARICA, προστατευμένα από έκθεση σε νερό και φωτιά. Λαμβάνονται όλα τα κατάλληλα μέτρα προκειμένου όλα τα αποθηκευτικά μέσα να είναι ανθεκτικά σε αλλοιώσεις.

Σε περίπτωση χρήσης επαναχρησιμοποιούμενων αποθηκευτικών μέσων (πχ memory flash disks), τα αρχεία διαγράφονται με ασφάλεια προκειμένου να μην υπάρχει δυνατότητα επαναχρησιμοποίησης.

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 των εξυπηρετητών της HARICA. Το ιδιωτικό κλειδί της κάθε ΑΠ αποθηκεύεται πάντα κρυπτογραφημένο. Η μυστική φράση αποκρυπτογράφησης του κλειδιού είναι γνωστή τμηματικά, στο αρμόδιο έμπιστο προσωπικό των ΑΠ. Τα ιδιωτικά κλειδιά των Αρχών Πιστοποίησης που διαχειρίζεται η HARICA, βρίσκονται σε αποσπώμενα αποθηκευτικά μέσα. Αντίγραφο ασφαλείας όλης της Υποδομής Δημοσίου Κλειδιού της HARICA, βρίσκεται σε μαγνητική ταινία που κατέχει εξουσιοδοτημένο προσωπικό. 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 τους κεντρικούς εξυπηρετητές της HARICA, 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 με συγκεκριμένες διαδικασίες. Οι ρόλοι και τα καθήκοντα του προσωπικού περιγράφονται με σαφήνεια. Ανάλογα με το ρόλο, καθορίζονται και τα καθήκοντα του προσωπικού ακολουθώντας πάντα την αρχή των ελάχιστα απαιτούμενων προνομίων πρόσβασης (access rights) προκειμένου να μπορούν να εκτελούν απρόσκοπτα τα καθήκοντά τους.

Το προσωπικό που ορίζεται να διαχειρίζεται τους εξυπηρετητές των Αρχών Καταχώρισης 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

Το προσωπικό που έχει έμπιστους ρόλους, πρέπει να αναγνωρίζεται/ταυτοποιείται στο σύστημα ΑΠ/ΑΚ πριν εκτελέσει συγκεκριμένα καθήκοντα που εμπίπτουν στον έμπιστο ρόλο που του έχει ανατεθεί.

5.2.4 Ρόλοι που απαιτούν διαχωρισμό καθηκόντων

Επιπλέον, θα εξασφαλίζεται ότι το προσωπικό που ανήκει στο ρόλο «ελεγκτή ασφάλειας ΑΠ» δεν θα ανήκει σε ρόλο που αναλαμβάνει καθημερινές διαχειριστικές εργασίες.

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. Θα απασχολείται ικανός αριθμός ανθρώπων με υψηλή εξειδίκευση.

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 κάθε φορέα που διαχειρίζεται Αρχές Πιστοποίησης και Αρχές Καταχώρησης. Όλα τα μέλη τους προσωπικού απαγορεύεται να έχουν σύγκρουση συμφερόντων με την υπηρεσία.

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 της HARICA από τεχνικούς του GUnet. Για το σκοπό αυτό υπάρχει κατάλληλη τεκμηρίωση που περιγράφει όλες τις λειτουργικές διαδικασίες της υποδομής. Το προσωπικό που λειτουργεί μέσα στην ΥΔΚ HARICA πρέπει να γνωρίζει μεταξύ άλλων όλα τα κείμενα πολιτικής/διαδικασιών και ειδικά την Δήλωση Διαδικασιών Πιστοποίησης και την Πολιτική Πιστοποίησης της ΥΔΚ HARICA.

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.

5.3.7 Έλεγχος σε προσωπικό ανεξάρτητων εργολάβων που εργάζονται εκτός του GUnet και εμπλέκονται με την ΥΔΚ HARICA

Σε περίπτωση κλήσης ανεξάρτητων εργολάβων για εργασίες στην ΥΔΚ HARICA, 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 από το GUnet και παρέχεται στους εκπαιδευόμενους που αναλαμβάνουν συγκεκριμένους ρόλους μέσα στην ΥΔΚ HARICA.

5.4 Διαδικασίες παρακολούθησης συναλλαγών συμβάντων

5.4.1 Τύποι συναλλαγών-συμβάντων που καταγράφονται

Τα συστήματα της ΥΔΚ HARICA 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 HARICA 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 όπως περιγράφεται στην παράγραφο 6.8.

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.

5.4.6 Σύστημα συγκέντρωσης αρχείων συναλλαγών-συμβάντων (εσωτερικό ή εξωτερικό σε σχέση με την οντότητα)

Δεν ορίζεται.

5.4.7 Ενημέρωση του υποκειμένου που προκάλεσε καταγραφή συναλλαγής-συμβάντος, για την ύπαρξη της καταγραφής

Δεν ορίζεται.

5.4.8 Αξιολογήσεις ευπάθειας του συστήματος καταγραφής συναλλαγών-συμβάντων

Η HARICA αξιολογείται ως προς την ασφάλεια των συστημάτων της με penetration tests, σε τακτά χρονικά διαστήματα, από έμπειρη ομάδα ασφάλειας η οποία εποπτεύεται από τον υπεύθυνο ασφάλειας της υποδομής.

5.5 Αρχειοθέτηση εγγραφών

5.5.1 Τύποι εγγραφών που αρχειοθετούνται

Όλα τα αρχεία συναλλαγών που αναφέρονται στην παράγραφο 5.4 αρχειοθετούνται με ασφάλεια, 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 που σχετίζονται με τα αιτήματα πιστοποιητικών και τους ελέγχους συνδρομητών, τηρούνται για χρονικό διάστημα τουλάχιστον **τριάντα (30) ετών** από τη λήξη/ακύρωση κάθε πιστοποιητικού, 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 με τις διαδικασίες της παραγράφου 4.1.

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 συνδρομητών/συσκευών ή σε περίπτωση παραβίασης των αλγορίθμων και των παραμέτρων που χρησιμοποιήθηκαν για τη δημιουργία ιδιωτικών κλειδιών και των 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 ευάλωτης 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, κάθε 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 συσταθεί ξανά με δημιουργία νέων Αρχών Πιστοποίησης, ξεκινώντας από νέα Κορυφαία Κεντρική Αρχή Πιστοποίησης.

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

Η ΥΔΚ HARICA έχει προβλέψει δυνατότητες αδιάλειπτης λειτουργίας με αποθήκευση αντιγράφων όλων των συστημάτων/υποσυστημάτων σε ασφαλή τοποθεσία εκτός των χώρων των εξυπηρετητών της HARICA, σύμφωνα με συγκεκριμένο πλάνο επιβίωσης (business continuity plan).

Σε περίπτωση σημαντικής καταστροφής ή άλλης απώλειας, λαμβάνονται κατάλληλα μέτρα για την αποφυγή παρόμοιου περιστατικού στο μέλλον.

5.8 Τερματισμός Αρχής Πιστοποίησης – Αρχής Καταχώρησης

Κατά τον τερματισμό της, κάθε 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 τον τερματισμό της λειτουργίας της. Σε κάθε περίπτωση, ισχύουν οι διατάξεις του Άρθρου 6 του ΦΕΚ 603/Β/16-5-2002 «Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής».

Τα αρχεία καταγραφής των ΑΚ και ΑΠ που σχετίζονται με τα αιτήματα πιστοποιητικών και οι έλεγχοι συνδρομητών, τηρούνται για χρονικό διάστημα τουλάχιστον **τριάντα (30) ετών** από τη λήξη/ακύρωση κάθε πιστοποιητικού, ώστε να είναι διαθέσιμα για ενδεχόμενο νόμιμο έλεγχο. Το διάστημα αυτό δύναται να τροποποιηθεί ανάλογα με τις εξελίξεις της σχετικής νομοθεσίας.

6 Έλεγχοι τεχνικής ασφάλειας

6.1 Δημιουργία ζεύγους κλειδιών και εγκατάσταση

6.1.1 Δημιουργία ζεύγους κλειδιών

Τα κλειδιά των συνδρομητών 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. 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, όπως περιγράφεται στην παράγραφο 3.2.3.1, θα πρέπει να υποβάλει την αίτηση παρουσία τεχνικού Αρχής Καταχώρησης ώστε να πιστοποιηθεί η χρήση της hardware κρυπτοσυσκευής, όπως ορίζεται στην παράγραφο 6.2.1.

