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 4.3 (18 Φεβρουαρίου 2021)

Πίνακας περιεχομένων

ΑΚΑΔΗΜΑΪΚΟ ΔΙΑΔΙΚΤΥΟ (GUNET) 2

1 ΕΙΣΑΓΩΓΗ 8

1.1 ΕΠΙΣΚΟΠΗΣΗ 8
1.2 ΟΝΟΜΑΣΙΑ ΚΑΙ ΑΝΑΓΝΩΡΙΣΗ ΚΕΙΜΕΝΟΥ 9
1.3 ΚΟΙΝΟΤΗΤΑ ΕΦΑΡΜΟΓΗΣ ΤΗΣ ΥΔΚ 10
1.3.1 Αρχές πιστοποίησης 10
1.3.2 Αρχές Καταχώρισης 11
1.3.3 Συνδρομητές 11
1.3.4 Βασιζόμενα Μέρη (Relying Parties) 12
1.3.5 Άλλοι συμμετέχοντες 12
1.4 ΧΡΗΣΗ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ 13
1.4.1 Κατάλληλες χρήσεις των πιστοποιητικών 13
1.4.2 Απαγορευμένες χρήσεις των πιστοποιητικών 14
1.5 ΔΙΑΧΕΙΡΙΣΗ ΤΗΣ ΠΟΛΙΤΙΚΗΣ 14
1.5.1 Οργανισμός που διαχειρίζεται την πολιτική 14
1.5.2 Πρόσωπο επικοινωνίας 14
1.5.3 Πρόσωπο που κρίνει τη συμμόρφωση στην πολιτική 15
1.5.4 Διαδικασίες έγκρισης ΠΠ/ΔΔΠ 15
1.6 ΟΡΙΣΜΟΙ ΚΑΙ ΑΚΡΩΝΥΜΙΑ 16
1.6.1 Ορισμοί 16
1.6.2 Ακρωνύμια 30

2 ΔΗΜΟΣΙΟΠΟΙΗΣΗ ΚΑΙ ΑΠΟΘΕΤΗΡΙΑ 33

2.1 ΑΠΟΘΕΤΗΡΙΑ 33
2.2 ΔΗΜΟΣΙΟΠΟΙΗΣΗ ΠΛΗΡΟΦΟΡΙΩΝ ΤΗΣ ΑΡΧΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ 33
2.3 ΣΥΧΝΟΤΗΤΑ ΔΗΜΟΣΙΟΠΟΙΗΣΗΣ 33
2.4 ΈΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ ΣΤΟΝ ΙΣΤΟΧΩΡΟ ΑΠΟΘΕΤΗΡΙΟΥ 34

3 ΑΝΑΓΝΩΡΙΣΗ ΚΑΙ ΤΑΥΤΟΠΟΙΗΣΗ 34

3.1 ΟΝΟΜΑΤΟΛΟΓΙΑ 34
3.1.1 Τύποι ονομάτων 34
3.1.1.1 Συμμόρφωση του ονόματος Πιστοποιητικού με Baseline Requirements 34
3.1.2 Υποχρέωση τα ονόματα να έχουν συγκεκριμένο νόημα 34
3.1.3 Δυνατότητα έκδοσης ανώνυμων πιστοποιητικών ή πιστοποιητικών με ψευδώνυμα 34
3.1.4 Κανόνες ερμηνείας διαφόρων τύπων ονομάτων 34
3.1.4.1 Τελικά Πιστοποιητικά για ηλεκτρονικές υπογραφές 36
3.1.4.2 Τελικά Πιστοποιητικά για ηλεκτρονικές σφραγίδες 36
3.1.4.3 Πιστοποιητικά συσκευών για χρήση SSL/TLS 36
3.1.4.4 Πιστοποιητικά Υπογραφής Κώδικα 37
3.1.4.5 Πιστοποιητικά για επαλήθευση ταυτότητας Web Client 37
3.1.5 Μοναδικότητα ονομάτων 38
3.1.6 Διαδικασία επίλυσης διαφορών σχετικά με την κυριότητα ονόματος και ο ρόλος των εμπορικών σημάτων 38
3.2 ΑΡΧΙΚΗ ΕΠΑΛΗΘΕΥΣΗ ΤΑΥΤΟΤΗΤΑΣ 38
3.2.1 Τρόπος απόδειξης κατοχής ιδιωτικού κλειδιού 39
3.2.2 Επαλήθευση ταυτότητας οργανισμού 39
3.2.2.1 Ταυτότητα 40
3.2.2.2 Διακριτικός Τίτλος (DBA) / Επωνυμία / Ρόλοι 40
3.2.2.3 Επαλήθευση της Χώρας 41
3.2.2.4 Επιβεβαίωση Κατοχής ή Ελέγχου Ονόματος Χώρου 41
3.2.2.5 Επαλήθευση ταυτότητας για μία Διεύθυνση IP 49
3.2.2.6 Έλεγχος εγκυρότητας Ονομάτων Χώρου Μπαλαντέρ 51
3.2.2.7 Ακρίβεια Πηγής δεδομένων 52
3.2.2.8 Εγγραφές CAA 53
3.2.3 Επαλήθευση ταυτότητας φυσικού προσώπου 54
3.2.3.1 Πρόσωπο που αιτείται πιστοποιητικό χρήστη 54
3.2.3.2 Πρόσωπο που αιτείται πιστοποιητικό συσκευής 57
3.2.4 Μη επιβεβαιωμένα στοιχεία του συνδρομητή 57

3.2.5 Επιβεβαίωση της Εξουσιοδότησης *57*
3.2.6 Κριτήρια για διαλειτουργικότητα *58*
3.3 ΕΠΑΛΗΘΕΥΣΗ ΤΑΥΤΟΤΗΤΑΣ ΓΙΑ ΕΠΑΝΕΚΔΟΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΜΕ ΝΕΟ ΚΛΕΙΔΙ 58
3.3.1 Επαλήθευση ταυτότητας και εξουσιοδότηση για αίτηση έκδοσης νέου κλειδιού-πιστοποιητικού *58*
3.3.2 Επαλήθευση ταυτότητας και εξουσιοδότηση για αίτηση έκδοσης νέου κλειδιού-πιστοποιητικού μετά από ανάκληση *58*
3.4 ΕΠΑΛΗΘΕΥΣΗ ΤΑΥΤΟΤΗΤΑΣ ΚΑΙ ΕΞΟΥΣΙΟΔΟΤΗΣΗ ΓΙΑ ΑΙΤΗΜΑΤΑ ΑΝΑΚΛΗΣΗΣ 58
3.4.1 Αίτημα ανάκλησης από Εκδούσα Αρχή *59*
3.4.2 Αίτημα ανάκλησης από Συνδρομητή *59*
3.4.3 Αίτημα ανάκλησης από μη-Συνδρομητή *59*

4 ΛΕΙΤΟΥΡΓΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΚΥΚΛΟΥ ΖΩΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ 60

4.1 ΑΙΤΗΣΗ ΓΙΑ ΠΙΣΤΟΠΟΙΗΤΙΚΟ 60
4.1.1 Ποιος δικαιούται να καταθέσει αίτηση για πιστοποιητικό *60*
4.1.2 Διαδικασία ένταξης και ευθύνες *60*
4.1.2.1 Διαδικασία ένταξης για EV Πιστοποιητικά 61
4.2 ΕΠΕΞΕΡΓΑΣΙΑ ΑΙΤΗΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ 61
4.2.1 Διαδικασίες εξακρίβωσης ταυτότητας Συνδρομητή *61*
4.2.2 Έγκριση ή απόρριψη αιτήσεων πιστοποιητικών *62*
4.2.3 Χρόνος επεξεργασίας αιτήσεων πιστοποιητικών *63*
4.2.4 Certificate Authority Authorization (CAA) *63*
4.3 ΈΚΔΟΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ 64
4.3.1 Διαδικασίες Αρχών Πιστοποίησης κατά την έκδοση Πιστοποιητικών *64*
4.3.2 Ενημέρωση του Συνδρομητή από την ΑΠ σχετικά με την έκδοση του πιστοποιητικού *64*
4.4 ΑΠΟΔΟΧΗ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ 64
4.4.1 Δεοντολογία που διέπει τη διαδικασία αποδοχής πιστοποιητικού *64*
4.4.2 Δημοσίευση πιστοποιητικού από την ΑΠ *64*
4.4.3 Ενημέρωση άλλων οντοτήτων για την έκδοση πιστοποιητικού από την ΑΠ *64*
4.5 ΖΕΥΓΟΣ ΚΛΕΙΔΙΩΝ ΚΑΙ ΧΡΗΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ 65
4.5.1 Χρήση ιδιωτικού κλειδιού και πιστοποιητικού Συνδρομητή *65*
4.5.2 Χρήση του δημόσιου κλειδιού και πιστοποιητικού από Βασιζόμενα Μέρη *65*
4.6 ΑΝΑΝΕΩΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ 65
4.6.1 Συνθήκες κατά τις οποίες μπορεί να γίνει ανανέωση πιστοποιητικού *65*
4.6.2 Ποιος μπορεί να καταθέσει αίτημα ανανέωσης πιστοποιητικού *65*
4.6.3 Επεξεργασία αιτημάτων ανανέωσης πιστοποιητικού *65*
4.6.4 Ενημέρωση Συνδρομητή για έκδοση νέου πιστοποιητικού *66*
4.6.5 Δεοντολογία που διέπει την αποδοχή ανανεωμένου πιστοποιητικού *66*
4.6.6 Δημοσίευση του ανανεωμένου πιστοποιητικού από την ΑΠ *66*
4.6.7 Ενημέρωση άλλων οντοτήτων για την έκδοση πιστοποιητικού *66*
4.7 ΑΛΛΑΓΗ ΚΛΕΙΔΙΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ 66
4.7.1 Συνθήκες κατά τις οποίες μπορεί να γίνει αλλαγή κλειδιών *66*
4.7.2 Ποιος μπορεί να αιτηθεί πιστοποίηση νέου δημόσιου κλειδιού *66*
4.7.3 Διαδικασίες για αιτήματα αλλαγής κλειδιών *66*
4.7.4 Ενημέρωση Συνδρομητή για τα πιστοποιητικό στο οποίο πραγματοποιήθηκε αλλαγή κλειδιού *67*
4.7.5 Δεοντολογία που διέπει την διαδικασία αποδοχής πιστοποιητικού στο οποίο έγινε αλλαγή κλειδιού *67*
4.7.6 Δημοσίευση πιστοποιητικών στα οποία έγινε αλλαγή κλειδιού από την ΑΠ *67*
4.7.7 Ενημέρωση από την ΑΠ άλλων οντοτήτων για την έκδοση πιστοποιητικών με νέο κλειδί *67*
4.8 ΜΕΤΑΒΟΛΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ 67
4.8.1 Συνθήκες κατά τις οποίες μπορεί να γίνει μεταβολή πιστοποιητικών *67*
4.8.2 Πώς μπορεί να γίνει αίτημα μεταβολής πιστοποιητικών *67*
4.8.3 Διαδικασίες για αιτήματα μεταβολής πιστοποιητικών *67*
4.8.4 Ενημέρωση Συνδρομητή για το νέο πιστοποιητικά που μεταβλήθηκε *67*

4.8.5 Δεοντολογία που διέπει τη διαδικασία αποδοχή πιστοποιητικών που μεταβλήθηκαν ... 67
4.8.6 Δημοσίευση πιστοποιητικών που μεταβλήθηκαν από την ΑΠ ... 67
4.8.7 Ενημέρωση από την ΑΠ άλλων οντοτήτων για την έκδοση πιστοποιητικών που μεταβλήθηκαν ... 67
4.9 ΑΝΑΣΤΟΛΗ ΚΑΙ ΑΝΑΚΛΗΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ... 68
4.9.1 Συνθήκες για ανάκληση ... 68
4.9.1.1 Λόγοι για την Ανάκληση Πιστοποιητικού Συνδρομητή ... 68
4.9.1.2 Λόγοι για την ανάκληση Πιστοποιητικού Ενδιάμεσης ΑΠ ... 70
4.9.2 Ποιος μπορεί να αιτηθεί ανάκληση ... 71
4.9.3 Διαδικασία αιτήματος ανάκλησης ... 71
4.9.3.1 Ανάκληση του πιστοποιητικού από το Συνδρομητή ... 71
4.9.3.2 Ανάκληση του πιστοποιητικού από άλλη οντότητα ... 71
4.9.3.3 Αίτημα Ανάκλησης από Προμηθευτή Εφαρμογής Λογισμικού ... 72
4.9.3.4 Αίτημα Ανάκλησης από τον Εθνικό Φορέα Εποπτείας eIDAS ... 72
4.9.3.5 Αίτημα Ανάκλησης από Αρμόδια Εθνική Αρχή ... 72
4.9.4 Χρονική περίοδος στην οποία μπορεί να γίνει αίτημα ανάκλησης ... 73
4.9.4.1 Ημερομηνία ανάκλησης για Πιστοποιητικά τύπου «Υπογραφών» ... 73
4.9.5 Χρόνος απόκρισης της ΑΠ για ανακλήσεις πιστοποιητικών ... 74
4.9.6 Μηχανισμοί με τους οποίους Βασιζόμενα Μέρη ελέγχουν την κατάσταση των πιστοποιητικών ... 74
4.9.7 Συχνότητα έκδοσης ΛΑΠ ... 75
4.9.8 Χρόνος δημοσίευσης ΛΑΠ στο Αποθετήριο ... 75
4.9.9 Διαθεσιμότητα υπηρεσίας ελέγχου κατάστασης πιστοποιητικών σε πραγματικό χρόνο (OCSP) ... 75
4.9.10 Απαιτήσεις ελέγχων για ανάκληση σε πραγματικό χρόνο ... 76
4.9.11 Άλλες μορφές ανακοίνωσης ανάκλησης πιστοποιητικών ... 77
4.9.12 Παραλλαγές για την περίπτωση έκθεσης/παραβίασης ιδιωτικού κλειδιού ... 77
4.9.12.1 Δημιουργία και υπογραφή δοκιμαστικού αρχείου ... 77
4.9.12.2 Δημιουργία CSR που περιλαμβάνει ειδικό κείμενο ... 78
4.9.12.3 Δημοσίευση του Ιδιωτικού Κλειδιού ... 78
4.9.13 Περιπτώσεις αναστολής πιστοποιητικών ... 78
4.9.14 Ποιος μπορεί να αιτηθεί αναστολή πιστοποιητικών ... 78
4.9.15 Διαδικασία αιτήματος αναστολής πιστοποιητικού ... 78
4.9.16 Χρονική περίοδος αναστολής πιστοποιητικού ... 78
4.10 ΥΠΗΡΕΣΙΕΣ ΕΛΕΓΧΟΥ ΚΑΤΑΣΤΑΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ... 79
4.10.1 Λειτουργικά χαρακτηριστικά ... 79
4.10.1.1 Υπηρεσία ελέγχου κατάστασης πιστοποιητικών πραγματικού χρόνου OCSP ... 79
4.10.1.2 On-line Αποθετήριο πιστοποιητικών ... 79
4.10.1.3 Χρήση των Λιστών Ανάκλησης Πιστοποιητικών (ΛΑΠ) ... 79
4.10.2 Διαθεσιμότητα υπηρεσίας ελέγχου κατάστασης πιστοποιητικών ... 80
4.10.3 Προαιρετικά χαρακτηριστικά ... 80
4.11 ΛΗΞΗ ΣΥΝΔΡΟΜΗΣ ... 80
4.12 ΜΕΣΕΓΓΥΗΣΗ ΙΔΙΩΤΙΚΟΥ ΚΛΕΙΔΙΟΥ (KEY ESCROW) ΚΑΙ ΕΠΑΝΑΦΟΡΑ ΚΛΕΙΔΙΟΥ 80
4.12.1 Διαδικασίες και πρακτικές συνοδείας ιδιωτικού κλειδιού και επαναφοράς ... 80
4.12.2 Ενθυλάκωση κλειδιού συνόδου (session key) και διαδικασίες και πρακτικές επαναφοράς ... 80