Τα κλειδιά των ΑΠ δημιουργούνται σε ασφαλές περιβάλλον, είτε από ειδικό λογισμικό και στη συνέχεια εγκαθίστανται σε ειδικές κρυπτοσυσκευές (Hardware Security Modules – HSMs), είτε απευθείας σε κρυπτοσυσκευές (HSMs). Οι ειδικές κρυπτοσυσκευές πρέπει να καλύπτουν τις προδιαγραφές που ορίζονται στην παράγραφο 6.2.1.

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.

Για την έκδοση κλειδιών Κορυφαίας ή ενδιάμεσης ΑΠ, τηρείται προκαθορισμένη διαδικασία (key generation ceremony) η οποία εκτελείται παρουσία μελών εξουσιοδοτημένης Επιτροπής. Ειδικότερα για την έκδοση Κορυφαίας (ROOT) Αρχής Πιστοποίησης ή για ενδιάμεση «ΑΠ εξωτερικής διαχείρισης», η διαδικασία είτε γίνεται παρουσία εξωτερικού ελεγκτή (auditor) είτε βιντεοσκοπείται και στη συνέχεια αποστέλλεται σε εξωτερικό ελεγκτή ο οποίος εκδίδει σχετικό πόρισμα.

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 ή αυστηρότερη 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.
- Σε περίπτωση που η ΑΠ ή κάποια ΑΚ αντιληφθεί ότι το ιδιωτικό κλειδί συνδρομητή έχει δοθεί σε μη εξουσιοδοτημένο πρόσωπο ή οργανισμό που δεν σχετίζεται με τον συνδρομητή, τότε η ΑΠ ΠΡΕΠΕΙ να ανακαλέσει όλα τα πιστοποιητικά που περιέχουν το δημόσιο κλειδί που αντιστοιχεί στο ιδιωτικό κλειδί που απωλέσθηκε.

Ειδικά για την έκδοση «Αναγνωρισμένων Πιστοποιητικών σε ασφαλείς διατάξεις» (QCP+SSCD), ΑΠΑΓΟΡΕΥΕΤΑΙ Η ΔΗΜΙΟΥΡΓΙΑ ΙΔΙΩΤΙΚΟΥ ΚΛΕΙΔΙΟΥ ΧΩΡΙΣ ΤΟΝ ΑΠΟΛΥΤΟ ΕΛΕΓΧΟ ΤΟΥ ΣΥΝΔΡΟΜΗΤΗ.

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 αποστέλλουν αίτηση με ηλεκτρονικό ταχυδρομείο. Η ΑΠ αποστέλλει με ταχυδρομείο σε μαγνητικό μέσο το πιστοποιητικό της, το οποίο εμπεριέχει το δημόσιο κλειδί της. Εναλλακτικά, το πιστοποιητικό της κάθε ΑΠ δημοσιοποιείται μέσω ασφαλούς ιστοσελίδας, της οποίας η ταυτότητα πιστοποιείται από διαφορετική έμπιστη τρίτη οντότητα.

Αρκετά πριν τη λήξη ενός δημόσιου κλειδιού ΑΠ, θα δημιουργείται νέο ζεύγος κλειδιού προκειμένου να αποφευχθούν διακοπές στην παροχή των υπηρεσιών Πιστοποίησης.

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 RSA ή το αντίστοιχο του ECC (P256) ανεξάρτητα από τη χρήση του κλειδιού αυτού. Από την 1^{η} Ιανουαρίου 2016, οι ΑΠ που εκδίδουν πιστοποιητικά τύπου “codeSigning”, πρέπει να καταλήγουν σε Κορυφαία Αρχή Πιστοποίησης η οποία να έχει μέγεθος κλειδιού τουλάχιστον 4096 bits

σε περίπτωση χρήσης αλγόριθμου RSA ή το αντίστοιχο του ECC (P384). Τα πιστοποιητικά των ΑΠ που συνδέονται με πιστοποιητικά τύπου "codeSigning" πρέπει να χρησιμοποιούν αλγόριθμους κατακερματισμού τύπου "SHA2".

6.1.6 Παράμετροι δημιουργίας δημοσίων κλειδιών

Δεν ορίζεται.

6.1.7 Σκοποί χρήσης των κλειδιών (ως προς το αντίστοιχο πεδίο του X509)

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 τουλάχιστον τις παρακάτω χρήσεις:

Κλάσεις πιστοποιητικών φυσικών προσώπων:

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

Περισσότερες πληροφορίες για τα «προφίλ πιστοποιητικών» που χρησιμοποιούνται πιο συχνά, βρίσκονται στο ΠΑΡΑΡΤΗΜΑ Β (Προφίλ Πιστοποιητικών HARICA).

6.2 Προστασία ιδιωτικού κλειδιού

6.2.1 Προδιαγραφές για κρυπτογραφικές μονάδες

Όλα τα ιδιωτικά κλειδιά ΑΠ τα οποία φυλάσσονται σε κρυπτογραφικές μονάδες (Hardware Security Modules – HSMs), πρέπει να καλύπτουν κατ' ελάχιστο τις προδιαγραφές FIPS PUB 140-2 level 3 ή αντίστοιχα EAL 4+ ή υψηλότερες σύμφωνα με το πρότυπο ISO/IEC 15408. Υπάρχουν ειδικοί έλεγχοι για την αποτροπή φαινομένων παραβίασης και για έλεγχο καλής λειτουργίας των κρυπτογραφικών μονάδων. Τα ιδιωτικά κλειδιά των ΑΠ δεν μπορούν να εξαχθούν σε οποιαδήποτε μορφή και δεν είναι προσβάσιμα από εξωτερικούς –ως προς το HSM- μηχανισμούς.

Ιδιωτικά κλειδιά συνδρομητών μπορεί να δημιουργούνται και να φυλάσσονται είτε σε λογισμικό είτε σε ασφαλείς διατάξεις (ΑΔΔΥ). Στις περιπτώσεις «Αναγνωρισμένων Πιστοποιητικών σε Ασφαλείς Διατάξεις» (QCP+SSCD) (πιστοποιητικά «κλάσης Α»), το ιδιωτικό κλειδί πρέπει να δημιουργηθεί και να αποθηκευτεί σε ειδική ασφαλή διάταξη δημιουργίας υπογραφής κατά την έννοια και τις προδιαγραφές που περιγράφονται στο Παράρτημα ΙΙΙ του ΠΔ 150/2001. Οι ασφαλείς

διατάξεις δημιουργίας υπογραφής, ΠΡΕΠΕΙ να καλύπτουν κατ' ελάχιστο τις προδιαγραφές FIPS PUB 140-2 level 3 ή αντίστοιχα EAL 4+ ή υψηλότερες σύμφωνα με το πρότυπο ISO/IEC 15408.

6.2.2 Έλεγχος ιδιωτικού κλειδιού από πολλαπλά πρόσωπα (N-M)

Για τα ιδιωτικά κλειδιά των Αρχών Πιστοποίησης, προβλέπεται μηχανισμός κατακερματισμού των κωδικών ενεργοποίησης των ιδιωτικών κλειδιών ο οποίος περιγράφεται σε ξεχωριστό εσωτερικό έγγραφο.

6.2.3 Συνοδεία ιδιωτικού κλειδιού

Δεν ορίζεται.

6.2.4 Αντίγραφα ασφαλείας ιδιωτικού κλειδιού

Το ιδιωτικό κλειδί κάθε Αρχής Πιστοποίησης πρέπει να φυλάσσεται σε αντίγραφο ασφαλείας. Το κλειδί στο αντίγραφο πρέπει να είναι κρυπτογραφημένο και να ακολουθούνται οι διαδικασίες που περιγράφονται στην παράγραφο 5.1.6. Η πρόσβαση στο αντίγραφο ασφαλείας επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.

Η τήρηση αντιγράφων ασφαλείας για τα ιδιωτικά κλειδιά τελικών πιστοποιητικών συνδρομητών-συσκευών (εφόσον επιτρέπεται τεχνικά η συγκεκριμένη δυνατότητα), είναι αποκλειστικά στην ευχέρεια και ευθύνη των κατόχων των ιδιωτικών κλειδιών που αντιστοιχούν στα τελικά πιστοποιητικά που διαχειρίζονται.

6.2.5 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 Επίσης, ακολουθούνται οι διαδικασίες που περιγράφονται στην παράγραφο 5.1.6. Η πρόσβαση στο αρχειοθετημένο αντίγραφο ασφαλείας επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.

Όλα τα αντίγραφα ιδιωτικών κλειδιών Αρχών Πιστοποίησης που έχουν λήξει, αποσύρονται και δεν ξαναχρησιμοποιούνται.

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

Οι κάτοχοι των ιδιωτικών κλειδιών, μπορούν να μεταφέρουν κατά την κρίση τους το ιδιωτικό κλειδί τους από ειδικό κρυπτογραφικό σύστημα μορφής λογισμικού (software certificate store) σε οποιοδήποτε κρυπτογραφικό σύστημα μορφής υλικού (hardware) πχ crypto-tokens, smartcards. Αυτή η διαδικασία ΔΕΝ αλλάζει την κλάση του πιστοποιητικού από Β σε Α διότι το ιδιωτικό κλειδί δεν δημιουργήθηκε εξ αρχής σε hardware κρυπτοσυσκευή. Η αντίστροφη διαδικασία (μεταφορά κλειδιού από hardware σε software certificate store) δεν επιτρέπεται.

6.2.7 Με ποια μορφή αποθηκεύεται ένα ιδιωτικό κλειδί σε κρυπτογραφικό σύστημα

Τα ιδιωτικά κλειδιά ΑΠ ΠΡΕΠΕΙ να βρίσκονται εγκατεστημένα σε ειδικά κρυπτογραφικά συστήματα προκειμένου να εκτελέσουν εργασίες υπογραφής. Τα ιδιωτικά κλειδιά των συνδρομητών μπορούν επίσης να δημιουργηθούν σε ασφαλή διάταξη δημιουργίας υπογραφής. Ειδικά για την περίπτωση «Αναγνωρισμένων Πιστοποιητικών σε ασφαλή διάταξη δημιουργίας υπογραφής» (ΑΔΔΥ) (κατηγορίας Class A), το ιδιωτικό κλειδί ΠΡΕΠΕΙ να δημιουργηθούν σε ασφαλή διάταξη δημιουργίας υπογραφής και δεν μπορούν να μπορούν να εξαχθούν από αυτήν με κανένα μηχανισμό.

Τα κρυπτογραφικά συστήματα για ειδικές κατηγορίες πιστοποιητικών, ΠΡΕΠΕΙ να συμμορφώνονται με τις προδιαγραφές που περιγράφονται στην παράγραφο 6.2.1.

6.2.8 Μέθοδοι ενεργοποίησης (προς χρήση) ιδιωτικών κλειδιών.

6.2.8.1 Ποιος μπορεί να ενεργοποιήσει (χρησιμοποιήσει) ιδιωτικό κλειδί;

Μόνο συνδυασμός από εξουσιοδοτημένους διαχειριστές μπορεί να ενεργοποιήσει το ιδιωτικό κλειδί της κάθε ΑΠ προκειμένου να πραγματοποιήσουν κρυπτογραφικές διαδικασίες. Η διαδικασία περιγράφεται σε εσωτερικό κείμενο διαδικασιών της ΥΔΚ HARICA που περιγράφει την «τελετή ενεργοποίησης Αρχών Πιστοποίησης». Οι κρυπτογραφικές διαδικασίες (υπογραφές με χρήση των κλειδιών ΑΠ) πραγματοποιούνται μόνο μετά την ενεργοποίηση των κλειδιών που βρίσκονται στην ειδική κρυπτογραφική συσκευή HSM.

Το ιδιωτικό κλειδί τελικών πιστοποιητικών συνδρομητών-συσκευών συνίσταται να βρίσκεται επίσης προστατευμένο-κρυπτογραφημένο. Ο κάτοχος του κλειδιού είναι αποκλειστικά υπεύθυνος για την ενεργοποίηση και προστασία του ιδιωτικού κλειδιού που αντιστοιχεί στο τελικό πιστοποιητικό που διαχειρίζεται.

6.2.8.2 Ενέργειες που πρέπει να εκτελεστούν για την ενεργοποίηση ενός ιδιωτικού κλειδιού

Για την ενεργοποίηση κλειδιών Αρχών Πιστοποίησης που βρίσκονται σε ειδικές κρυπτοσυσκευές (HSMs), απαιτείται συνδυασμός στοιχείων ενεργοποίησης που γνωρίζει/κατέχει εξουσιοδοτημένο προσωπικό. Κάθε εξουσιοδοτημένο μέλος που κατέχει το ρόλο «ενεργοποίηση κλειδιών ΑΠ» γνωρίζει διαφορετικό στοιχείο των συστατικών ενεργοποίησης. Μόνο συνδυασμός από εξουσιοδοτημένα μέλη που κατέχουν το ρόλο «ενεργοποίηση κλειδιών ΑΠ» μπορεί να ενεργοποιήσει ένα ιδιωτικό κλειδί.

Για την ενεργοποίηση κλειδιών που χρησιμοποιούν κρυπτογραφικά συστήματα σε μορφή λογισμικού (πχ CryptoAPI στα MS Windows), ενδέχεται να μην ερωτάται 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 (file system permissions) ή άλλων αντίστοιχων μέτρων και μέσων προστασίας.

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

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

Ειδικά για το κλειδί που συνδυάζεται με πιστοποιητικά ROOT, το κλειδί παραμένει «ενεργό» μόνο για το διάστημα που απαιτείται να εκτελεστούν κρυπτογραφικές διαδικασίες πχ υπογραφή ενδιάμεσης ΑΠ, πιστοποιητικού OCSP, δημιουργία ΛΑΠ.

6.2.9 Μέθοδοι απενεργοποίησης ιδιωτικών κλειδιών.

Δεν ορίζεται.

6.2.10 Μέθοδοι καταστροφής ιδιωτικών κλειδιών.

Τα ιδιωτικά κλειδιά ΑΠ καταστρέφονται χρησιμοποιώντας ειδικές λειτουργίες διαγραφής με ασφάλεια, εντός του ειδικού κρυπτογραφικού συστήματος (HSM). Η καταστροφή αυτή, δεν εφαρμόζεται σε όλα τα αντίγραφα του ιδιωτικού κλειδιού παρά μόνο στα αντίγραφα που φυλάσσονται στο HSM. Μόνο συνδυασμός εξουσιοδοτημένου προσωπικού μπορεί να καταστρέψει ιδιωτικό κλειδί μιας ΑΠ.

Οι συνδρομητές είναι αποκλειστικά υπεύθυνοι, σε περίπτωση που το επιθυμούν. για την καταστροφή των ιδιωτικών κλειδιών που αντιστοιχούν στα πιστοποιητικά που διαχειρίζονται.

6.2.11 Βαθμολόγηση-αξιολόγηση κρυπτογραφικών συστημάτων

Δεν ορίζεται.

6.3 Άλλα θέματα διαχείρισης ζεύγους κλειδιών

6.3.1 Αρχειοθέτηση των δημόσιων κλειδιών

Τα δημόσια κλειδιά ενσωματώνονται στα ψηφιακά πιστοποιητικά κατά την έκδοσή τους και αρχειοθετούνται σύμφωνα με τις διαδικασίες που περιγράφονται στην παράγραφο 5.4.

6.3.2 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 **είκοσι (20)** έτη για Κεντρική ΑΠ, σε **δέκα (10**) έτη για ενδιάμεση ΑΠ, σε **πέντε (5) έτη** για πιστοποιητικά τελικών χρηστών και σε **τρία (3)** έτη για πιστοποιητικά 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 και εγκατάσταση δεδομένων ενεργοποίησης και εγκατάσταση

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

Σε περίπτωση ιδιωτικών κλειδιών τελικών χρηστών όπου χρησιμοποιείται μηχανισμός καταστροφής του ιδιωτικού κλειδιού μετά από ορισμένο αριθμό εσφαλμένων προσπαθειών πρόσβασης το μέγεθος του PIN μπορεί να είναι μικρότερο. Σε κάθε περίπτωση ισχύουν οι διαδικασίες που περιγράφονται στην παράγραφο 6.2.8.