5 ΔΙΟΙΚΗΤΙΚΟΙ, ΤΕΧΝΙΚΟΙ ΚΑΙ ΛΕΙΤΟΥΡΓΙΚΟΙ ΕΛΕΓΧΟΙ ... 81

5.1 ΦΥΣΙΚΗ ΑΣΦΑΛΕΙΑ ΚΑΙ ΕΛΕΓΧΟΣ ΠΡΟΣΒΑΣΗΣ ... 81
5.1.1 Τοποθεσία εγκαταστάσεων ... 81
5.1.2 Φυσική πρόσβαση ... 81
5.1.3 Κλιματισμός και ρύθμιση τροφοδοσίας με ρεύμα ... 81
5.1.4 Έκθεση σε νερό ... 81
5.1.5 Πρόληψη και προστασία από φωτιά ... 81
5.1.6 Αποθηκευτικά μέσα ... 81
5.1.7 Διάθεση απορριμμάτων ... 82
5.1.8 Τήρηση αντιγράφων ασφαλείας εκτός εγκαταστάσεων ... 82
5.2 ΈΛΕΓΧΟΣ ΔΙΑΔΙΚΑΣΙΩΝ ... 82
5.2.1 Έμπιστοι ρόλοι ... 82
5.2.2 Αριθμός ατόμων που απαιτούνται ανά εργασία ... 83

5.2.3 Εξακρίβωση ταυτότητας για κάθε ρόλο *83*
5.2.4 Ρόλοι που απαιτούν διαχωρισμό καθηκόντων *83*
5.3 ΈΛΕΓΧΟΣ ΑΣΦΑΛΕΙΑΣ ΠΡΟΣΩΠΙΚΟΥ 83
5.3.1 Προσόντα, εμπειρία και ειδικές εξουσιοδοτήσεις που πρέπει το προσωπικό να διαθέτει *83*
5.3.2 Διαδικασίες ελέγχου παρελθόντος για το προσωπικό των ΑΠ και το λοιπό προσωπικό *83*
5.3.3 Απαιτήσεις και διαδικασίες εκπαίδευσης *84*
5.3.4 Διαδικασίες και συχνότητα επανεκπαιδεύσεων *84*
5.3.5 Εναλλαγή και σειρά αλλαγής ρόλων *84*
5.3.6 Κυρώσεις που επιβάλλονται για μη εξουσιοδοτημένες ενέργειες *84*
5.3.7 Έλεγχος σε προσωπικό εξωτερικών εργολάβων που εργάζονται εκτός της GUnet και εμπλέκονται με την ΥΔΚ HARICA *84*
5.3.8 Τεκμηρίωση που παρέχεται στο προσωπικό κατά τη διάρκεια εκπαίδευσης *84*
5.4 ΔΙΑΔΙΚΑΣΙΕΣ ΠΑΡΑΚΟΛΟΥΘΗΣΗΣ ΣΥΝΑΛΛΑΓΩΝ ΣΥΜΒΑΝΤΩΝ 85
5.4.1 Τύποι συναλλαγών-συμβάντων που καταγράφονται *85*
5.4.2 Συχνότητα αρχειοθέτησης των επεξεργασμένων συναλλαγών-συμβάντων *86*
5.4.3 Διάστημα τήρησης του αρχείου συναλλαγών-συμβάντων *86*
5.4.4 Προστασία του αρχείου συναλλαγών-συμβάντων *86*
5.4.5 Διαδικασίες αντιγράφων ασφαλείας αρχείων συναλλαγών- συμβάντων *86*
5.4.6 Σύστημα συγκέντρωσης αρχείων συναλλαγών-συμβάντων (εσωτερικό ή εξωτερικό σε σχέση με την οντότητα) *87*
5.4.7 Ενημέρωση του υποκειμένου που προκάλεσε καταγραφή συναλλαγής-συμβάντος, για την ύπαρξη της καταγραφής *87*
5.4.8 Αξιολογήσεις ευπάθειας του συστήματος καταγραφής συναλλαγών-συμβάντων *87*
5.5 ΑΡΧΕΙΟΘΕΤΗΣΗ ΕΓΓΡΑΦΩΝ 87
5.5.1 Τύποι εγγραφών που αρχειοθετούνται *87*
5.5.2 Διάστημα διατήρησης του αρχείου εγγραφών *87*
5.5.3 Προστασία του αρχείου εγγραφών *88*
5.5.3.1 Πρόσβαση 88
5.5.3.2 Προστασία κατά των μεταβολών αρχείων εγγραφών 88
5.5.3.3 Προστασία κατά των διαγραφών αρχείων εγγραφών 88
5.5.3.4 Προστασία κατά της φθοράς των μέσων αποθήκευσης 88
5.5.3.5 Προστασία κατά της μελλοντικής έλλειψης διαθεσιμότητας συσκευών ανάγνωσης των παλαιών μέσων αποθήκευσης 88
5.5.4 Διαδικασίες αντιγράφων ασφαλείας αρχείων εγγραφών *88*
5.5.5 Απαίτηση χρονοσήμανσης αρχείων εγγραφών *88*
5.5.6 Σύστημα συγκέντρωσης αρχείων εγγραφών (εσωτερικό ή εξωτερικό σε σχέση με την οντότητα) *88*
5.5.7 Διαδικασίες για ανάκτηση και επαλήθευση των στοιχείων των αρχείων εγγραφών *89*
5.6 ΡΙΖΙΚΗ ΑΛΛΑΓΗ ΚΛΕΙΔΙΟΥ 89
5.7 ΕΠΑΝΑΦΟΡΑ ΑΠΟ ΠΑΡΑΒΙΑΣΗ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΚΑΤΑΣΤΡΟΦΗ 89
5.7.1 Διαδικασίες και χειρισμός περιστατικών παραβίασης *89*
5.7.2 Διαδικασίες αντιμετώπισης σε περίπτωση παραβίασης-καταστροφής ή υποψίας παραβίασης-καταστροφής υπολογιστικών συστημάτων, λογισμικού, δεδομένων *89*
5.7.3 Διαδικασίες αντιμετώπισης σε περίπτωση απώλειας ιδιωτικών κλειδιών *90*
5.7.4 Δυνατότητες αδιάλειπτης λειτουργίας της υπηρεσίας σε περίπτωση φυσικών ή άλλων καταστροφών *90*
5.8 ΤΕΡΜΑΤΙΣΜΟΣ ΑΡΧΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ Η ΑΡΧΗΣ ΚΑΤΑΧΩΡΗΣΗΣ 91

6 ΈΛΕΓΧΟΙ ΤΕΧΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ 92

6.1 ΔΗΜΙΟΥΡΓΙΑ ΖΕΥΓΟΥΣ ΚΛΕΙΔΙΩΝ ΚΑΙ ΕΓΚΑΤΑΣΤΑΣΗ 92
6.1.1 Δημιουργία ζεύγους κλειδιών *92*
6.1.1.1 Δημιουργία Ζεύγους Κλειδιού για Αρχές Πιστοποίησης και Μονάδες Χρονοσήμανσης 92
6.1.1.2 Δημιουργία Ζεύγους Κλειδιών για Αρχές Καταχώρησης 92
6.1.1.3 Δημιουργία Ζεύγους Κλειδιών Συνδρομητών 92
6.1.2 Παράδοση Ιδιωτικού κλειδιού σε Συνδρομητή *94*
6.1.3 Παράδοση δημόσιου κλειδιού συνδρομητή στην Αρχή Πιστοποίησης *94*

6.1.4 Παράδοση του δημόσιου κλειδιού της Αρχής Πιστοποίησης σε βασιζόμενα μέρη 95
6.1.5 Μεγέθη κλειδιών 95
6.1.6 Παράμετροι δημιουργίας δημοσίων κλειδιών και έλεγχος ποιότητας 95
6.1.7 Σκοποί χρήσης των κλειδιών (ως προς το αντίστοιχο πεδίο του X509) 96
6.2 ΠΡΟΣΤΑΣΙΑ ΙΔΙΩΤΙΚΟΥ ΚΛΕΙΔΙΟΥ ΚΑΙ ΈΛΕΓΧΟΙ ΠΡΟΣΤΑΣΙΑΣ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΣΥΣΚΕΥΩΝ 96
6.2.1 Προδιαγραφές για κρυπτογραφικές μονάδες 96
6.2.2 Έλεγχος ιδιωτικού κλειδιού από πολλά πρόσωπα (N-M) 98
6.2.3 Μεσεγγύηση ιδιωτικού κλειδιού 98
6.2.4 Αντίγραφα ασφαλείας ιδιωτικού κλειδιού 98
6.2.5 Αρχειοθέτηση αντιγράφων ασφαλείας ιδιωτικών κλειδιών 98
6.2.6 Μεταφορά Ιδιωτικού Κλειδιού από και προς ένα κρυπτογραφικό σύστημα 99
6.2.7 Αποθήκευση ιδιωτικού κλειδιού σε κρυπτογραφική συσκευή 99
6.2.8 Μέθοδοι ενεργοποίησης (προς χρήση) ιδιωτικών κλειδιών. 99
6.2.8.1 Ποιος μπορεί να ενεργοποιήσει (χρησιμοποιήσει) ένα ιδιωτικό κλειδί; 99
6.2.8.2 Ενέργειες που πρέπει να εκτελεστούν για την ενεργοποίηση ενός ιδιωτικού κλειδιού 99
6.2.8.3 Από τη στιγμή ενεργοποίησης, για πόσο χρονικό διάστημα είναι το κλειδί «ενεργό»; 100
6.2.9 Μέθοδοι απενεργοποίησης ιδιωτικών κλειδιών. 100
6.2.10 Μέθοδοι καταστροφής ιδιωτικών κλειδιών. 100
6.2.11 Βαθμολόγηση-αξιολόγηση κρυπτογραφικών συστημάτων 101
6.3 ΆΛΛΑ ΘΕΜΑΤΑ ΔΙΑΧΕΙΡΙΣΗΣ ΖΕΥΓΟΥΣ ΚΛΕΙΔΙΩΝ 101
6.3.1 Αρχειοθέτηση των δημόσιων κλειδιών 101
6.3.2 Περίοδοι χρήσης του πιστοποιητικού και του ζεύγους κλειδιού 101
6.4 ΔΕΔΟΜΕΝΑ ΕΝΕΡΓΟΠΟΙΗΣΗΣ 102
6.4.1 Δημιουργία και εγκατάσταση δεδομένων ενεργοποίησης και εγκατάσταση 102
6.4.2 Προστασία δεδομένων ενεργοποίησης 102
6.4.3 Άλλα θέματα δεδομένων ενεργοποίησης 102
6.5 ΈΛΕΓΧΟΙ ΑΣΦΑΛΕΙΑΣ ΥΠΟΛΟΓΙΣΤΩΝ 102
6.5.1 Συγκεκριμένες τεχνικές απαιτήσεις ασφάλειας 102
6.5.2 Βαθμολόγηση ασφάλειας υπολογιστών 102
6.6 ΚΥΚΛΟΣ ΖΩΗΣ ΤΕΧΝΙΚΩΝ ΕΛΕΓΧΩΝ 102
6.6.1 Έλεγχοι ανάπτυξης συστημάτων 102
6.6.2 Έλεγχοι διαχείρισης ασφάλειας 103
6.6.3 Κύκλος ζωής ελέγχων ασφάλειας 103
6.7 ΈΛΕΓΧΟΙ ΑΣΦΑΛΕΙΑΣ ΔΙΚΤΥΟΥ 103
6.8 ΧΡΟΝΟΣΗΜΑΝΣΗ 103
6.8.1 Έκδοση Χρονοσφραγίδων 103
6.8.2 Μονάδα Χρονοσήμανσης 103
6.8.3 Τεκμήρια Χρονοσήμανσης 104
6.8.4 Συγχρονισμός ρολογιού με την ΣΠΩ 104

7 ΠΕΡΙΓΡΑΜΜΑ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ, ΛΑΠ ΚΑΙ OCSP 105