6.4.2 Προστασία δεδομένων ενεργοποίησης

Δεν ορίζεται.

6.4.3 Άλλα θέματα δεδομένων ενεργοποίησης

Δεν ορίζεται.

6.5 Έλεγχοι ασφαλείας υπολογιστών

6.5.1 Συγκεκριμένες τεχνικές απαιτήσεις ασφάλειας

- Τα Λειτουργικά Συστήματα των υπολογιστών της ΥΔΚ HARICA διατηρούνται σε υψηλό επίπεδο ασφάλειας με εφαρμογή όλων των διεθνών προτύπων σε θέματα και οδηγίες ασφάλειας
- Υπάρχουν συστήματα καταγραφής ενεργειών και συναγερμού στους υπολογιστές της ΥΔΚ HARICA και περιοδικός έλεγχος των αρχείων καταγραφής για διαπίστωση τυχόν ανωμαλιών και απόπειρες παραβίασης, προκειμένου να ενεργοποιηθούν διαδικασίες αντίδρασης. Οι διαδικασίες αντίδρασης θα επιτρέψουν το προσωπικό να παρέμβει το συντομότερο δυνατό προκειμένου να περιορίσει το μέγεθος της παραβίασης της ασφάλειας.
- Τα προγράμματα που συνοδεύουν το Λειτουργικό Σύστημα είναι τα απολύτως απαραίτητα για την εύρυθμη λειτουργία των ΑΚ/ΑΠ και οι υπολογιστές θα προστατεύονται από κακόβουλο λογισμικό και μη εξουσιοδοτημένη εγκατάστασή του Όλα τα προγράμματα θα αναβαθμίζονται στις τελικές τους εκδόσεις όταν εμφανίζονται διορθώσεις προβλημάτων ασφάλειας που αφορούν το λογισμικό της ΥΔΚ.

6.5.2 Βαθμολόγηση ασφάλειας υπολογιστών

Δεν ορίζεται.

6.6 Έλεγχοι ασφαλείας κύκλου ζωής

6.6.1 Έλεγχοι ανάπτυξης συστημάτων

Δεν ορίζεται.

6.6.2 Έλεγχοι διαχείρισης ασφάλειας

Δεν ορίζεται.

6.6.3 Βαθμολόγηση ασφάλειας κύκλου ζωής

Δεν ορίζεται.

6.7 Έλεγχοι ασφαλείας δικτύου

Απαγορεύεται η σύνδεση των ΑΠ σε ευρύτερα δίκτυα δεδομένων ή άλλο τηλεπικοινωνιακό μέσο (πχ στο τηλεφωνικό δίκτυο μέσω modem). Η Αρχή Καταχώρισης προστατεύεται από το διαδίκτυο με ισχυρούς μηχανισμούς ασφάλειας συμπεριλαμβανομένου και firewall. Η δικτυακή μετάδοση ευαίσθητων πληροφοριών θα προστατεύεται μέσω κρυπτογραφικών μεθόδων για να εξασφαλιστεί η ακεραιότητα και μυστικότητα των πληροφοριών.

6.8 Χρονοσφραγίδες-Χρονοσήμανση

Όλες οι χρονοσφραγίδες και η χρονοσήμανση στην ΥΔΚ HARICA (είτε σε Αρχές Καταχώρισης είτε σε Αρχές Πιστοποίησης) ΠΡΕΠΕΙ να συγχρονίζονται μέσω πρωτοκόλλου NTP (Network Time Protocol).

7 Περίγραμμα πιστοποιητικού, ΛΑΠ και OCSP

7.1 Περίγραμμα πιστοποιητικού

Χρησιμοποιείται περίγραμμα πιστοποιητικού σύμφωνα με το RFC 5280 “Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile”

7.1.1 Βασικά χαρακτηριστικά Πιστοποιητικών

7.1.1.1 Έκδοση

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

7.1.1.2 Σειριακός Αριθμός

Κάθε πιστοποιητικό έχει ενσωματωμένο σειριακό αριθμό που δημιουργείται αυτόματα από το σύστημα. Απαγορεύεται να χρησιμοποιηθεί ο ίδιος σειριακός αριθμός σε άλλο πιστοποιητικό εντός της ίδιας Αρχής έκδοσης (subordinate CA).

7.1.1.3 Αλγόριθμος Υπογραφής

Αναφέρεται ο αλγόριθμος που χρησιμοποιήθηκε για τη δημιουργία του ψηφιακού πιστοποιητικού. Περιορισμοί στην επιλογή των αλγορίθμων, αναφέρονται στην παράγραφο 7.1.3.

7.1.1.4 Υπογραφή

Η υπογραφή της ΑΠ που εκδίδει το πιστοποιητικό. Οι αλγόριθμοι που χρησιμοποιούνται για τη δημιουργία υπογραφής αναφέρεται εντός των εκδοθέντων πιστοποιητικών όπως περιγράφεται στην παράγραφο 7.1.1.3.

7.1.1.5 Αρχή Έκδοσης

Το πεδίο «Αρχή Έκδοσης» (Issuer Information) περιλαμβάνει:

- Common Name (CN) (προαιρετικό αν υπάρχει OU): Το «κοινό όνομα» της Αρχής Έκδοσης. Πρέπει να είναι μοναδικό στην ΥΔΚ HARICA
- Organizational Unit (OU) (προαιρετικό αν υπάρχει CN): Η Αρχή Έκδοσης. Πρέπει να είναι μοναδικό στην ΥΔΚ HARICA
- Organization (O): Το όνομα του οργανισμού
- Country (C): Χώρα έκδοσης. Η HARICA περιορίζει τη χώρα έκδοσης σε GR

7.1.1.6 Έγκυρο Από

Η χρονική στιγμή (ημερομηνία/ώρα) μετά από την οποία το πιστοποιητικό είναι έγκυρο (μορφή: DD/MM/YYYY HH:MM A.M/P.M GMT)

7.1.1.7 Έγκυρο Έως

Η χρονική στιγμή (ημερομηνία/ώρα) μετά από την οποία το πιστοποιητικό είναι άκυρο (μορφή: DD/MM/YYYY HH:MM A.M/P.M GMT)

7.1.1.8 Πληροφορίες Υποκειμένου

Οι πληροφορίες στο πεδίο «υποκείμενο» (subject) του πιστοποιητικού, προσδιορίζουν το υποκείμενο που σχετίζεται με το δημόσιο κλειδί το οποίο βρίσκεται αποθηκευμένο στο πεδίο «Δημόσιο Κλειδί Υποκειμένου» (subject Public Key). Περιλαμβάνει τα εξής:

- Common Name (CN) (Προαιρετικό για πιστοποιητικά που προορίζονται για SSL): Ένα κοινό όνομα για το υποκείμενο. Αν υπάρχει το συγκεκριμένο πεδίο, για πιστοποιητικά που προορίζονται για SSL χρήση, τότε ΠΡΕΠΕΙ υποχρεωτικά να περιλαμβάνει ένα FQDN που υπάρχει στην επέκταση subjectAltName του πιστοποιητικού.
- Organizational Unit (OU) (Optional): Η οργανωτική μονάδα ή υπο-μονάδα του υποκειμένου ή ειδικά χαρακτηριστικά του υπογράφοντος ανάλογα με τους σκοπούς χρήσης ή των χαρακτηριστικών του πιστοποιητικού
- Organization (O): Ο οργανισμός του υποκειμένου
- Locality (L) (Προαιρετικό): Η πόλη που βρίσκεται το αντικείμενο
- Email (E) (Προαιρετικό για πιστοποιητικά χρήσης SSL): Η διεύθυνση e-mail του υποκειμένου
- Country (C): Χώρα έκδοσης. Η HARICA περιορίζει τη χώρα έκδοσης σε GR
- Subject Public Key Information: Περιέχει το Δημόσιο κλειδί, τον αλγόριθμο δημιουργίας του και το μέγεθός του. Πιστοποιητικά που χρησιμοποιούνται για Code Signing ΠΡΕΠΕΙ να ακολουθούν διαδρομή πιστοποίησης που συνδέεται με Αρχή Πιστοποίησης μεγέθους κλειδιού 4096-bit RSA ή αντίστοιχα ECC (P384).

7.1.2 Επεκτάσεις πιστοποιητικού

Σε κάθε πιστοποιητικό που εκδίδεται θα πρέπει να ακολουθούνται επεκτάσεις σύμφωνα με το πρότυπο πιστοποιητικών X.509 v3. Ακολουθεί λίστα με τις επεκτάσεις που χρησιμοποιούνται στην ΥΔΚ HARICA. Η λίστα αυτή δεν είναι περιοριστική.

- basicConstraints (critical): Ενεργοποιεί τη δυνατότητα το υποκείμενο του πιστοποιητικού να συμπεριφέρεται σαν Αρχή Πιστοποίησης (CA) και θέτει τον μέγιστο αριθμό βημάτων αλυσίδας πιστοποίησης που περιλαμβάνει το συγκεκριμένο πιστοποιητικό. Χρησιμοποιεί την τιμή cA=true για ΑΠ. Παραλείπεται για τελικά πιστοποιητικά.
- keyUsage (critical): Αναφέρονται οι «χρήσεις» του κλειδιού που βρίσκεται στο πιστοποιητικό. Για ΑΠ, έχει τις τιμές *keyCertSign* και *cRLSign*. Για τελικά πιστοποιητικά, έχει τις τιμές *digitalSignature* (αυθεντικοποίηση - authentication), *nonrepudiation* (ψηφιακή υπογραφή και μη αποποίηση ευθύνης αλλά χρησιμοποιείται μόνο σε συνδυασμό με το *digitalSignature)*, *keyEncipherment* (κρυπτογράφηση - encryption).
- certificatePolicies: περιγράφεται στην παράγραφο 7.1.6
- cRLDistributionPoints (not critical): Περιλαμβάνει URL προς τη Λίστα Ανάκλησης Πιστοποιητικών (ΛΑΠ) της εκδότριας ΑΠ
- authorityInformationAccess: Περιλαμβάνει URL προς τον εξυπηρετητή OCSP και μπορεί να περιλαμβάνει URL προς το ψηφιακό πιστοποιητικό της εκδότριας ΑΠ
- Authority Key Identifier: Περιλαμβάνει πληροφορία που προσδιορίζει με μοναδικό τρόπο το Δημόσιο Κλειδί που αντιστοιχεί στο Ιδιωτικό Κλειδί που χρησιμοποιήθηκε για να εκδώσει το συγκεκριμένο πιστοποιητικό. Το πεδίο αυτό περιλαμβάνει την τιμή του "Subject Key Identifier" της εκδότριας ΑΠ
- Subject Key Identifier: Περιλαμβάνει πληροφορία που προσδιορίζει με μοναδικό τρόπο το συγκεκριμένο Δημόσιο Κλειδί του κατόχου του πιστοποιητικού.
- Subject Alternative Name: Περιλαμβάνει πολλαπλές τιμές για e-mail addresses, Microsoft UPNs, DNS ονόματα ή άλλα Uniform Resource Identifiers (URIs)
- Extended Key Usage (EKU): Περιλαμβάνει μια ή περισσότερες χρήσεις για τις οποίες μπορεί να χρησιμοποιηθεί το συγκεκριμένο πιστοποιητικό. Πιθανές τιμές είναι *smartcardlogon, clientAuth, serverAuth, emailProtection, codeSigning, Encrypting File System, TimeStamping, OCSP Signing, IP Sec, Document Signing*. Η συγκεκριμένη λίστα δεν είναι περιοριστική. Επιπλέον, **δεν επιτρέπεται** να υπάρχει ενδιάμεση Αρχή Πιστοποίησης η οποία θα εκδίδει **ταυτόχρονα** πιστοποιητικά με την επέκταση χρήσης serverAuth (1.3.6.1.5.5.7.3.1) και codeSigning (1.3.6.1.5.5.7.3.3).
- Qualified Certificate Statements (qcStatements): Περιλαμβάνει μία ή περισσότερες τιμές οι οποίες ορίζουν τις ιδιότητες του Αναγνωρισμένου Πιστοποιητικού. Απαραίτητη είναι η τιμή id-etsi-qcs-QcCompliance η οποία ορίζει ότι το πιστοποιητικό είναι Αναγνωρισμένο με βάση 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». Επιπρόσθετα, τα πιστοποιητικά κλάσης Α

περιλαμβάνουν και την τιμή id-etsi-qcs-QcSSCD η οποία ορίζει ότι το ιδιωτικό κλειδί δημιουργήθηκε σε hardware κρυπτοσυσκευή.

Περισσότερες πληροφορίες για τα «προφίλ πιστοποιητικών» που χρησιμοποιούνται πιο συχνά, βρίσκονται στο ΠΑΡΑΡΤΗΜΑ Β (Προφίλ Πιστοποιητικών HARICA).

7.1.3 Αναγνωριστικά αντικειμένων αλγορίθμων

Για την υπογραφή των πιστοποιητικών ΠΡΕΠΕΙ να χρησιμοποιείται ο αλγόριθμος SHA1 ή ισχυρότερος. Απαγορεύεται η χρήση του αλγόριθμου MD5 ή άλλων για τους οποίους υπάρχουν αποδείξεις ότι έχουν παραβιαστεί. Όλοι οι αλγόριθμοι που χρησιμοποιούνται στις ΑΠ και στα πιστοποιητικά συνδρομητών, πρέπει να ακολουθούν τις τεχνολογικές εξελίξεις στον τομέα της κρυπτογραφίας προκειμένου να παρέχουν ικανό επίπεδο ασφάλειας για τους σκοπούς χρήσης τους.

7.1.4 Μορφή ονομάτων

Η μορφή των ονομάτων είναι σύμφωνη με τους κανόνες της παραγράφου 3.1.

7.1.5 Περιορισμοί ονομάτων

Η HARICA εφαρμόζει περιορισμούς ονομάτων σε όλες τις ΑΠ σύμφωνα με το RFC 5280. Η συγκεκριμένη επέκταση χαρακτηρίζεται ως « μη κρίσιμη».

Η Κεντρική Αρχή Πιστοποίησης της HARICA περιορίζεται στα domains: .gr, .eu, .edu, .org.

Ειδικά για το domain ".org", σε περίπτωση που κάποιο Ίδρυμα απαιτεί πιστοποιητικό εξυπηρετητή για συγκεκριμένη εκπαιδευτική ή ερευνητική δράση (δεν θα επιτρέπεται έκδοση πιστοποιητικών χρηστών για το συγκεκριμένο domain), η αίτηση θα εξυπηρετηθεί από μία κεντρική ενδιάμεση Αρχή Πιστοποίησης που θα περιορίζεται μόνο στο domain .org. Αυτή η ενδιάμεση Αρχή Πιστοποίησης δεν υφίσταται ακόμα αλλά θα δημιουργηθεί μόλις υπάρξει σχετικό αίτημα.

Οι ενδιάμεσες Αρχές Πιστοποίησης ΠΡΕΠΕΙ να περιορίζονται στο domain του Ιδρύματος που εξυπηρετούν. Για παράδειγμα, η Αρχή Πιστοποίησης του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης θα είναι περιορισμένη στο domain "auth.gr", εφαρμόζοντας το σχετικό χαρακτηριστικό πιστοποιητικού.

7.1.6 Αναγνωριστικό πολιτικής πιστοποίησης

Το αναγνωριστικό της πολιτικής πιστοποίησης, OID (Object Identifier) : 1.3.6.1.4.1.**26513.1.0.3.2**. Ανάλογα με την κλάση κάθε πιστοποιητικού, τα παρακάτω αναγνωρισμένα OIDs μπορούν να προστεθούν στην επέκταση certificatePolicies:

- QCP Public+SSCD (**QCP+**) όπως περιγράφεται στο πρότυπο ETSI TS 101 456: OID **0.4.0.1456.1.1**
- QCP Public (**QCP**) όπως περιγράφεται στο πρότυπο ETSI TS 101 456: OID **0.4.0.1456.1.2**
- **NCP** (Normalized Certificate Policy) όπως περιγράφεται στο πρότυπο ETSI TS 102 042: OID **0.4.0.2042.1.1**

- **NCP+** (Extended Normalized Certificate Policy) όπως περιγράφεται στο πρότυπο ETSI TS 102 042: OID **0.4.0.2042.1.2**

- **DVCP** (Domain Validated Certificate Policy) όπως περιγράφεται στο πρότυπο ETSI TS 102 042: OID **0.4.0.2042.1.6**
- **OVCP** (Organizational Validatation Certificate Policy) όπως περιγράφεται στο πρότυπο ETSI TS 102 042: OID **0.4.0.2042.1.7**

Ειδικά για τις ενδιάμεσες Αρχές Πιστοποίησης, μπορεί να χρησιμοποιηθεί το ειδικό αναγνωριστικό "AnyPolicy" με OID: **2.5.29.32.0** ή στην περίπτωση «ΑΠ εξωτερικής διαχείρισης», το αντίστοιχο OID του CP/CPS.