7.1 ΠΕΡΙΓΡΑΜΜΑ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ 105
7.1.1 Έκδοση 105
7.1.2 Επεκτάσεις Πιστοποιητικού 105
7.1.3 Αναγνωριστικά αλγορίθμων 107
7.1.3.1 SubjectPublicKeyInfo 107
7.1.3.2 Signature AlgorithmIdentifier 108
7.1.4 Μορφή πεδίων πιστοποιητικού 110
7.1.4.1 Σειριακός Αριθμός 110
7.1.4.2 Αλγόριθμος Υπογραφής 110
7.1.4.3 Υπογραφή 110
7.1.4.4 Αρχή Έκδοσης 110
7.1.4.5 Έγκυρο Από 112
7.1.4.6 Έγκυρο Έως 112
7.1.4.7 Πληροφορίες στο πεδίο «Υποκείμενο» του Πιστοποιητικού 112
7.1.4.8 Επέκταση Subject Alternative Name 116
7.1.5 Επέκταση name constraints 116
7.1.6 Αναγνωριστικό πολιτικής πιστοποίησης 117

7.1.7 Χρήση της επέκτασης Περιορισμοί πολιτικής (Policy Constraints) 119
7.1.8 Σύνταξη και σημασιολογία του χαρακτηριστικού πολιτικής 119
7.1.9 Επεξεργασία σημασιολογίας για την κρίσιμη επέκταση Πολιτικές Πιστοποίησης (Certificate Policies) 120
7.2 ΠΕΡΙΓΡΑΜΜΑ ΛΑΠ 120
7.2.1 Αριθμός έκδοσης 120
7.2.2 ΛΑΠ και επεκτάσεις εγγραφών ΛΑΠ 120
7.2.2.1 Υπογραφή 120
7.2.2.2 Αλγόριθμος Κατακερματισμού 120
7.2.2.3 Όνομα Εκδότη 120
7.2.2.4 Ημερομηνία Ενημέρωσης 120
7.2.2.5 Επόμενη Ενημέρωση 120
7.2.2.6 Πιστοποιητικά που ανακλήθηκαν 121
7.2.2.7 Αριθμός ΛΑΠ (OID 2.5.29.20) 121
7.2.2.8 Authority Key Identifier 121
7.2.2.9 Ληγμένα Πιστοποιητικά στη ΛΑΠ (OID: 2.5.29.60) 121
7.2.2.10 Κωδικός Αιτιολογίας (OID 2.5.29.21) 122
7.2.3 ΛΑΠ και επεκτάσεις των εγγραφών της ΛΑΠ 122
Δεν ορίζεται. 122
7.3 ΠΕΡΙΓΡΑΜΜΑ OCSP 122
7.3.1 Αριθμός έκδοσης 122
7.3.2 OCSP και επεκτάσεις των εγγραφών 123

8 ΈΛΕΓΧΟΣ ΣΥΜΜΟΡΦΩΣΗΣ ΚΑΙ ΆΛΛΕΣ ΑΞΙΟΛΟΓΗΣΕΙΣ 123

8.1 ΣΥΧΝΟΤΗΤΑ Η ΣΥΝΘΗΚΕΣ ΤΗΣ ΑΞΙΟΛΟΓΗΣΗΣ 123
8.2 ΤΑΥΤΟΤΗΤΑ/ΠΡΟΣΟΝΤΑ ΤΟΥ ΑΞΙΟΛΟΓΗΤΗ 123
8.3 ΣΧΕΣΗ ΤΟΥ ΑΞΙΟΛΟΓΗΤΗ ΜΕ ΤΗΝ ΑΞΙΟΛΟΓΟΥΜΕΝΗ ΟΝΤΟΤΗΤΑ 123
8.4 ΤΑ ΘΕΜΑΤΑ ΠΟΥ ΚΑΛΥΠΤΟΝΤΑΙ ΑΠΟ ΤΗΝ ΑΞΙΟΛΟΓΗΣΗ 123
8.5 ΔΡΑΣΕΙΣ ΠΟΥ ΛΑΜΒΑΝΟΝΤΑΙ ΩΣ ΑΠΟΤΕΛΕΣΜΑ ΤΗΣ ΑΝΕΠΑΡΚΕΙΑΣ 124
8.6 ΑΝΑΚΟΙΝΩΣΗ ΤΩΝ ΑΠΟΤΕΛΕΣΜΑΤΩΝ 124
8.7 ΕΣΩΤΕΡΙΚΟΣ ΈΛΕΓΧΟΣ 124

9 ΕΜΠΟΡΙΚΑ ΚΑΙ ΝΟΜΙΚΑ ΘΕΜΑΤΑ 125

9.1 ΚΟΣΤΗ ΕΓΓΡΑΦΗΣ 125
9.1.1 Κόστος έκδοσης και ανανέωσης πιστοποιητικών 125
9.1.2 Κόστος πρόσβασης σε πιστοποιητικά 125
9.1.3 Κόστος ανάκλησης ή ερώτηση κατάστασης πιστοποιητικών 125
9.1.4 Κόστος άλλων υπηρεσιών 125
9.1.5 Διαδικασίες επιστροφής χρημάτων 125
9.2 ΟΙΚΟΝΟΜΙΚΗ ΕΥΘΥΝΗ 125
9.3 ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΠΛΗΡΟΦΟΡΙΩΝ ΕΜΠΟΡΙΚΟΥ ΧΑΡΑΚΤΗΡΑ 126
9.3.1 Πεδίο εμπιστευτικών πληροφοριών 126
9.3.2 Πληροφορίες που δεν εμπίπτουν στο πεδίο των εμπιστευτικών πληροφοριών 126
9.3.3 Ευθύνες για την προστασία των εμπιστευτικών πληροφοριών 126
9.4 ΕΜΠΙΣΤΕΥΤΙΚΟΤΗΤΑ ΠΛΗΡΟΦΟΡΙΩΝ ΠΡΟΣΩΠΙΚΟΥ ΧΑΡΑΚΤΗΡΑ 126
9.4.1 Σχέδιο εμπιστευτικότητας 126
9.4.2 Πληροφορίες που χαρακτηρίζονται εμπιστευτικές 126
9.4.3 Πληροφορίες που δεν θεωρούνται εμπιστευτικές 127
9.4.4 Ευθύνη για την προστασία δεδομένων προσωπικού χαρακτήρα 127
9.4.5 Ενημέρωση και συγκατάθεση χρήσης εμπιστευτικών δεδομένων 127
9.4.6 Γνωστοποίηση πληροφοριών σε δικαστικές ή δημόσιες αρχές 127
9.4.7 Άλλες περιπτώσεις διάθεσης πληροφοριών 127
9.5 ΔΙΚΑΙΩΜΑΤΑ ΠΝΕΥΜΑΤΙΚΗΣ ΙΔΙΟΚΤΗΣΙΑΣ 128
9.6 ΔΗΛΩΣΕΙΣ ΚΑΙ ΔΙΑΒΕΒΑΙΩΣΕΙΣ 128
9.6.1 Δηλώσεις και Διαβεβαιώσεις ΑΠ 128
9.6.1.1 Αρμοδιότητες από Αρχών Πιστοποίησης Εξωτερικής Λειτουργίας 130
9.6.2 Δηλώσεις και Διαβεβαιώσεις των ΑΚ 130
9.6.3 Δηλώσεις και Διαβεβαιώσεις Συνδρομητή 132
9.6.4 Δηλώσεις και Διαβεβαιώσεις Βασιζόμενων Μερών 133
9.6.5 Δηλώσεις και Διαβεβαιώσεις Λοιπών Συμμετεχόντων 134
9.7 ΑΠΟΠΟΙΗΣΗ ΕΥΘΥΝΗΣ 134

9.8 ΠΕΡΙΟΡΙΣΜΟΙ ΕΥΘΥΝΩΝ 134
9.9 ΑΠΟΖΗΜΙΩΣΗ 136
9.10 ΧΡΟΝΙΚΗ ΠΕΡΙΟΔΟΣ ΙΣΧΥΟΣ ΤΗΣ ΠΑΡΟΥΣΑΣ ΠΠ/ΔΔΠ ΚΑΙ ΛΗΞΗ ΤΗΣ 136
9.10.1 Περίοδος ισχύος και τερματισμός των Συμβάσεων Συνδρομητή 136
9.11 ΑΤΟΜΙΚΕΣ ΕΙΔΟΠΟΙΗΣΕΙΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΑ ΜΕΤΑΞΥ ΤΩΝ ΜΕΡΩΝ 137
9.12 ΤΡΟΠΟΠΟΙΗΣΕΙΣ 137
9.12.1 Διαδικασία τροποποιήσεων 137
9.12.2 Διαδικασίες ενημέρωσης και περίοδος ενημέρωσης 137
9.12.3 Συνθήκες κάτω από τις οποίες το OID θα πρέπει να αλλάζει 137
9.13 ΔΙΑΔΙΚΑΣΙΕΣ ΕΠΙΛΥΣΗΣ ΔΙΑΦΟΡΩΝ 137
9.14 ΙΣΧΥΟΥΣΑ ΝΟΜΟΘΕΣΙΑ 138
9.15 ΣΥΜΜΟΡΦΩΣΗ ΜΕ ΤΗΝ ΚΕΙΜΕΝΗ ΝΟΜΟΘΕΣΙΑ 138
9.16 ΔΙΑΦΟΡΕΣ ΔΙΑΤΑΞΕΙΣ 138
9.16.1 Συνολική Συμφωνία 138
9.16.2 Εκχώρηση 138
9.16.3 Αυτοτέλεια 138
9.16.4 Εκτελεστότητα 139
9.16.5 Ανωτέρα Βία 139
9.17 ΆΛΛΕΣ ΠΑΡΟΧΕΣ 140

10 ΠΑΡΑΡΤΗΜΑ Α (ΚΕΝΤΡΙΚΕΣ ΑΠ - ROOTS HARICA) 141

11 ΠΑΡΑΡΤΗΜΑ Β (ΠΕΡΙΓΡΑΜΜΑΤΑ ΚΟΙΝΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ HARICA) 144

12 ΠΑΡΑΡΤΗΜΑ Γ (ΙΕΡΑΡΧΙΑ ΤΗΣ HARICA) 151

12.1 UNCONSTRAINED SUBORDINATE CAS 151
12.2 TECHNICALLY CONSTRAINED SUBORDINATE CAS 151
12.3 INTERNALLY-OPERATED SUBORDINATE CAS WITH KEYS DESTROYED AND EXTERNALLY AUDITED 153

13 ΠΑΡΑΡΤΗΜΑ Δ "CAA CONTACT TAG" 155

13.1 ΜΕΘΟΔΟΙ CAA 155
13.1.1 Ιδιότητα CAA contactemail 155
13.1.2 Ιδιότητα CAA contactphone 155
13.2 ΜΕΘΟΔΟΣ DNS TXT 156
13.2.1 Email Επαφής Εγγραφής DNS TXT 156
13.2.2 Τηλέφωνο Επαφής Εγγραφής DNS TXT 156

14 ΠΑΡΑΡΤΗΜΑ Ε ΕΚΔΟΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΓΙΑ .ONION DOMAIN NAMES 157

15 ΠΑΡΑΡΤΗΜΑ ΣΤ ΑΝΑΓΝΩΡΙΣΤΙΚΑ ΠΟΛΙΤΙΚΩΝ HARICA 158

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 Ελληνική νομοθεσία 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 • Τροποποιήσεις σε κλάσεις πιστοποιητικών όσον αφορά στα πιστοποιητικά χρηστών • Αλλαγές στα περιγράμματα OCSP
2.3	Μάιος 2011	• Αλλαγή για ελάχιστο μέγεθος κλειδιού σε 2048bits • Αλλαγές σε χρόνους που αφορούν ΛΑΠ και OCSP • 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 αποθετηρίου πιστοποιητικών
2.7	Απρίλιος 2013	• Προσαρμογές στην πολιτική CA/B Forum Baseline Requirements for Publicly-Trusted Certificates v1.1,

		• Αλλαγές σε συχνότητα έκδοσης ΛΑΠ, OCSP πεδία nextUpdate
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 στο Mozilla 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 αν ελέγχονται τα CAA records • Προσαρμογή στις πολιτικές CA/B Forum BR 1.2.5
3.3	Μάρτιος 2016	• Νέες Κορυφαίες Αρχές Πιστοποίησης • Προσαρμογή στο ενημερωμένο Microsoft Root Program Policy • Προσαρμογή στις πολιτικές CA/B Forum BR 1.3.1 • Βελτίωση της συμβατότητας με το RFC3647 • Βελτίωση της συμβατότητας με το RFC5480 (keyUsage bits για Πιστοποιητικά ECDSA)
3.4	Απρίλιος 2016	• Βελτίωση στη χρήση των όρων “ΑΠ” και ”ΠΥΕ”

		• Προσθήκη δυνατότητας cross signing
3.5	Μάιος 2017	• Βελτίωση στη χρήση του όρου «Ενδιάμεση ΑΠ» • Συμμόρφωση στα ETSI EN 319 411-1, EN 319 411-2, EN 319 421 • Διαχωρισμός πιστοποιητικών για χρονοσήμανση από τα πιστοποιητικά SSL, S/MIME, υπογραφής κώδικα • Προσαρμογή στο "Minimum Requirements of the Issuance and Management of Publicly-Trusted Code Signing Certificates" που είναι διαθέσιμο στο https://aka.ms/csbr (Ισχύει από την 1η Φεβρουαρίου του 2017) • Προσαρμογή στις πολιτικές CA/B Forum BRs 1.4.5 • Αλλαγή διάρκειας ισχύος των τελικών Πιστοποιητικών SSL/Χρηστών • Νέο Συμβόλαιο Ασφάλειας επαγγελματικής ευθύνης, ενημέρωση κανόνων αστικής ευθύνης
3.6	Φεβρουάριος 2018	• Προσαρμογή στις πολιτικές CA/B Forum BRs 1.5.6 • Προσθήκη όρων για ελέγχους Πνευματικής Ιδιοκτησίας • Προσθήκη όρων για τη δημιουργία ζεύγους-κλειδιού στα πιστοποιητικά Υπογραφής Κώδικα και για την προστασία του Ιδιωτικού Κλειδιού
3.7	Οκτώβριος 2018	• Τυπογραφικές διορθώσεις • Υποστήριξη για Διαφάνεια Πιστοποιητικών (Certificate Transparency)