7.1.7 Χρήση της επέκτασης περιορισμού πολιτικής

Δεν ορίζεται.

7.1.8 Σύνταξη και σημασιολογία του χαρακτηριστικού πολιτικής

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

7.1.9 Επεξεργασία σημασιολογίας για την κρίσιμη επέκταση πολιτικής πιστοποίησης

Δεν ορίζεται.

7.2 Περίγραμμα ΛΑΠ

7.2.1 Βασικά Περιεχόμενα ΛΑΠ

7.2.1.1 Έκδοση

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

7.2.1.2 Αλγόριθμος Υπογραφής

Ο αλγόριθμος που χρησιμοποιείται για υπογραφή ΛΑΠ ΠΡΕΠΕΙ να είναι SHA1 ή ισχυρότερος

7.2.1.3 Εκδότης

Το διακεκριμένο όνομα της Αρχής Πιστοποίησης που έχει υπογράψει και έχει εκδώσει τη ΛΑΠ.

7.2.1.4 Ημερομηνία Έκδοσης

Η ημερομηνία έκδοσης της ΛΑΠ.

7.2.1.5 Επόμενη Ενημέρωση

Η μέγιστη χρονικά ημερομηνία έκδοσης της επόμενης ΛΑΠ.

7.2.1.6 Πιστοποιητικά που ανακλήθηκαν

Λίστα με όλα τα πιστοποιητικά που έχουν ανακληθεί, συμπεριλαμβάνοντας τους σειριακούς αριθμούς και την ημερομηνία και ώρα της ανάκλησης κάθε πιστοποιητικού.

7.2.2 ΛΑΠ και επεκτάσεις των εγγραφών της ΛΑΠ

7.2.2.1 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 ΠΡΕΠΕΙ να συμμορφώνονται με το RFC6960.

7.3.1 Έκδοση

Υποστηρίζεται η έκδοση 1 των προδιαγραφών OCSP όπως αυτή ορίζεται στο RFC6960.

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 Έλεγχος συμμόρφωσης

Η ΥΔΚ HARICA καλύπτει τις προδιαγραφές του ETSI TS 101 456 "*Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates*", του ETSI TS 102 042 "*Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates"* και του ΠΔ 150/2001. Ένας εξωτερικός έλεγχος συμμόρφωσης απαιτείται σε ετήσια βάση για την εξέταση της συμμόρφωσης της ΥΔΚ προς την ΠΠ/ΔΔΠ.

Επίσης, η ΥΔΚ HARICA έχει ενσωματώσει στις τρέχουσες διαδικασίες της (CP/CPS), οδηγίες και διαδικασίας από το κείμενο "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v1.1.9" της σύμπραξης CA/Browser Forum (www.cabforum.org).

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.

Σε περίπτωση που κάποια ΑΠ βρεθεί να μη συμμορφώνεται σύμφωνα με τις προδιαγραφές των προτύπων ETSI TS 101 456 και ETSI TS 102 042, και αποτύχει να συμμορφωθεί σε ικανοποιητικό βαθμό με τους στόχους που θέτουν, θα πρέπει να σταματήσει την έκδοση πιστοποιητικών που φέρουν το τρέχον αναγνωριστικό πολιτικής (policy identifier), μέχρι να αξιολογηθεί ως συμμορφωμένη.

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 ΥΔΚ HARICA δεν αναλαμβάνει ούτε και αποδέχεται οποιαδήποτε οικονομική ευθύνη εκτός αν άλλως ορίζεται ειδικότερα στο παρόν.

9.3 Εμπιστευτικότητα πληροφοριών εμπορικού χαρακτήρα

Η ΥΔΚ της HARICA δεν χειρίζεται πληροφορίες εμπορικού χαρακτήρα.

9.4 Εμπιστευτικότητα πληροφοριών προσωπικού χαρακτήρα

9.4.1 Σχέδιο εμπιστευτικότητας

Δεν ορίζεται.

9.4.2 Πληροφορίες που χαρακτηρίζονται εμπιστευτικές

Πληροφορίες που τηρούνται από τις Αρχές Πιστοποίησης και Καταχώρησης 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 HARICA, των δεδομένων που χαρακτηρίζονται εμπιστευτικά και προσωπικού χαρακτήρα, συμμορφώνεται με τη σχετική νομοθεσία περί προστασίας Προσωπικών Δεδομένων και την Ευρωπαϊκή οδηγία περί προστασίας δεδομένων. Θα εφαρμόζονται κατάλληλα τεχνικά μέτρα για την αποτροπή μη εξουσιοδοτημένης ή παράνομης επεξεργασίας ή εξ' αμελείας απώλεια προσωπικών και ιδιωτικών πληροφοριών.

9.4.5 Διάθεση πληροφοριών σε αρχές επιβολής του νόμου

Οι μη εμπιστευτικές πληροφορίες που τηρεί κάθε Αρχή Πιστοποίησης και Καταχώρησης είναι διαθέσιμες στις αρχές επιβολής του νόμου, 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 διοίκησης του φορέα λειτουργίας της HARICA. Εφόσον πρόκειται για στοιχεία Αρχών Πιστοποίησης και Καταχώρησης που βρίσκονται υπό τη διαχείριση ιδρυμάτων της HARICA, η αίτηση θα πρέπει να γίνεται μέσω της διοίκησης του εκάστοτε ιδρύματος. Σήμερα, φορέας λειτουργίας της HARICA είναι η GUnet A.E. Ιδιωτικά κλειδιά που χρησιμοποιούνται 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 την αναζήτηση οντοτήτων

Οι μη εμπιστευτικές πληροφορίες που τηρεί κάθε ΑΠ και ΑΚ 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 κάθε ΑΠ και ΑΚ 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 HARICA δεν έχει δικαιώματα πνευματικής ιδιοκτησίας στα εκδιδόμενα πιστοποιητικά.

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

9.6 Αντιπροσωπεύσεις και εξουσιοδοτήσεις

Δεν ορίζεται

9.7 Αποκηρύξεις και Εγγυήσεις

Δεν ορίζεται

9.8 Περιορισμοί ευθυνών

Η Υποδομή Δημοσίου Κλειδιού της HARICA δεν ευθύνεται για προβλήματα ή ζημιές που μπορεί να προκύψουν από πλημμελή λειτουργία της που δεν οφείλεται σε υπαιτιότητά της, κατά τα κάτωθι αναφερόμενα, ή από την κακή χρήση των πιστοποιητικών που εκδίδει. Η χρήση της ΥΔΚ HARICA και των υπηρεσιών Πιστοποίησης προϋποθέτει την ανεπιφύλακτη παραδοχή εκ μέρους του χρήστη ότι η ΥΔΚ HARICA δεν ευθύνεται για ζημία ή βλάβη ή διαφυγόν κέρδος ή οποιαδήποτε ειδική, έμμεση, τυχαία, παρεπόμενη ή οικονομική ζημία με όποιο τρόπο και αν προκλήθηκε. Επίσης η ΥΔΚ HARICA δεν αναλαμβάνει, ούτε μπορούν να της αποδοθούν οικονομικές, αστικές ή άλλου είδους ευθύνες, παρά μόνο σε περιπτώσεις που αποδεικνύεται δόλος ή βαριά αμέλειά της στη σφαίρα επιρροής της. Στην περίπτωση δε αυτή, τυχόν ευθύνη της περιορίζεται απέναντι στον χρήστη στη θετική ζημία που αυτός θα υποστεί, αποκλειόμενης οποιασδήποτε άλλης ευθύνης όπως για ενέργειες ή παραλείψεις τρίτων, περιλαμβανομένων και των χρηστών.