		• Άδεια χρήσης των εκδιδόμενων Πιστοποιητικών σε οικονομικές συναλλαγές • Ενημέρωση πληροφοριών που σχετίζονται με την Αναφορά Προβλήματος Πιστοποιητικού • Διατάξεις αναστολής Πιστοποιητικών που χρησιμοποιούνται για «Υπογραφή» • Διευκρινίσεις για περιπτώσεις «Επανέκδοσης» Πιστοποιητικών με νέο κλειδί • Προσαρμογή στο Mozilla Policy 2.6.1
3.8	Μάρτιος 2019	• Τυπογραφικές διορθώσεις • Υποστήριξη για Πιστοποιητικά “Extended Validation (EV)” και “Qualified Website Authentication (QCP-w)”. • Υποστήριξη για Πιστοποιητικά QCP-w-PSD2 • Υποστήριξη διευθύνσεων IP στα πιστοποιητικά SSL/TLS • Υποστήριξη για Πιστοποιητικά Μπαλαντέρ (Wildcard) • Προσαρμογή στις πολιτικές BRs 1.6.4 • Προσαρμογή στις Οδηγίες EV 1.6.8 • Προσαρμογή στις Οδηγίες Υπογραφής Κώδικα EV 1.4 • Εκχώρηση προσαρμοσμένης πολιτικής OIDs για κάθε είδος Πιστοποιητικού
3.9	Οκτώβριος 2019	• Ενημέρωση πρακτικών για EV Code Signing και εξ’ αποστάσεως ΕΔΔΥ • Ενημέρωση Παραρτήματος με Προφίλ Πιστοποιητικών

		• Ενημέρωση ορισμών για Εγκεκριμένες υπογραφές/σφραγίδες • Αλλαγή επωνυμίας GUnet • Ενημέρωση δοκιμαστικών URLs για έλεγχο των User Agents
4.0	Μάρτιος 2020	• Προσθήκη Αριθμών Μητρώου για GUnet • Ενημέρωση Προφίλ Πιστοποιητικών • Προσαρμογή στην πολιτική 2.7 του Mozilla Root CA Program • Προσαρμογή στα BRs 1.6.9 • Προσαρμογή στα EV Guidelines 1.7.1 • Ενημέρωση πληροφορίας ανακλήσεων • Αφαίρεση υποχρέωσης NONCE για OCSP Responders • Μείωση διάρκειας SSL/TLS πιστοποιητικών σε 397 ημέρες από 2020/08/01
4.1	Αύγουστος 2020	• Προσαρμογή στις πολιτικές BRs 1.7.0 • Προσαρμογή στις Οδηγίες EV 1.7.2 • Διευκρινίσεις για τις μεθόδους επαλήθευσης email διευθύνσεων χρησιμοποιώντας επαλήθευση Domain για το μέρος χώρου ονομάτων (domain portion) των email διευθύνσεων • Προσθήκη αναφοράς στον eIDAS ως προς την εξακρίβωση ταυτότητας • Ενημέρωση συχνότητας έκδοσης CRL • Ενημέρωση ενότητας 6.1.1 για απόρριψη κλειδιών που είναι κοινώς γνωστά ότι έχουν εκτεθεί είτε έχουν εκτεθεί. • Προσθήκη αναγνωριστικού πολιτικής για εξ αποστάσεως ΕΔΔΥ

		• Ενημέρωση ενότητας 6.2.1 με αναφορές σε εξ αποστάσεως ΕΔΔΥ και στη λίστα του άρθρου 31 του eIDAS • Δημοσιοποίηση Registration/Incorporating Agencies για EV πιστοποιητικά
4.2	Σεπτέμβριος 2020	• Βελτίωση κειμένου επόμενης ενημέρωσης OCSP • Ειδική απαγόρευση χρήσης πιστοποιητικών για υπηρεσίες τύπου “man-in-the-middle” (παρεμβολής) • Προσαρμογή στις πολιτικές BRs SSL/TLS 1.7.2, ballots SC28, SC35 • Προσαρμογή στις Οδηγίες EV 1.7.3 • Προσαρμογή στις πολιτικές BRs Code Signing 2.0 • Ενημέρωση απαιτήσεων καταγραφής • Ενημέρωση νεότερου RFC για CAA • Ενημέρωση προφίλ OCSP και CRL • Ενημέρωση πρακτικών δημοσιοποίησης τελικών πιστοποιητικών στο Αποθετήριο
4.3	Φεβρουάριος 2021	• Προσαρμογή στις πολιτικές BRs SSL/TLS 1.7.3 • Αφαίρεση δυνατότητας έκδοσης TLS πιστοποιητικών χωρίς OCSP URI στην επέκταση AIA, με υποχρέωση OCSP stapling για συνδρομητές υψηλής επισκεψιμότητας • Περιγραφή καταστροφής MBK ως μέθοδος καταστροφής αντιγράφων ασφαλείας κλειδιών ΑΠ και Πιστοποιητικών Χρονοσήμανσης

		• Οι μέθοδοι συμφωνημένης αλλαγής αρχείων ιστοχώρων δεν θα επιτρέπονται για απόδειξη ελέγχου κατοχής Domain Namespace • Διευκρινίσεις για το τι επιτρέπεται να υπογράφουν Root πιστοποιητικά • Αλλαγή διαστήματος επαναχρησιμοποίησης αποδεικτικών για Domain Name και IP Address σε 397 ημέρες • Τερματισμός χρήσης ΑΔΔΥ για την έκδοση Πιστοποιητικών για Εγκεκριμένες Υπογραφές/Σφραγίδες

1 Εισαγωγή

Η Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure – PKI) των Ελληνικών Ακαδημαϊκών και Ερευνητικών Ιδρυμάτων υποστηρίζεται και διαχειρίζεται από το Ακαδημαϊκό Διαδίκτυο (Greek Universities Network – GUnet) (https://www.gunet.gr), μία αστική μη κερδοσκοπική εταιρία με μέλη όλα τα Πανεπιστήμια της Ελλάδας, με Α.Φ.Μ. **099028220** και αριθμό καταχώρησης **13392/28-9-2000** στα βιβλία εταιριών του Πρωτοδικείου Αθηνών. Η υπηρεσία αυτή της GUnet, η οποία στη συνέχεια θα αναφέρεται ως Αρχή Πιστοποίησης των Ελληνικών Ακαδημαϊκών και Ερευνητικών Ιδρυμάτων (Hellenic Academic & Research Institutions Certification Authority – HARICA), ενεργεί ως Πάροχος Υπηρεσιών Εμπιστοσύνης (Trust Service Provider – TSP) γνωστός και ως «Αρχή Πιστοποίησης» (Certificate Authority), και ως «Εγκεκριμένος» Πάροχος Υπηρεσιών Εμπιστοσύνης (Qualified Trust Service Provider- QTSP). Στο υπόλοιπο κείμενο ΠΠ/ΔΔΠ, οι όροι "TSP" και "QTSP" θεωρούνται ισοδύναμοι.

Η ΥΔΚ HARICA ενεργεί συγκεκριμένα ως "Διαχειριστής Κορυφαίας (Root) ΑΠ". 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 της GUnet. Η διαχείριση της ΥΔΚ HARICA γίνεται από το Κέντρο Ηλεκτρονικής Διακυβέρνησης του Αριστοτελείου Πανεπιστήμιου Θεσσαλονίκης, ένα μέλος της GUnet. Οι φορείς που συμμετέχουν σε αυτή την Υποδομή Δημοσίου Κλειδιού, αποδέχονται ανεπιφύλακτα την παρούσα Δήλωση Διαδικασιών Πιστοποίησης/Πολιτική Πιστοποίησης και συνυπογράφουν το Μνημόνιο Συνεργασίας.

1.1 Επισκόπηση

Η παρούσα Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης περιγράφει το σύνολο κανόνων και διαδικασιών που αφορούν τα ψηφιακά πιστοποιητικά στα πλαίσια της Υποδομής Δημοσίου Κλειδιού HARICA.

Η ΥΔΚ HARICA, ενεργώντας ως «Διαχειριστής Κορυφαίας (Root) ΑΠ» εκδίδει Πιστοποιητικά Ενδιάμεσων Αρχών Πιστοποίησης και Πιστοποιητικά τελικών χρηστών-συσκευών για Φυσικά και Νομικά Πρόσωπα. Εκδίδει επίσης χρονοσημάνσεις και εγκεκριμένες χρονοσημάνσεις. Όλα τα πιστοποιητικά τελικών χρηστών-συσκευών περιέχουν αναφορά στο παρόν κείμενο ή στο κείμενο ΠΠ/ΔΔΠ του Διαχειριστή της Ενδιάμεσης ΑΠ. Οι κάτοχοι πιστοποιητικών καθώς και τα Βασιζόμενα Μέρη θα πρέπει να λαμβάνουν γνώση και να συμμορφώνονται με το παρόν κείμενο.

Η Υποδομή Δημοσίου Κλειδιού HARICA συμμορφώνεται με τα ακόλουθα πρότυπα:

- ETSI EN 319 411-1 v1.2.2. Ο έλεγχος έγινε σύμφωνα με τις τεχνικές διαδικασίες που περιγράφονται στο πρότυπο Electronic Signatures and Infrastructures (ESI); "Policy and security requirements for Trust Service Providers issuing certificates; Part1: General requirements" για συμμόρφωση σε έκδοση πιστοποιητικών που καλύπτουν προδιαγραφές τύπου NCP, NCP+, LCP, DVCP, OVCP, EVCP.
- ETSI EN 319 411-2 v2.2.2. Ο έλεγχος έγινε σύμφωνα με τις τεχνικές διαδικασίες που περιγράφονται στο πρότυπο Electronic Signatures and Infrastructures (ESI); "Policy and security requirements for Trust Service Providers issuing certificates; Part2: Requirements for Trust Service Providers issuing EU qualified certificates

για συμμόρφωση σε έκδοση πιστοποιητικών που καλύπτουν προδιαγραφές τύπου QCP-n, QCP-n-qscd, QCP-l, QCP-l-qscd, QCP-w.

- ETSI EN 319 421 v1.1.1. Ο έλεγχος έγινε σύμφωνα με τις τεχνικές διαδικασίες που περιγράφονται στο πρότυπο Electronic Signatures and Infrastructures (ESI); "Policy and security requirements for Trust Service Providers issuing Time-Stamps" που καλύπτουν προδιαγραφές τύπου BTSP.
- Εγκεκριμένος Πάροχος Υπηρεσιών Εμπιστοσύνης (QTSP), ακολουθώντας τον Ευρωπαϊκό Κανονισμό Νο 910/2014 (e-IDAS) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης σε ηλεκτρονικές συναλλαγές εντός της εσωτερικής αγοράς.

Επιπλέον των παραπάνω προτύπων, η ΥΔΚ HARICA συμμορφώνεται με το πρότυπο ETSI TS 119 495 v1.4.1 που υποστηρίζει Περιγράμματα Εγκεκριμένων Πιστοποιητικών και Απαιτήσεις Πολιτικής του Παρόχου Υπηρεσιών Εμπιστοσύνης (TSP) σύμφωνα με την Οδηγία (EU) 2015/2366 για υπηρεσίες πληρωμής και τον Εξουσιοδοτημένο Κανονισμό (EU) 2018/389 σχετικά με τα Κανονιστικά Τεχνικά Πρότυπα για ισχυρή ταυτοποίηση πελατών και τα κοινά και ασφαλή ανοικτά πρότυπα επικοινωνίας.

1.2 Ονομασία και αναγνώριση κειμένου

Το παρόν κείμενο ονομάζεται «Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης της Υποδομής Δημοσίου Κλειδιού HARICA» και αποτελεί την τεκμηρίωση και το κανονιστικό πλαίσιο λειτουργίας της Υποδομής Δημοσίου Κλειδιού της Αρχής Πιστοποίησης των Ελληνικών Ακαδημαϊκών και Ερευνητικών Ιδρυμάτων (Hellenic Academic & Research Institutions Certification Authority – HARICA). Σε συντομογραφία 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, τρίτα μέρη που εξαρτώνται από τις παρεχόμενες υπηρεσίες, άλλοι οργανισμοί, Ιδρύματα και Αρχές) τους όρους και τις επιχειρησιακές πρακτικές που εφαρμόζονται ή διέπουν την παροχή των Υπηρεσιών Πιστοποίησης της ΥΔΚ HARICA.

Η δομή του παρόντος κειμένου βασίζεται στο πρότυπο IETF RFC 3647. Η ΥΔΚ HARICA συμμορφώνεται με την εκάστοτε έκδοση του κειμένου προδιαγραφών:

- "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates",
- "Guidelines for the Issuance and Management of Extended Validation Certificates",
- "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Code Signing Certificates" and
- "Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates",

που δημοσιεύονται στη διεύθυνση https://www.cabforum.org. Σε περίπτωση οποιασδήποτε διαφοροποίησης μεταξύ αυτού του κειμένου και του κειμένου των πιο πάνω προδιαγραφών, προηγούνται οι πιο πάνω προδιαγραφές έναντι αυτού του

κειμένου. Αυτό σημαίνει ότι η ΥΔΚ HARICA συνεχώς θα παρακολουθεί τις αλλαγές των πολιτικών CA/B Forum και θα προσαρμόζεται σε αυτές πριν την ημερομηνία έναρξης ισχύος τους, ενώ ταυτόχρονα θα ενημερώνει αντίστοιχα αυτό το κείμενο ΠΠ/ΔΔΠ.
Ο παγκόσμια μοναδικός Αριθμός Αναγνώρισης (OID) αυτού του εγγράφου είναι: 1.3.6.1.4.1.**26513.1.0.4.3** όπου:

1.3.6.1.4.1.**26513**	Αριθμός Αναγνώρισης (OID) της ΥΔΚ HARICA, καταχωρημένος από τον οργανισμό IANA (www.iana.org)
1	Υπηρεσία Πιστοποίησης
0	Δήλωση Διαδικασιών Πιστοποίησης
4.3	Πρώτο και δεύτερο ψηφίο του αριθμού έκδοσης (version) της Δήλωσης Διαδικασιών Πιστοποίησης

1.3 Κοινότητα εφαρμογής της ΥΔΚ

Το σύνολο των οντοτήτων, συμπεριλαμβάνοντας Φυσικά Πρόσωπα (συνολικά αναφέρονται στο εξής ως «οντότητες») που χρησιμοποιούν ψηφιακά πιστοποιητικά που εκδίδονται από την Υποδομή Δημοσίου Κλειδιού HARICA απαρτίζουν την κοινότητα που διέπεται από αυτή την Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης.

1.3.1 Αρχές πιστοποίησης

Οι Αρχές Πιστοποίησης είναι οι οντότητες της Υποδομής Δημόσιου Κλειδιού που εκδίδουν και διαχειρίζονται ψηφιακά πιστοποιητικά. Αυτά τα πιστοποιητικά συνδέονται ιεραρχικά με σημείο εκκίνησης ένα Πιστοποιητικό Κορυφαίας (Root) Αρχής Πιστοποίησης (συνήθως δημοσίως έμπιστη) και διαδοχικές Ενδιάμεσες (Subordinate) Αρχές Πιστοποίησης.

Η Ιεραρχία της ΥΔΚ HARICA που ενεργεί ως Πάροχος Υπηρεσιών Εμπιστοσύνης αποτελείται από τις παρακάτω οντότητες:

1. **Κορυφαίες Αρχές Πιστοποίησης**, οι οποίες εκδίδουν αποκλειστικά ψηφιακά πιστοποιητικά για Ενδιάμεσες Αρχές Πιστοποίησης και δεν εκδίδουν πιστοποιητικά τελικών χρηστών/συσκευών. Κατ' εξαίρεση, επιτρέπεται η έκδοση πιστοποιητικών για τους OCSP responders σύμφωνα με την παράγραφο 4.2.2.2 του RFC 6960. Η διάρκεια ισχύος του πιστοποιητικού HaricaRootCA2011 είναι είκοσι (20) χρόνια (θα πρέπει να αποσυρθεί μέχρι το έτος 2030) και της HaricaRootCA2015 και HaricaECCRootCA2015 είναι εικοσιπέντε (25) χρόνια. Τα πιστοποιητικά των Ενδιάμεσων ΑΠ είτε εκδίδονται για Ενδιάμεσες ΑΠ Εξωτερικής Διαχείρισης είτε εκδίδονται για Ενδιάμεσες ΑΠ Εσωτερικής Διαχείρισης.
2. **Ενδιάμεσες ΑΠ Εσωτερικής Διαχείρισης**, οι οποίες είναι υπό τον έλεγχο της ΥΔΚ HARICA που είναι διαχειριστής Κορυφαίας ΑΠ, για λογαριασμό οργανισμών συνεργαζόμενων με την ΥΔΚ HARICA που συμμορφώνονται και υιοθετούν πλήρως την παρούσα Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης. Τα πιστοποιητικά των Ενδιάμεσων ΑΠ έχουν διάρκεια ισχύος από οκτώ (8) έως δεκαπέντε (15) έτη. Σε περίπτωση που μια Ενδιάμεση ΑΠ Εσωτερικής Διαχείρισης ακολουθεί διαφορετική πολιτική και διαδικασίες πιστοποίησης σε σχέση με το παρόν κείμενο, πρέπει να δημιουργηθεί ξεχωριστό κείμενο ΠΠ/ΔΔΠ (με μοναδικό αναγνωριστικό OID).

Οι Ενδιάμεσες ΑΠ Εσωτερικής Διαχείρισης μπορεί να χρησιμοποιούν Πιστοποιητικά ΑΠ με τεχνικούς περιορισμούς ως προς τη χρήση (π.χ. Χρονοσήμανση, Υπογραφή Κώδικα, SSL/TLS, Client-S/MIME) υπό τον έλεγχο της HARICA ως διαχειριστής Κορυφαίας ΑΠ.

3. **Ενδιάμεσες ΑΠ Εξωτερικής Διαχείρισης**, που πρέπει να επιθεωρούνται ή θα πρέπει υποχρεωτικά να έχουν τεχνικούς περιορισμούς σύμφωνα με το RFC 5280 και ως προς τις πολιτικές των προγραμμάτων Microsoft/Mozilla/Apple και να συμμορφώνονται με τον Ευρωπαϊκό Κανονισμό 910/2014 (eIDAS). Στην περίπτωση των Ενδιάμεσων ΑΠ Εξωτερικής Διαχείρισης πρέπει να συμπεριλαμβάνεται το αναγνωριστικό OID της ΠΠ/ΔΔΠ της Ενδιάμεσης ΑΠ στο κατάλληλο πεδίο της επέκτασης του αντίστοιχου Πιστοποιητικού της Ενδιάμεσης ΑΠ που αφορά στην πολιτική.
4. Η ΥΔΚ HARICA επιτρέπεται να εκδώσει πιστοποιητικά δια-πιστοποίησης (cross-certificates) σύμφωνα με την παράγραφο 3.2.6.

Στο ΠΑΡΑΡΤΗΜΑ Γ (Ιεραρχία της ΥΔΚ HARICA) είναι διαθέσιμο ένα διάγραμμα που απεικονίζει την ιεραρχία των ΑΠ την ημέρα δημοσίευσης της παρούσας ΠΠ/ΔΔΠ.

1.3.2 Αρχές Καταχώρισης

Οι Αρχές Καταχώρισης (ΑΚ) είναι οντότητες αρμόδιες για την επαλήθευση της ταυτότητας των Αιτούντων πριν από την έκδοση του πιστοποιητικού. Οι ΑΚ διαβιβάζουν με ασφαλή τρόπο τις αιτήσεις στην αρμόδια ΑΠ. Στην ΥΔΚ HARICA λειτουργεί Κεντρική Αρχή Καταχώρησης που επαληθεύει τις ταυτότητες των Αιτούντων, τη διαχείριση χώρου ονομάτων (domain control) και όλες τις σχετικές διαδικασίες αξιολόγησης κι ελέγχου εγκυρότητας πριν την έκδοση Πιστοποιητικού.

Η ΥΔΚ HARICA μπορεί να αξιοποιεί γραφεία καταχώρισης Συνεργατών για την επαλήθευση της ταυτότητας των Αιτούντων που ανήκουν στον οργανισμό των Συνεργατών κι αιτούνται πιστοποιητικά. Αυτή η μέθοδος ομοιάζει με το μοντέλο “Εταιρική ΑΚ” στο οποίο επαληθεύονται αιτήσεις για πιστοποιητικά από τον ίδιο τον οργανισμό της “Εταιρικής ΑΚ”. Τα συγκεκριμένα πιστοποιητικά πρέπει να είναι στην αρμοδιότητα της Περιοχής Ονόματος Χώρου του Οργανισμού του Συνεργάτη και το αντίστοιχο Πιστοποιητικό της Ενδιάμεσης ΑΠ πρέπει να είναι Τεχνικά Περιορισμένο στον οργανισμό του Συνεργάτη και της Περιοχής Ονόματος Χώρου του σύμφωνα με την παράγραφο 7.1.5.

Η HARICA δεν θα εκχωρεί τη δυνατότητα εξακρίβωσης του “domain portion” μιας διεύθυνσης email καθώς και τις διαδικασίες επαλήθευσης που περιγράφονται στις ενότητες 3.2.2.4 και 3.2.2.5, σε Έμπιστα Τρίτα Μέρη.

Η Κεντρική Αρχή Καταχώρησης επαληθεύει επίσης, οντότητες που σχετίζονται με τις εσωτερικές λειτουργίας της ΥΔΚ HARICA (διαχειριστές ΥΔΚ HARICA και Πιστοποιητικά για χρήση από υποδομές).

1.3.3 Συνδρομητές

Ο όρος Συνδρομητές ΥΔΚ περιγράφεται στην παράγραφο 1.6.1 και είναι οι οντότητες που αιτούνται και αποκτούν ψηφιακό πιστοποιητικό που εκδίδεται από Ενδιάμεση ΑΠ το οποίο συνδέεται με ένα από τα αξιόπιστα Κορυφαία Πιστοποιητικά της αλυσίδας πιστοποιητικών της ΥΔΚ HARICA. Στην περίπτωση Χρονοσφραγίδας, Συνδρομητές

είναι οι οντότητες που συμφωνούν με αυτό το κείμενο ΠΠ/ΔΔΠ και έχουν αποκτήσει Χρονοσήμανση από ΜΧΣ της ΥΔΚ HARICA.

Η εγγραφή ρόλων (π.χ. «Πρύτανης», «Πρόεδρος») ή μη υπαρκτών προσώπων στην Υπηρεσία, εκτός από την περίπτωση των δικτυακών συσκευών, δεν προβλέπεται στο παρόν κείμενο ούτε απαγορεύεται. Η έκδοση «ψηφιακών πιστοποιητικών ρόλων» από μία Ενδιάμεση ΑΠ είναι δυνατή, εφόσον έχει προβλεφθεί και περιγραφεί η σχετική διαδικασία σε ξεχωριστή ΔΔΠ ή εμπεριέχεται σε μελλοντική έκδοση του παρόντος ΠΠ-ΔΔΠ και εφόσον η διαδικασία αυτή δεν συγκρούεται με κάποιον από τους όρους του παρόντος κειμένου.

1.3.4 Βασιζόμενα Μέρη (Relying Parties)

Οι οντότητες που εμπιστεύονται τις παρεχόμενες υπηρεσίες εμπιστοσύνης ή αλλιώς τα «Βασιζόμενα Μέρη» (Relying Parties) μπορεί να είναι οποιοδήποτε φυσικό ή νομικό πρόσωπο το οποίο βασίζεται σε υπηρεσία εμπιστοσύνης και το οποίο χρησιμοποιεί με οποιονδήποτε τρόπο τα τεκμήρια πιστοποίησης (ψηφιακά πιστοποιητικά, ψηφιακές υπογραφές, χρονοσφραγίδες κλπ) και επαφίεται 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 πιστοποιητικών που βρίσκονται στο παρόν κείμενο και τη σχετική πολιτική πιστοποίησης και αφού ελέγξουν και επαληθεύσουν την εγκυρότητα ενός πιστοποιητικού που έχει εκδοθεί από την Υπηρεσία Πιστοποίησης της ΥΔΚ 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 εύλογη πεποίθηση.

Για την επαλήθευση της εγκυρότητας της υπογραφής που δημιουργήθηκε από ένα Πιστοποιητικό, τα Βασιζόμενα Μέρη θα πρέπει να ελέγξουν ότι:

- √ Το Πιστοποιητικό βρισκόταν εντός της περιόδου ισχύος του.
- √ Το πιστοποιητικό συνδέεται σωστά και ιεραρχικά με Πιστοποιητικό Ενδιάμεσης ΑΠ που μεσολαβεί μέχρι ένα από τα δημόσια έμπιστα Κορυφαία Πιστοποιητικά της ΥΔΚ HARICA στην αλυσίδα Πιστοποιητικών.
- √ Δεν είχε ανακληθεί για οποιοδήποτε λόγο όταν πραγματοποιήθηκε η διαδικασία υπογραφής.
- √ 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 ΥΔΚ HARICA.
- √ Ακολουθούνται οι όροι και οι προϋποθέσεις που περιγράφονται στο παρόν κείμενο.

1.3.5 Άλλοι συμμετέχοντες

Οι Συνδρομητές της ΥΔΚ HARICA μπορούν να επιλέξουν να χρησιμοποιούν έναν τρίτο πάροχο εξ αποστάσεως ΕΔΔΥ. Ένας τέτοιος πάροχος πρέπει να είναι ο ίδιος ΕΠΥΕ που έχει πιστοποιηθεί σύμφωνα με τον κανονισμό eIDAS από πιστοποιημένο ελεγκτικό φορέα και πρέπει να έχει συμμορφωθεί με τις απαιτήσεις της ενότητας 8 αυτού του ΠΠ/ΔΔΠ και του Άρθρου 20 του Ευρωπαϊκού Κανονισμού 910/2014 (eIDAS), ή να συνεργάζεται με έναν ΕΠΥΕ. Η ΥΔΚ HARICA θα πρέπει να επαληθεύει

ότι ο τρίτος Πάροχος Υπηρεσιών Εμπιστοσύνης πληροί τις κατάλληλες απαιτήσεις όσον αφορά τις πιστοποιήσεις.

1.4 Χρήση των πιστοποιητικών

1.4.1 Κατάλληλες χρήσεις των πιστοποιητικών

Τα Πιστοποιητικά της ΥΔΚ HARICA μπορούν να χρησιμοποιηθούν για επαλήθευση ταυτότητας, κρυπτογράφηση, έλεγχο πρόσβασης και ψηφιακή υπογραφή, σε όλες τις δικτυακές υπηρεσίες και εφαρμογές στις οποίες το απαιτούμενο επίπεδο ασφάλειας είναι ίδιο ή χαμηλότερο από αυτό της διαδικασίας έκδοσης των πιστοποιητικών.

Ενδεικτικές εφαρμογές στις οποίες μπορούν να χρησιμοποιηθούν τα ψηφιακά πιστοποιητικά που εκδίδονται από την ΥΔΚ HARICA είναι οι εξής (η λίστα δεν είναι περιοριστική):

α) Υπογραφή ενός «ηλεκτρονικού εγγράφου» από ένα φυσικό ή νομικό πρόσωπο με τη χρήση του ψηφιακού πιστοποιητικού του και του αντίστοιχου ιδιωτικού κλειδιού, κατά προτίμηση με τη χρήση μιας «Ασφαλούς Διάταξης Δημιουργίας Υπογραφής» ΑΔΔΥ ή «Εγκεκριμένης Διάταξης Δημιουργίας Υπογραφής/Σφραγίδας» ΕΔΔΥ (π.χ. έξυπνη κάρτα ή κρυπτογραφική συσκευή), 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 μετά, και

3) η δέσμευση του υπογράφοντα ως προς το περιεχόμενο του εγγράφου και η μη αποποίηση ευθύνης της υπογραφής (non-repudiation).

β) Υπογραφή «μηνυμάτων ηλεκτρονικού ταχυδρομείου», για την εξασφάλιση της αυθεντικότητας της διεύθυνσης ηλεκτρονικού ταχυδρομείου του αποστολέα και για όλα τα χαρακτηριστικά που αναφέρονται στο α). Επιπλέον, μπορούν να χρησιμοποιηθούν για την αποστολή «ασφαλών αποδείξεων παραλαβής μηνυμάτων» (μη άρνηση παραλαβής).