9.9 Αποζημιώσεις

Η Υποδομή Δημοσίου Κλειδιού HARICA και οι Πάροχοι Υπηρεσιών Πιστοποίησής της, δεν αναλαμβάνουν ούτε μπορούν να τους αποδοθούν οικονομικές, αστικές ή άλλου είδους ευθύνες, παρά μόνο σε περιπτώσεις που αποδεικνύεται δόλος ή βαριά αμέλειά τους που εντάσσονται στη σφαίρα επιρροής τους. Επίσης, η ΥΔΚ και οι υπηρεσίες που παρέχει, χρησιμοποιούνται αποκλειστικά για Ακαδημαϊκούς και Ερευνητικούς σκοπούς και απαγορεύεται ρητά η εμπορική εκμετάλλευσή της. Συνεπώς, η ΥΔΚ αποποιείται οιασδήποτε ευθύνης και απαλλάσσεται από κάθε τυχόν ζημία, που δε συνδέεται αιτιωδώς με την χρήση των υπηρεσιών πιστοποίησης για τους παραπάνω σκοπούς και δεν οφείλεται σε αποδεδειγμένο δόλο ή βαριά αμέλεια, τυχόν δε ευθύνη κατά τα προαναφερθέντα περιορίζεται απέναντι στον χρήστη στη θετική ζημία που αυτός θα υποστεί, αποκλειόμενης οποιασδήποτε άλλης ευθύνης, όπως για ενέργειες ή παραλείψεις τρίτων περιλαμβανομένων και των χρηστών.

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

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

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 HARICA, οφείλει να ενημερώσει εγγράφως την Κεντρική Υπηρεσία Πιστοποίησης. Ανάλογη επικοινωνία επιβάλλεται σε περιπτώσεις εκδήλωσης ενδιαφέροντος από μονάδες της Ελληνικής Ακαδημαϊκής και Ερευνητικής κοινότητας που επιθυμούν να συμμετέχουν στην ΥΔΚ HARICA.

Έγκυρα μέσα για ενημέρωση τρίτων, σε ό,τι αφορά την παρούσα ΠΠ/ΔΔΠ, είναι το ηλεκτρονικό ταχυδρομείο, απλό ταχυδρομείο και ιστοσελίδες εκτός αν ορίζεται διαφορετικά. Ενημέρωση μέσω τηλεφώνου θα μπορεί να χρησιμοποιηθεί ως εναλλακτική μέθοδος επικοινωνίας, όποτε καταστεί αναγκαίο (πχ σε διαδικασίες ανάκλησης).

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 HARICA, 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: http://www.harica.gr/documents/CPS.php

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 HARICA, θα πρέπει να μεταβληθεί το όνομα και το αναγνωριστικό (OID) της πολιτικής πιστοποίησης το οποίο αναφέρεται στην παράγραφο 1.2.

9.13 Διαδικασίες επίλυσης διαφορών

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

9.14 Ισχύουσα νομοθεσία

Η ΥΔΚ HARICA δημιουργήθηκε για να υπηρετήσει την Ελληνική Ακαδημαϊκή και Ερευνητική κοινότητα. Κάθε πιστοποιητικό που εκδίδεται, αναφέρει ρητά στο πεδίο Certificate Policy Notice, το κείμενο: "*This certificate is subject to Greek laws and our CPS. This Certificate must only be used for administrative, academic, research or educational purposes*" το οποίο μεταφράζεται στο εξής κείμενο: «*Το συγκεκριμένο πιστοποιητικό υπόκειται στην Ελληνική νομοθεσία και την Πολιτική*

Πιστοποίησης/Δήλωση Διαδικασιών Πιστοποίησης όπως εκάστοτε ισχύει. Το πιστοποιητικό αυτό πρέπει να χρησιμοποιείται αποκλειστικά για διοικητική, ακαδημαϊκή, ερευνητική ή εκπαιδευτική χρήση». Η λειτουργία της ΥΔΚ HARICA καθώς και η ερμηνεία της Πολιτικής Πιστοποίησης/Δήλωσης Διαδικασιών Πιστοποίησης διέπεται από το ελληνικό δίκαιο και υπόκεινται στα Ακαδημαϊκά ήθη. 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 θεωρούνται ως «Αναγνωρισμένα Πιστοποιητικά» (“Qualified Certificates”). Η ΥΔΚ HARICA είναι καταχωρημένη στο Μητρώο Έμπιστων Αρχών Πιστοποποίησης της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.).

9.15 Συμμόρφωση με την κείμενη νομοθεσία

Η ΥΔΚ HARICA 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 της HARICA δεσμεύονται:

- √ Να παρέχουν και να συντηρούν την υποδομή που απαιτείται για την σύσταση μιας ιεραρχίας πιστοποίησης για την ελληνική ακαδημαϊκή και ερευνητική κοινότητα, σύμφωνα με τις Πολιτικές Πιστοποίησης 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 Διαδικτύου, όπως HTTP, FTP και LDAP.
- √ Να ανακαλούν πιστοποιητικά όταν συντρέχουν λόγοι ή μετά από αίτημα του υποκειμένου ενός πιστοποιητικού.
- √ Να διατηρούν τις ΛΑΠ πρόσφατα ενημερωμένες.
- √ Να διαχειρίζονται εμπιστευτικά όλες τις προσωπικές πληροφορίες που παρέχονται από τους εγγραφόμενους στις Αρχές Καταχώρησης.
- √ Να ενημερώνουν άμεσα το τεχνικό προσωπικό των υφιστάμενων ΑΠ, για έκθεση, απώλεια, δημοσιοποίηση, τροποποίηση, ή μη εγκεκριμένη χρήση του ιδιωτικού 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 ή δια-πιστοποιούμενη Αρχή Πιστοποίησης εγκεκριμένη από την Υποδομή Δημοσίου Κλειδιού της HARICA 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 (π.χ. φοιτητή, εργαζόμενου, κλπ.).
- √ Να ενημερώνει άμεσα την σχετική Κεντρική Αρχή Πιστοποίησης της HARICA σε περιπτώσεις έκθεσης του ιδιωτικού της κλειδιού.
- √ Να προστατεύει το μυστικό 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.
- √ Σε περίπτωση που κάποιο ίδρυμα –το οποίο συμμετέχει στη HARICA- επιθυμεί να λειτουργήσει αυτόνομη Αρχή Πιστοποίησης, ΠΡΕΠΕΙ να καταθέσει επίσημο πιστοποιητικό ελέγχου συμμόρφωσης σύμφωνα με τις απαιτήσεις της τελευταίας έκδοσης του προτύπου ETSI TS 101 456, ETSI TS 102 042 (ή αντίστοιχου) και της τελευταίας έκδοσης του κειμένου “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” του CA/Browser Forum (www.cabforum.org).

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 αίτησης 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.
- √ Σε περίπτωση που κάποιο ίδρυμα –το οποίο συμμετέχει στη HARICA- επιθυμεί να λειτουργήσει αυτόνομη Αρχή Καταχώρισης, ΠΡΕΠΕΙ να καταθέσει επίσημο πιστοποιητικό ελέγχου συμμόρφωσης σύμφωνα με τις απαιτήσεις της τελευταίας έκδοσης του προτύπου ETSI TS 101 456, ETSI TS 102 042 (ή αντίστοιχου) και της τελευταίας έκδοσης του κειμένου "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" του CA/Browser Forum (www.cabforum.org).

9.16.4 Υποχρεώσεις των εγγραφόμενων

- √ 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 ανάκλησή 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,
- √ τη Δήλωση Διαδικασιών Πιστοποίησης/Πολιτική Πιστοποίησης,
- √ το Μνημόνιο Συνεργασίας και Συναντίληψης,
- √ τα εκδοθέντα πιστοποιητικά και τη ΛΑΠ.