γ) Ισχυρή ταυτοποίηση (Strong Authentication) ενός φυσικού προσώπου ή μιας συσκευής κατά την επικοινωνία με άλλες οντότητες, εξασφαλίζοντας επιπλέον χαρακτηριστικά ασφάλειας, ισχυρότερα από αυτά που παρέχει η κλασική μέθοδος πρόσβασης με συνθηματικό (password).

δ) «Κρυπτογράφηση εγγράφων και μηνυμάτων» με τη 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) Πιστοποίηση άλλων Παρόχων Υπηρεσιών Πιστοποίησης είτε πρόκειται για Ενδιάμεσες 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/TLS, IPSec κλπ.

Η ΥΔΚ HARICA επίσης, λειτουργεί ως «Εγκεκριμένη Αρχή Χρονοσήμανσης» παρέχοντας «Εγκεκριμένη» και «Μη-Εγκεκριμένη» Χρονοσήμανση. Αν μια Μονάδα Χρονοσήμανσης εκδίδει Χρονοσήμανση που ισχυρίζεται ότι είναι «Εγκεκριμένη Χρονοσήμανση» σύμφωνα με τον Ευρωπαϊκό Κανονισμό 910/2014 (eIDAS), τότε η

συγκεκριμένη Μονάδα Χρονοσήμανσης δεν επιτρέπεται να εκδίδει «Μη-Εγκεκριμένη» Χρονοσήμανση.

1.4.2 Απαγορευμένες χρήσεις των πιστοποιητικών

Τα πιστοποιητικά δεν μπορούν να χρησιμοποιηθούν σε υπηρεσίες ή συστήματα που σε περίπτωση διακοπής ή αστοχίας εξαιτίας των πιστοποιητικών, οδηγεί σε σημαντική ζημία σε ενσώματα ή άϋλα αγαθά, ή κίνδυνο ζωής ή σε χρήσεις που δεν περιλαμβάνονται σε αυτές της 1ης παραγράφου της ενότητας 1.4.1.

Απαγορεύεται η χρήση TLS Πιστοποιητικών εξυπηρετητών για παρεμβολές τύπου “man-in-the-middle” ή διαχείριση κίνησης χώρου ονομάτων (domain names) ή IP διευθύνσεων όπου ο κάτοχος δεν τα κατέχει νόμιμα ή δεν βρίσκονται υπό τον έλεγχό του. Η συγκεκριμένη χρήση πιστοποιητικών απαγορεύεται ρητά.

1.5 Διαχείριση της πολιτικής

1.5.1 Οργανισμός που διαχειρίζεται την πολιτική

Το παρόν κείμενο ΠΠ/ΔΔΠ 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 (ΕΔΠΠ) HARICA (Policy Management Committee – PMC) που έχει οριστεί από το Διοικητικό Συμβούλιο της GUnet.

ca-admin at 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 at harica.gr
Δημήτρης Ζαχαρόπουλος [dzacharo at harica.gr]
Τηλ: 2310 998483
Fax: 2310 999100

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

Σπύρος Μπόλης [sbol at gunet.gr]
Τηλ: 210 7275611
Fax: 210 7275601

Αρχή Πιστοποίησης HARICA
ΑΚΑΔΗΜΑΪΚΟ ΔΙΑΔΙΚΤΥΟ GUnet
Ε.Κ.Π.Α. - ΚΕΝΤΡΟ ΛΕΙΤΟΥΡΓΙΑΣ & ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΟΥ
ΠΑΝΕΠΙΣΤΗΜΙΟΥΠΟΛΗ 157 84
Τηλ: +30-2310 998483, +30-2310 998435
Fax: +30-2310 999100

Επικοινωνήστε με την ΥΔΚ HARICA για Αναφορές Προβλημάτων Πιστοποιητικού αποστέλλοντας email στη διεύθυνση **"cert-problem-report at harica.gr"**.

Η HARICA παρέχει δυνατότητα απόκρισης 24x7 σε Αναφορές Προβλημάτων Πιστοποιητικού με υψηλή προτεραιότητα λαμβάνοντας μηνύματα στη διεύθυνση **"high-priority-cert-problem-report at harica.gr"**, και όπου χρειάζεται, προωθεί συγκεκριμένα παράπονα/καταγγελίες στις κατάλληλες δημόσιες αρχές και/ή ανακαλεί το Πιστοποιητικό που σχετίζεται με το πρόβλημα. Δείτε επίσης, τις παραγράφους 4.9.3.2 και 4.9.3.3.

1.5.3 Πρόσωπο που κρίνει τη συμμόρφωση στην πολιτική

ca at harica.gr
Δημήτρης Ζαχαρόπουλος [dzacharo at harica.gr]
Τηλ: 2310 998483
Fax: 2310 999100

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

Σπύρος Μπόλης [sbol at gunet.gr]
Τηλ: 210 7275611
Fax: 210 7275601

Διοίκηση Αρχής Πιστοποίησης HARICA
ΑΚΑΔΗΜΑΙΚΟ ΔΙΑΔΙΚΤΥΟ GUnet
Ε.Κ.Π.Α. - ΚΕΝΤΡΟ ΛΕΙΤΟΥΡΓΙΑΣ & ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΟΥ
ΠΑΝΕΠΙΣΤΗΜΙΟΥΠΟΛΗ 157 84
Τηλ: +30-2310 998483, +30-2310 995000
Fax: +30-2310 999100

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 σε δημόσια προσβάσιμο Αποθετήριο.

Σημαντικές αλλαγές της ΠΠ/ΔΔΠ θα ανακοινώνονται στους Συνδρομητές σε εύλογο χρονικό διάστημα, πριν τεθούν σε εφαρμογή.

Η HARICA παρακολουθεί σε τακτική βάση Forums που σχετίζονται με Υπηρεσίες Εμπιστοσύνης όπως το Mozilla dev-security-policy Forum και δημόσια δημοσιευμένα περιστατικά τύπου "ca-compliance" στο https://bugzilla.mozilla.org. Επίσης, η HARICA συμμετέχει ως μέλος με δικαίωμα ψήφου στο CA/Browser Forum (https://cabforum.org) και στην Τεχνική Επιτροπή του ETSI ESI (https://www.etsi.org/committee/esi).

Ακόμα κι αν δεν υπάρχει απαίτηση αλλαγής της ΠΠ/ΔΔΠ, η ΕΔΠΠ θα πραγματοποιεί τουλάχιστον σε ετήσια βάση διαδικασία αναθεώρησης προκειμένου να βελτιώνει την πολιτική και τις διαδικασίες (ευκαιρία για βελτίωση).

1.6 Ορισμοί και ακρωνύμια

1.6.1 Ορισμοί

Προηγμένη Ηλεκτρονική Σφραγίδα: Ηλεκτρονική υπογραφή που πληροί τις προϋποθέσεις του άρθρου 36 του Ευρωπαϊκού Κανονισμού 910/2014.

Προηγμένη Ηλεκτρονική Υπογραφή: Ηλεκτρονική υπογραφή που πληροί σ τις προϋποθέσεις του άρθρου 26 του Ευρωπαϊκού Κανονισμού 910/2014.

Συνδεδεμένη Οντότητα: Μια εταιρεία, συνεταιρισμός, κοινοπραξία ή άλλη οντότητα που ελέγχει, ελέγχεται από, ή τελεί υπό κοινό έλεγχο με μια άλλη οντότητα ή γραφείο αντιπροσώπευσης, τμήμα ή οποιαδήποτε οντότητα που λειτουργεί υπό τον άμεσο έλεγχο ενός Κυβερνητικού Φορέα.

Αιτών: Το φυσικό πρόσωπο ή το Νομικό Πρόσωπο που αιτείται (ή επιδιώκει ανανέωση) ενός Πιστοποιητικού. Μόλις το πιστοποιητικό εκδοθεί, ο αιτών αναφέρεται ως ο Συνδρομητής. Για πιστοποιητικά που έχουν εκδοθεί για συσκευές, ο Αιτών είναι ο φορέας που ελέγχει ή λειτουργεί τη συσκευή που κατονομάζεται στο πιστοποιητικό, ακόμη και αν η συσκευή υποβάλλει την ίδια την αίτηση για πιστοποιητικό.

Εκπρόσωπος Αιτούντος: Ένα φυσικό πρόσωπο ο οποίος ενεργεί για λογαριασμό του Αιτούντος, με νομικώς δεσμευτικό τρόπο, ο οποίος είτε εργάζεται στον Αιτούντα, ή σε συνεργάτη του τελευταίου, ο οποίος είναι νομίμως εξουσιοδοτημένος να εκπροσωπεί τον Αιτούντα:

(i) ο οποίος υπογράφει και υποβάλλει, ή εγκρίνει αίτηση πιστοποιητικού για λογαριασμό του Αιτούντος, ή / και
(ii) ο οποίος υπογράφει και υποβάλλει Σύμβαση Συνδρομητή για λογαριασμό του Αιτούντος, ή / και
(iii) ο οποίος αναγνωρίζει και συμφωνεί με τους Όρους Χρήσης του Πιστοποιητικού εκ μέρους του αιτούντος, όταν ο Αιτών είναι Συνδεδεμένη Οντότητα της ΥΔΚ HARICA.

Προμηθευτής Λογισμικού: Ένας προμηθευτής λογισμικού πλοηγού Διαδικτύου ή άλλου λογισμικού εφαρμογής βασιζόμενου μέρους που εμφανίζει ή χρησιμοποιεί Πιστοποιητικά και εμπιστεύεται Κορυφαία Πιστοποιητικά της HARICA.

Έγγραφο Βεβαίωσης: Έγγραφο που βεβαιώνει ότι οι Πληροφορίες Ταυτότητας του Υποκειμένου είναι ορθές και το οποίο συντάσσεται από δικηγόρο, δημόσια αρχή, ή άλλους αξιόπιστους τρίτους οι οποίοι είθισται να εξακριβώνουν συγκεκριμένες πληροφορίες στις οποίες βασίζονται Τρίτοι.

Περίοδος Ελέγχου: Το χρονικό διάστημα ελέγχου που είναι η περίοδος μεταξύ της πρώτης και της τελευταίας ημέρας που καλύπτει η επιθεώρηση από τους ελεγκτές. Οι κανόνες ελέγχου και οι μέγιστοι περίοδοι ελέγχων περιγράφονται στην παράγραφο 8.1.

Έκθεση Ελέγχου: Έκθεση Συμμόρφωσης από Πιστοποιημένο Ελεγκτικό Φορέα που δηλώνει τη γνώμη του Φορέα για το εάν οι διαδικασίες και οι έλεγχοι μίας οντότητας συμμορφώνονται με τις υποχρεωτικές διατάξεις των προτύπων ελέγχου που απαριθμούνται στην παράγραφο 8.4.

Όνομα Χώρου Εξουσιοδότησης: Το Όνομα Χώρου το οποίο χρησιμοποιείται για εξουσιοδότηση προκειμένου να εκδοθεί πιστοποιητικό για συγκεκριμένο FQDN. Η HARICA μπορεί να χρησιμοποιήσει το FQDN που θα επιστρέψει μια DNS CNAME αναζήτηση ως το FQDN για τους σκοπούς ελέγχου ονόματος χώρου (Domain Validation). Αν το FQDN περιέχει τον χαρακτήρα αστερίσκο (*), τότε η HARICA πρέπει να αφαιρέσει όλους τους αστερίσκους από την αριστερότερη θέση του αιτούμενου FQDN. Η HARICA μπορεί να αφαιρέσει ένα η περισσότερα ονόματα από αριστερά προς τα δεξιά μέχρι να συναντήσει ένα Όνομα Χώρου Βάσης και μπορεί να χρησιμοποιήσει οποιαδήποτε από τις ενδιάμεσες τιμές για τους σκοπούς επαλήθευσης ονόματος χώρου (Domain Validation).

Εξουσιοδοτημένη Θύρα: Μία από τις ακόλουθες θύρες: 80 (http), 443 (https), 25 (smtp), 22 (ssh).

Όνομα Χώρου Βάσης : Το τμήμα ενός αιτούμενου FQDN το οποίο είναι το πρώτο όνομα χώρου στα αριστερά ενός ελεγχόμενου-από-καταχωρητή ή δημόσια-ελεγχόμενου ονόματος χώρου συν το όνομα χώρου του ελεγχόμενου-από-καταχωρητή ή δημόσια-ελεγχόμενου (π.χ. “example.co.uk” ή ”example.com”). Για FQDNs όπου το δεξιότερο όνομα χώρου είναι ένα gTLD το οποίο έχει χαρακτηρισμό “Specification 13” από τον οργανισμό ICANN στο συμφωνητικό του, τότε το gTLD από μόνο του μπορεί να χρησιμοποιηθεί ως Όνομα Χώρου Βάσης.

Πιστοποιητικό Αρχής Πιστοποίησης: Ένα Πιστοποιητικό το οποίο περιέχει το χαρακτηριστικό cA με τιμή “TRUE” στην επέκταση “basic Constraints”.

CAA: Μετάφραση από το RFC 8659: «Η DNS εγγραφή Certification Authority Authorization (CAA) επιτρέπει στον κάτοχο ενός DNS ονόματος να καθορίσει τις Αρχές Πιστοποίησης (ΑΠ) που είναι εξουσιοδοτημένες να εκδίδουν πιστοποιητικά γι’ αυτό το όνομα χώρου. Η δημοσίευση των εγγραφών DNS CAA επιτρέπει σε μία Αρχή Πιστοποίησης να εφαρμόσει συμπληρωματικούς ελέγχους για να μειώσει τον κίνδυνο της ακούσιας έκδοσης πιστοποιητικού».

Ζεύγος Κλειδιού ΑΠ: Ένα Ζεύγος Κλειδιού όπου το Δημόσιο Κλειδί εμφανίζεται ως Subject Public Key Info σε ένα ή περισσότερα Πιστοποιητικά Κορυφαίας ΑΠ ή/και Πιστοποιητικά Ενδιάμεσων ΑΠ.

Πιστοποιητικό: Ένα ηλεκτρονικό έγγραφο που χρησιμοποιεί ψηφιακή υπογραφή για να συνδέσει ένα δημόσιο κλειδί με μία ταυτότητα.

Υπεύθυνος Έγκρισης Πιστοποιητικού: ένα φυσικό πρόσωπο που είναι είτε ο Αιτών, εργάζεται στον Αιτούντα, είτε είναι ένας εξουσιοδοτημένος αντιπρόσωπος που έχει ρητή εξουσιοδότηση να εκπροσωπεί τον Αιτούντα για να i) ενεργεί ως ο Αιτών Πιστοποιητικού και να εξουσιοδοτεί άλλους υπαλλήλους ή τρίτους να ενεργούν ως οι Αιτούντες Πιστοποιητικού και ii) να εγκρίνει Αιτήσεις για Πιστοποιητικά EV που υποβάλλονται από άλλους Αιτούντες Πιστοποιητικών.

Δεδομένα Πιστοποιητικού: Οι αιτήσεις πιστοποιητικού και τα δεδομένα που σχετίζονται με αυτές (είτε προέρχονται από τον αιτούντα είτε από άλλη πηγή) και

βρίσκονται στην κατοχή ή τον έλεγχο της HARICA ή σε μέρη/υπηρεσίες που έχει πρόσβαση η HARICA.

Πιστοποιητικό για Ηλεκτρονική Υπογραφή: Ηλεκτρονικό έγγραφο που χρησιμοποιεί ψηφιακή υπογραφή για να συνδέσει ένα δημόσιο κλειδί με μία ταυτότητα.

Διεργασία Διαχείρισης Πιστοποιητικού: Οι διεργασίες, πρακτικές και διαδικασίες που σχετίζονται με τη χρήση κλειδιών, λογισμικού και υλικού, με τα οποία η HARICA επαληθεύει τα Δεδομένα Πιστοποιητικού, εκδίδει Πιστοποιητικά, διατηρεί ένα Αποθετήριο και ανακαλεί Πιστοποιητικά.

Πολιτική Πιστοποίησης: Ένα σύνολο κανόνων που περιγράφουν τη δυνατότητα χρήσης συγκεκριμένου Πιστοποιητικού σε συγκεκριμένη κοινότητα και / ή υλοποίηση ΥΔΚ με κοινές προδιαγραφές ασφάλειας.

Προφίλ Πιστοποιητικών: Μια σειρά κειμένων ή αρχείων που ρυθμίζουν τις απαιτήσεις για το περιεχόμενο Πιστοποιητικών και επεκτάσεις Πιστοποιητικών σύμφωνα με την ενότητα 7 ή ένα προ-τυποποιημένο αρχείο που χρησιμοποιεί το λογισμικό μιας ΑΠ.

Αναφορά Προβλήματος Πιστοποιητικού: Η αναφορά πιθανής Παραβίασης Κλειδιού, κακής χρήσης Πιστοποιητικού, ή άλλης μορφής απάτης, κακής χρήσης, ή μη αποδεκτής συμπεριφοράς που σχετίζεται με Πιστοποιητικά.

Αιτών Πιστοποιητικού: Ένα φυσικό πρόσωπο που είναι είτε ο Αιτών, είτε εργάζεται στον Αιτούντα, είτε είναι εξουσιοδοτημένος αντιπρόσωπος που έχει ρητή εξουσιοδότηση να εκπροσωπεί τον Αιτούντα, ή τρίτος (όπως ένας Πάροχος Υπηρεσιών Διαδικτύου ή μια εταιρεία που φιλοξενεί υπηρεσίες) που συμπληρώνει και υποβάλλει Αίτηση Πιστοποιητικού EV για λογαριασμό του Αιτούντος.

Λίστα Ανακληθέντων Πιστοποιητικών: Μία λίστα ανακληθέντων Πιστοποιητικών που ανανεώνεται τακτικά, φέρει χρονοσήμανση και η οποία δημιουργείται και υπογράφεται ψηφιακά από την ΑΠ που εξέδωσε τα Πιστοποιητικά.

Αρχή Πιστοποίησης: Ένας οργανισμός που είναι υπεύθυνος για τη δημιουργία, έκδοση, ανάκληση και διαχείριση Πιστοποιητικών.

Δήλωση Διαδικασιών Πιστοποίησης: Ένα από τα πολλά έγγραφα που αποτελούν το πλαίσιο διακυβέρνησης σύμφωνα με το οποίο τα Πιστοποιητικά δημιουργούνται, εκδίδονται, ελέγχονται, και χρησιμοποιούνται.

Συστήματα Πιστοποιητικών: Το σύστημα που χρησιμοποιεί η HARICA ή Εξουσιοδοτημένος Τρίτος Εταίρος για να παρέχει επαλήθευση ταυτότητας, καταχώριση και εγγραφή, έγκριση και έκδοση πιστοποιητικού, κατάσταση εγκυρότητας, υποστήριξη και άλλες υπηρεσίες που σχετίζονται με την ΥΔΚ.

Διαφάνεια Πιστοποιητικών (Certificate Transparency): Ένα σύστημα δημόσιας καταγραφής ψηφιακών πιστοποιητικών αποκλειστικά με δυνατότητα προσθήκης εγγραφών, όπως περιγράφεται στο RFC 6962.

Πιστοποιητικό Υπογραφής Κώδικα: Ψηφιακό πιστοποιητικό που περιέχει την τιμή "code Signing" στην επέκταση "Extended Key Usage" και το εμπιστεύεται ένας Προμηθευτής Λογισμικού για να υπογράφει εκτελέσιμο λογισμικό.

Έλεγχος (νομικής οντότητας): Ο «Έλεγχος» (και οι συνακόλουθες έννοιες, «που ελέγχεται από» και «υπό κοινό έλεγχο με») σημαίνει κατοχή, άμεση ή έμμεση, της εξουσίας να: (1) διευθύνει την διοίκηση, το προσωπικό, τα οικονομικά, ή τα σχέδια της νομικής οντότητας, (2) ελέγχει την εκλογή της πλειοψηφίας των μελών της Διοίκησης ή (3) να ψηφίζει με το ποσοστό των δικαιωμάτων ψήφου που απαιτούνται για την άσκηση ελέγχου σύμφωνα με το εφαρμοστέο δίκαιο που ισχύει για την συγκεκριμένη νομική οντότητα ή το Καταστατικό αυτής, το οποίο σε καμία περίπτωση δεν μπορεί να είναι λιγότερο από 10%.

Συντονισμένη Παγκόσμια Ώρα: Βαθμίδα χρόνου με ακρίβεια δευτερολέπτου όπως ορίζεται στη Σύσταση ITU-R TF.460-6.

Χώρα: Είτε ένα μέλος του Οργανισμού Ηνωμένων Εθνών (ΟΗΕ) είτε μία γεωγραφική περιοχή που αναγνωρίζεται ως κυρίαρχο έθνος από δύο τουλάχιστον κράτη-μέλη του ΟΗΕ.

Πιστοποιητικό Δια-πιστοποίησης: Ένα πιστοποιητικό που χρησιμοποιείται για τη δημιουργία μιας σχέσης εμπιστοσύνης μεταξύ δύο Κορυφαίων ΑΠ.

CSPRNG: Γεννήτρια τυχαίων αριθμών που χρησιμοποιείται σε κρυπτογραφικό σύστημα.

Εξουσιοδοτημένος Τρίτος Εταίρος: Ένα φυσικό ή νομικό πρόσωπο που ταυτίζεται με τη HARICA και έχει εξουσιοδοτηθεί από αυτήν να βοηθά στη Διεργασία Διαχείρισης Πιστοποιητικού αποδίδοντας ή εκπληρώνοντας μία ή περισσότερες από τις απαιτήσεις της HARICA που βρίσκονται σε αυτό το κείμενο.

Email Επαφής DNS CAA: Η διεύθυνση email όπως ορίζεται στην ενότητα 13.1.1.

Τηλέφωνο Επαφής DNS CAA: Η διεύθυνση email όπως ορίζεται στην ενότητα 13.1.2.

Email Επαφής Εγγραφής DNS TXT : Η διεύθυνση email όπως ορίζεται στην ενότητα 13.2.1.

Τηλέφωνο Επαφής Εγγραφής DNS TXT: Ο αριθμός τηλεφώνου όπως ορίζεται στην ενότητα 13.2.2

Έγγραφο Ονόματος Χώρου Εξουσιοδότησης: Έγγραφα που παρέχονται από, ή η τεκμηρίωση της επικοινωνίας της HARICA με, έναν Καταχωρητή Ονόματος Χώρου (Registrar), έναν Καταχωρίζων Ονόματος Χώρου (Registrant) ή με το πρόσωπο ή οντότητα που αναφέρεται στο WHOIS ως ο Καταχωρίζων Ονόματος Χώρου (συμπεριλαμβανομένης οποιασδήποτε υπηρεσίας ιδιωτικής, ανώνυμης, ή εγγραφής μέσω Τρίτου) η οποία βεβαιώνει την δικαιοδοσία του Αιτούντος να ζητήσει ένα Πιστοποιητικό για μια συγκεκριμένη Περιοχή Ονόματος Χώρου.

Επαφή Ονόματος Χώρου (Domain Contact): Τα στοιχεία επικοινωνίας του Καταχωρίζοντα Ονόματος Χώρου, τεχνικού ή διοικητικού εκπροσώπου (ή τα ισοδύναμα σημεία επαφής όταν το Όνομα Χώρου βρίσκεται σε ιεραρχία ccTLD) όπως καταγράφονται στην εγγραφή WHOIS του Ονόματος Χώρου Βάσης ή σε εγγραφή SOA του DNS, ή όπως αποκτήθηκαν από την άμεση επικοινωνία με τον Καταχωρητή Ονομάτων Χώρου.

Όνομα Χώρου (Domain Name): Το όνομα που έχει ανατεθεί σε έναν κόμβο στο σύστημα ονομάτων χώρου (DNS).

Περιοχή Ονόματος Χώρου (Domain Namespace): Το σύνολο όλων των πιθανών Ονομάτων Χώρου που υπάγονται σε ένα μοναδικό κόμβο του Συστήματος Ονομάτων Χώρου (DNS).

Καταχωρίζων Ονόματος Χώρου (Domain Name Registrant): Μερικές φορές αναφέρεται ως "ιδιοκτήτης" του Ονόματος Χώρου, αλλά πιο ορθά το πρόσωπο(-α) ή η οντότητα (-ες) που έχει καταχωρηθεί σε έναν Καταχωρητή Ονομάτων Χώρου, ότι έχει το δικαίωμα να ελέγχει πώς ένα όνομα χώρου χρησιμοποιείται, όπως το φυσικό ή νομικό πρόσωπο που αναφέρεται ως ο "Καταχωρίζων" από το WHOIS ή τον Καταχωρητή Ονόματος Χώρου.

Καταχωρητής Ονόματος Χώρου (Domain Name Registrar): Ένα πρόσωπο ή οντότητα η οποία καταχωρεί τα Ονόματα Χώρου υπό την αιγίδα , ή σε συμφωνία με: (i) τον οργανισμό Internet Corporation for Assigned Names and Numbers (ICANN), (ii) μια εθνική Ονοματολογική αρχή / μητρώο, ή (iii) ένα Κέντρο Δικτύων (συμπεριλαμβανομένων των συνδεδεμένων οντοτήτων τους, εργολάβων, αντιπροσώπων, διαδόχων ή εκχωρητών).

Εγγραφή EBA PSD2: Η εγγραφή των ιδρυμάτων πληρωμών και των ιδρυμάτων ηλεκτρονικού χρήματος που αναπτύσσει, διαχειρίζεται και συντηρεί η ΕΑΤ (EBA) βάσει του άρθρου 15 της Οδηγίας της Ευρωπαϊκής Ένωσης (EU) 2015/2366.

EV Πιστοποιητικό Οργανισμού (Enterprise EV Certificate): Ένα EV Πιστοποιητικό όπου μία Εταιρική ΑΚ (Enterprise RA) εξουσιοδοτεί την HARICA να εκδώσει σε τρίτο και υψηλότερο επίπεδο χώρου ονομάτων. Τα EV Πιστοποιητικά Οργανισμών SSL/TLS μπορούν να εκδοθούν μόνο σε τρίτο ή υψηλότερο επίπεδο χώρου ονομάτων.

EV Εταιρική Αρχή Καταχώρησης: Ένας υπάλληλος ή ένας αντιπρόσωπος ενός οργανισμού που δεν συνεργάζεται με την ΥΔΚ HARICA και εξουσιοδοτεί την ΥΔΚ HARICA να εκδίδει EV Πιστοποιητικά.

Εταιρική Αρχή Καταχώρισης: Ένας υπάλληλος ή αντιπρόσωπος ενός οργανισμού που δεν ανήκει στην HARICA και εγκρίνει την έκδοση Πιστοποιητικών για τον εν λόγω οργανισμό.

EV Πιστοποιητικό: Ένα πιστοποιητικό που περιέχει πληροφορίες για το Υποκείμενο που έχουν προσδιοριστεί και οι οποίες έχουν επιβεβαιωθεί σύμφωνα με τα EV Guidelines του CA/B Forum. Υπάρχουν EV Πιστοποιητικά για SSL/TLS και για Υπογραφή Κώδικα. Και οι δύο τύποι πιστοποιητικών ακολουθούν τις ίδιες πρακτικές

ελέγχου εγκυρότητας Πληροφοριών του Υποκειμένου που σχετίζονται με την Ταυτότητα του Αιτούντα.

Ανανέωση EV Πιστοποιητικού: Η διαδικασία με την οποία ένας Αιτών που έχει ένα έγκυρο EV Πιστοποιητικό από την ΥΔΚ HARICA που δεν έχει λήξει και δεν έχει ανακληθεί, υποβάλλει αίτηση για έκδοση νέου Πιστοποιητικού EV που συμπεριλαμβάνει το ίδιο όνομα οργανισμού και Όνομα Χώρου όπως και το τρέχον EV πιστοποιητικό, μία νέα ημερομηνία ισχύος "“valid to” άλλη από την ημερομηνία λήξης του τρέχοντος Πιστοποιητικού EV και η αίτηση γίνεται πριν τη λήξη του τρέχοντος Πιστοποιητικού EV του Αιτούντα.

Αίτηση EV Πιστοποιητικού: Μία αίτηση από έναν Αιτούντα που ζητά EV Πιστοποιητικό, του οποίου το έγκυρο αίτημα εξουσιοδοτείται από τον Αιτούντα και υπογράφεται από τον Αντιπρόσωπο του Αιτούντος.