10 ΠΑΡΑΡΤΗΜΑ Α (ΚΕΝΤΡΙΚΕΣ ΑΠ - ROOTS HARICA)

BEGIN HARICA ROOT CA 2011 ===

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=GR, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research Institutions RootCA 2011
        Validity
            Not Before: Dec  6 13:49:52 2011 GMT
            Not After : Dec  1 13:49:52 2031 GMT
        Subject: C=GR, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research Institutions RootCA 2011
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:a9:53:00:e3:2e:a6:f6:8e:fa:60:d8:2d:95:3e:
                    f8:2c:2a:54:4e:cd:b9:84:61:94:58:4f:8f:3d:8b:
                    e4:43:f3:75:89:8d:51:e4:c3:37:d2:8a:88:4d:79:
                    1e:b7:12:dd:43:78:4a:8a:92:e6:d7:48:d5:0f:a4:
                    3a:29:44:35:b8:07:f6:68:1d:55:cd:38:51:f0:8c:
                    24:31:85:af:83:c9:7d:e9:77:af:ed:1a:7b:9d:17:
                    f9:b3:9d:38:50:0f:a6:5a:79:91:80:af:37:ae:a6:
                    d3:31:fb:b5:26:09:9d:3c:5a:ef:51:c5:2b:df:96:
                    5d:eb:32:1e:02:da:70:49:ec:6e:0c:c8:9a:37:8d:
                    f7:f1:36:60:4b:26:2c:82:9e:d0:78:f3:0d:0f:63:
                    a4:51:30:e1:f9:2b:27:12:07:d8:ea:bd:18:62:98:
                    b0:59:37:7d:be:ee:f3:20:51:42:5a:83:ef:93:ba:
                    69:15:f1:62:9d:9f:99:39:82:a1:b7:74:2e:8b:d4:
                    c5:0b:7b:2f:f0:c8:0a:da:3d:79:0a:9a:93:1c:a5:
                    28:72:73:91:43:9a:a7:d1:4d:85:84:b9:a9:74:8f:
                    14:40:c7:dc:de:ac:41:64:6c:b4:19:9b:02:63:6d:
                    24:64:8f:44:b2:25:ea:ce:5d:74:0c:63:32:5c:8d:
                    87:e5
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage:
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                A6:91:42:FD:13:61:4A:23:9E:08:A4:29:E5:D8:13:04:23:EE:41:25
```

X509v3 Name Constraints:
Permitted:
DNS:.gr
DNS:.eu
DNS:.edu
DNS:.org
email:.gr
email:.eu
email:.edu
email:.org

Signature Algorithm: sha1WithRSAEncryption
1f:ef:79:41:e1:7b:6e:3f:b2:8c:86:37:42:4a:4e:1c:37:1e:
8d:66:ba:24:81:c9:4f:12:0f:21:c0:03:97:86:25:6d:5d:d3:
22:29:a8:6c:a2:0d:a9:eb:3d:06:5b:99:3a:c7:cc:c3:9a:34:
7f:ab:0e:c8:4e:1c:e1:fa:e4:dc:cd:0d:be:bf:24:fe:6c:e7:
6b:c2:0d:c8:06:9e:4e:8d:61:28:a6:6a:fd:e5:f6:62:ea:18:
3c:4e:a0:53:9d:b2:3a:9c:eb:a5:9c:91:16:b6:4d:82:e0:0c:
05:48:a9:6c:f5:cc:f8:cb:9d:49:b4:f0:02:a5:fd:70:03:ed:
8a:21:a5:ae:13:86:49:c3:33:73:be:87:3b:74:8b:17:45:26:
4c:16:91:83:fe:67:7d:cd:4d:63:67:fa:f3:03:12:96:78:06:
8d:b1:67:ed:8e:3f:be:9f:4f:02:f5:b3:09:2f:f3:4c:87:df:
2a:cb:95:7c:01:cc:ac:36:7a:bf:a2:73:7a:f7:8f:c1:b5:9a:
a1:14:b2:8f:33:9f:0d:ef:22:dc:66:7b:84:bd:45:17:06:3d:
3c:ca:b9:77:34:8f:ca:ea:cf:3f:31:3e:e3:88:e3:80:49:25:
c8:97:b5:9d:9a:99:4d:b0:3c:f8:4a:00:9b:64:dd:9f:39:4b:
d1:27:d7:b8

=== END HARICA ROOT CA 2011 ===

ΠΑΡΑΡΤΗΜΑ Β (Προφίλ Πιστοποιητικών HARICA)

Friendly Name	Policy IDs	Χρήσεις Κλειδιών (Key Usages)	Άλλες επεκτάσεις
Ενδιάμεση Αρχή Πιστοποίησης HARICA	**2.5.29.32.0 (anyPolicy)** ή το CP/CPS OID σε περίπτωση «ΑΠ εξωτερικής διαχείρισης»	KU: **Certificate Signing, CRL Signing** EKU: None	Καμία
Πιστοποιητικό OCSP	**1.3.6.1.4.1.26513.1.0.3.2** **0.4.0.2042.1.7 (OVCP)**	KU: **Digital Signature** EKU: **OCSP Signing, OCSP No Check**	**OCSP No Check**
Πιστοποιητικό Χρήστη	**1.3.6.1.4.1.26513.1.0.3.2** **0.4.0.2042.1.1 (NCP)**	KU: **Non Repudiation, Digital Signature, Key Encipherment** EKU: **TLS Web Client Authentication, Email Protection,** Encrypting File System (προαιρετικά)	Καμία
«Αναγνωρισμένο Πιστοποιητικό» Χρήστη	**1.3.6.1.4.1.26513.1.0.3.2** **0.4.0.1456.1.2 (QCP)**	KU: **Non Repudiation, Digital Signature, Key Encipherment** EKU: **TLS Web Client Authentication, Email Protection,** Encrypting File System (προαιρετικά)	**QcStatements: id-etsi-qcs-QcCompliance**
«Αναγνωρισμένο Πιστοποιητικό σε ασφαλή διάταξη δημιουργίας υπογραφής» Χρήστη	**1.3.6.1.4.1.26513.1.0.3.2** **0.4.0.1456.1.1 (QCP+)**	KU: **Non Repudiation, Digital Signature, Key Encipherment** EKU: **TLS Web Client Authentication, Email Protection,** Smart Card Logon (προαιρετικά)	**QcStatements: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcSSCD** SmartcardUser (προαιρετικά)

Πιστοποιητικό Χρήστη με δυνατότητα υπογραφής κώδικα	**1.3.6.1.4.1.26513.1.0.3.2 0.4.0.2042.1.1 (NCP)**	KU: **Non Repudiation, Digital Signature, Key Encipherment** EKU: **TLS Web Client Authentication, Email Protection, Code Signing, Lifetime Signing,** Encrypting File System (προαιρετικά)	Καμία
«Αναγνωρισμένο Πιστοποιητικό» Χρήστη με δυνατότητα υπογραφής κώδικα	**1.3.6.1.4.1.26513.1.0.3.2 0.4.0.1456.1.2 (QCP)**	KU: **Non Repudiation, Digital Signature, Key Encipherment** EKU: **TLS Web Client Authentication, Email Protection, Code Signing, Lifetime Signing,** Encrypting File System (προαιρετικά)	**QcStatements: id-etsi-qcs-QcCompliance**
«Αναγνωρισμένο Πιστοποιητικό σε ασφαλή διάταξη δημιουργίας υπογραφής» Χρήστη με δυνατότητα υπογραφής κώδικα	**1.3.6.1.4.1.26513.1.0.3.2 0.4.0.1456.1.1 (QCP+)**	KU: **Non Repudiation, Digital Signature, Key Encipherment** EKU: **TLS Web Client Authentication, Email Protection, Code Signing, Lifetime Signing,** Smart Card Logon (προαιρετικά)	**QcStatements: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcSSCD** SmartcardUser (προαιρετικά)
Πιστοποιητικό Συσκευής	**1.3.6.1.4.1.26513.1.0.3.2 0.4.0.2042.1.7 (OVCP)**	KU: **Digital Signature, Key Encipherment** EKU: **TLS Web Client Authentication, TLS Web Server Authentication**	Καμία
Ενισχυμένο Πιστοποιητικό Συσκευής	**1.3.6.1.4.1.26513.1.0.3.2 0.4.0.2042.1.7 (OVCP)**	KU: **Digital Signature, Key Encipherment** EKU: **TLS Web Client**	Καμία

		Authentication, TLS Web Server Authentication, IPSec End System, IPSec Tunnel, IPSec User	