Οδηγίες για EV Πιστοποιητικά Υπογραφής Κώδικα: Το έγγραφο “Οδηγίες για Έκδοση και Διαχείριση Πιστοποιητικών Υπογραφής Κώδικα”, που δημοσιεύεται και συντηρείται από τη σύμπραξη CA/B Forum.

Οδηγίες EV: Το έγγραφο “Οδηγίες για Έκδοση και Διαχείριση Πιστοποιητικών Εκτεταμένου Ελέγχου Εγκυρότητας”, που δημοσιεύεται από τη σύμπραξη CA/B Forum. Αυτό το έγγραφο κυρίως εστιάζει σε Πιστοποιητικά SSL/TLS αλλά κάποιες από τις απαιτήσεις αναφέρονται σε Οδηγίες για Πιστοποιητικά Υπογραφής Κώδικα EV και Ευρωπαϊκά Πρότυπα ETSI (π.χ. ETSI EN 319 411-1).

Διεργασίες EV: Τα κλειδιά, το λογισμικό, οι διεργασίες και διαδικασίες με τις οποίες η ΥΔΚ HARICA επαληθεύει Δεδομένα Πιστοποιητικού, εκδίδει Πιστοποιητικά EV, συντηρεί μία Αποθήκη Πιστοποιητικών EV και ανακαλεί αυτά.

Ημερομηνία λήξης: Η ημερομηνία “Not After” που υπάρχει σε ένα Πιστοποιητικό που καθορίζει το τέλος της περιόδου ισχύος του .

Ενδιάμεση ΑΠ Εξωτερικής Διαχείρισης: Ένας τρίτος Διαχειριστής Ενδιάμεσης ΑΠ, που δεν είναι Συνεργάτης με την HARICA, και έχει στην κατοχή του ή ελέγχει ένα Ιδιωτικό Κλειδί Ενδιάμεσης ΑΠ που έχει εκδοθεί από την HARICA.

Πλήρως Πιστοποιημένο Όνομα Χώρου (FQDN): Ένα Όνομα Χώρου που περιλαμβάνει τις ετικέτες όλων των ανώτερων κόμβων στο Σύστημα Ονομάτων Χώρου Διαδικτύου.

Κρατική Υπηρεσία: Στην περίπτωση Ιδιωτικού Οργανισμού, ως Κρατική Υπηρεσία νοείται η κρατική υπηρεσία της δικαιοδοσίας σύστασης, υπό τον έλεγχο της οποίας συνεστήθη ως νομική οντότητα ο Ιδιωτικός Οργανισμός (π.χ., η κρατική υπηρεσία που εξέδωσε το Πιστοποιητικό Ίδρυσης). Στην περίπτωση Επιχειρήσεων, νοείται η κρατική υπηρεσία της δικαιοδοσίας λειτουργίας, η οποία καταχωρεί σε σχετικά μητρώα τις επιχειρήσεις. Στην περίπτωση Κρατικού Φορέα, η οντότητα η οποία εκδίδει νόμους, κανονισμούς ή διατάγματα για τη νομική υπόσταση του Κρατικού Φορέα.

Κρατικός Φορέας: Ένα νομικός φορέας υπό τον έλεγχο του Δημοσίου, υπηρεσίας, τμήματος, υπουργείου, παραρτήματος ή παρόμοιας μονάδας διακυβέρνησης μιας

χώρας, ή διοικητική μονάδα μέσα στη χώρα (όπως δήμος, γεωγραφικό διαμέρισμα, πόλη, επαρχία κλπ.).

Αίτηση Πιστοποιητικού Υψηλού Κινδύνου: Αίτηση που η HARICA σηματοδοτεί ότι χρήζει επιπλέον ελέγχους με βάση τα εσωτερικά κριτήρια και τις βάσεις δεδομένων που τηρούνται από την HARICA, που μπορεί να περιλαμβάνει ονόματα με μεγάλη πιθανότητα για χρήση σε ηλεκτρονικό «ψάρεμα» (phishing) ή άλλους τρόπους δόλιας χρήσης, ονόματα που περιέχονται σε Πιστοποιητικά που έχουν απορριφθεί στο παρελθόν ή ανακληθέντα πιστοποιητικά, ονόματα τα οποία βρίσκονται στη λίστα ηλεκτρονικού «ψαρέματος» Miller Smiles ή στη λίστα ασφαλούς περιήγησης της Google ή ονόματα που η HARICA αναγνωρίζει με βάση τα δικά της κριτήρια μείωσης του κινδύνου.

Περιοχή Προβλήματος Υψηλού Κινδύνου (HRRC): Μία γεωγραφική περιοχή όπου ο αριθμός Πιστοποιητικών Υπογραφής Κώδικα που ανιχνεύθηκαν με υπογεγραμμένο Ύποπτο Κώδικα ξεπερνά το 5% του συνολικού αριθμού των Πιστοποιητικών Υπογραφής Κώδικα που ανιχνεύθηκαν να προέρχονται ή να σχετίζονται με την ίδια γεωγραφική περιοχή. Αυτή η πληροφορία παρέχεται στο Παράρτημα Δ του εγγράφου “Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates”.

Υπηρεσία Σύστασης: Στην περίπτωση Ιδιωτικού Οργανισμού, η κρατική υπηρεσία δικαιοδσίας σύστασης υπό τον έλεγχο της οποίας καταχωρείται η νομική υπόσταση του Ιδιωτικού Οργανισμού (π.χ. η κρατική υπηρεσία που εκδίδει πιστοποιητικά ίδρυσης ή σύστασης). Στην περίπτωση Κρατικών Φορέων, ο φορέας που εκδίδει νόμους, κανονισμούς ή διατάγματα για τη νομική υπόσταση Κρατικών Φορέων.

Ενδιάμεση ΑΠ Εσωτερικής Διαχείρισης: Μια Ενδιάμεση ΑΠ, την οποία διαχειρίζεται η HARICA ή Συνεργάτης της, και κατέχει ή ελέγχει ένα Ιδιωτικό Κλειδί που συνδέεται με Πιστοποιητικό της.

Εσωτερικό Όνομα: Σειρά από χαρακτήρες (όχι μια διεύθυνση IP) στο πεδίο Common Name ή στο πεδίο Subject Alternative Name ενός Πιστοποιητικού που δεν μπορεί να επαληθευτεί ως παγκοσμίως μοναδικό στο πλαίσιο του δημόσιου DNS κατά τη στιγμή της έκδοσης του Πιστοποιητικού, διότι δεν τελειώνει με ένα TLD Χώρου το οποίο έχει καταχωρηθεί στο Μητρώο Κεντρικών Ζώνων (Root Zone Database) του οργανισμού IANA.

Διεύθυνση IP: Μία ετικέτα σε κωδικοποίηση 32-bit ή 128-bit που αποδόθηκε σε μία συσκευή που χρησιμοποιεί για την επικοινωνία της το Πρωτόκολλο Internet (Internet Protocol).

Επαφή Διεύθυνσης IP: Το πρόσωπο(α) ή φορέας(είς) που καταχωρήθηκαν στην Αρχή Καταχώρησης Διευθύνσεων IP με την ιδιότητα να ασκεί τον έλεγχο στον τρόπο χρήσης μίας ή περισσότερων Διευθύνσεων IP.

Αρχή Καταχώρησης Διεύθυνσης IP: Ο Οργανισμός Απόδοσης Διευθύνσεων Internet (IANA) ή ένα Τοπικό Μητρώο Internet (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

Εκδούσα ΑΠ: Σε συνδυασμό με ένα συγκεκριμένο Πιστοποιητικό, αποτελεί την ΑΠ που εξέδωσε το πιστοποιητικό αυτό. Αυτή θα μπορούσε να είναι είτε μία Κορυφαία ΑΠ είτε μία Ενδιάμεση ΑΠ.

Δικαιοδοσία Σύστασης: Στην περίπτωση Ιδιωτικού Οργανισμού, η χώρα και (κατά περίπτωση) ο δήμος ή το γεωγραφικό διαμέρισμα ή η τοποθεσία σύστασης της νομικής υπόστασης του οργανισμού με υποβολή σε ή πράξη μίας αρμόδιας κρατικής υπηρεσίας ή φορέα (π.χ. όπου συστάθηκε). Στην περίπτωση ενός Κρατικού Φορέα, η χώρα και (κατά περίπτωση) το δήμο ή το γεωγραφικό διαμέρισμα που η νομική υπόσταση του Φορέα συνεστήθη βάσει νόμου.

Δικαιοδοσία Καταχώρισης: Στην περίπτωση Επιχείρησης, πρόκειται για τον δήμο, το γεωγραφικό διαμέρισμα ή την τοποθεσία όπου έχει καταχωρισθεί σε σχετικό μητρώο η έναρξη δραστηριότητας της επιχείρησης με βάση δήλωση που έγινε από τον Αρμόδιο Διευθύνοντα την επιχείρηση.

Παραβίαση Κλειδιού: Ένα ιδιωτικό κλειδί θεωρείται πως έχει εκτεθεί αν έχει αποκαλυφθεί σε ένα μη εξουσιοδοτημένο άτομο ή ένα μη εξουσιοδοτημένο άτομο είχε πρόσβαση σε αυτό.

Σενάριο Δημιουργίας Κλειδιού: Ένα τεκμηριωμένο σχέδιο διαδικασιών για τη δημιουργία ενός Ζεύγους Κλειδιών ΑΠ.

Ζεύγος Κλειδιών: Το Ιδιωτικό Κλειδί και το αντίστοιχο Δημόσιο Κλειδί.

Συμβολαιογραφική Αρχή: Πρόσωπο με νομική κατάρτιση, του οποίου οι υπηρεσίες βάσει της ισχύουσας νομοθεσίας δεν περιλαμβάνουν μόνο την απόδοση εξουσιοδότησης για την εξακρίβωση της γνησιότητας της υπογραφής ενός εγγράφου, αλλά και την ευθύνη για την ορθότητα και το περιεχόμενο του εγγράφου. Αποδίδεται και με την έννοια «Συμβολαιογράφος Αστικού Δικαίου».

Νομικό Πρόσωπο: Μία ένωση, εταιρία, συνεταιρισμός, ιδιοκτησία, όμιλος, οντότητα της κυβέρνησης, ή άλλος φορέας με νομική υπόσταση στο νομικό σύστημα μιας χώρας.

Νομική Υπόσταση: Ένας Ιδιωτικός Οργανισμός, ένας Κρατικός Φορέας ή μία Επιχείρηση έχει Νομική Υπόσταση αν έχει συσταθεί με έγκυρο τρόπο και δεν έχει, με κάποιον τρόπο, πάψει, διαλυθεί ή εγκαταλειφθεί.

Νομικός: Πρόσωπο που είναι είτε δικηγόρος είτε Συμβολαιογραφική Αρχή (βλ. παραπάνω) και αρμόδιος να διατυπώσει γνώμη σχετικά με πραγματικούς ισχυρισμούς του Αιτούντα.

Lifetime Signing OID: Μία προαιρετική επέκταση χρήσης κλειδιού OID (1.3.6.1.4.1.311.10.3.13) που χρησιμοποιείται από το Microsoft Authenticode με σκοπό να περιορίσει τη διάρκεια ζωής της υπογραφής κώδικα στην ημερομηνία λήξης του πιστοποιητικού υπογραφής κώδικα.

Συμβολαιογράφος: Ένα πρόσωπο που έχει την εντολή σύμφωνα με την ισχύουσα νομοθεσία, μεταξύ άλλων, να πιστοποιεί την εκτελεστότητα και την γνησιότητα υπογραφής ενός εγγράφου.

Όχι-EV Πιστοποιητικό Υπογραφής Κώδικα: Όρος που χρησιμοποιείται για να σηματοδοτήσει απαιτήσεις που εφαρμόζονται σε Πιστοποιητικά Υπογραφής κώδικα τα οποία δεν χρειάζεται να καλύπτουν τις απαιτήσεις των EV Πιστοποιητικών Υπογραφής Κώδικα.

Αναγνωριστικό Αντικειμένου: Ένα μοναδικό αλφαριθμητικό ή αριθμητικό αναγνωριστικό που καταχωρίζεται στο πλαίσιο του Διεθνούς Οργανισμού Τυποποίησης σύμφωνα με το ισχύον πρότυπο και αφορά ένα συγκεκριμένο αντικείμενο ή κατηγορία αντικειμένων.

OCSP Responder: Ένας online διακομιστής που λειτουργεί υπό την εποπτεία της ΑΠ και συνδέεται με το Αποθετήριο της, για την επεξεργασία των αιτημάτων εύρεσης κατάστασης των Πιστοποιητικών και την παροχή απαντήσεων μέσω του Online Πρωτοκόλλου Κατάστασης Πιστοποιητικών. Δείτε επίσης, "Online Πρωτόκολλο Κατάστασης Πιστοποιητικών".

Online Πρωτόκολλο Κατάστασης Πιστοποιητικών (Online Certificate Status Protocol): Ένα online πρωτόκολλο ελέγχου Πιστοποιητικών που επιτρέπει σε μία εφαρμογή λογισμικού Βασιζόμενου Μέρους να προσδιορίσει την κατάσταση ενός έμπιστου Πιστοποιητικού. Δείτε επίσης: "OCSP Responder".

Μητρική Εταιρεία: Εταιρεία που ελέγχει μια θυγατρική εταιρεία.

Έλεγχος Διείσδυσης: Διαδικασία που αναγνωρίζει και προσπαθεί να εκμεταλλευτεί κενά ασφάλειας και ευπάθειες στο Σύστημα Πιστοποιητικών με χρήση γνωστών μεθόδων επίθεσης, συμπεριλαμβανομένου του συνδυασμού διαφορετικών τύπων ευπαθειών, με σκοπό την αποδόμηση διαφορετικών επιπέδων άμυνας και την αναφορά εκτεθειμένων ευπαθειών και αδυναμιών του συστήματος.

Τοποθεσία επιχείρησης: Η τοποθεσία οποιασδήποτε εγκατάστασης (όπως εργοστάσιο, κατάστημα λιανικής πώλησης, αποθήκη κ.λπ.) από όπου εκτελείται η επιχείρηση του Αιτούντος.

Precertificate: Όπως περιγράφεται στο RFC 6962, αποτελείται από το πιστοποιητικό που πρόκειται να εκδοθεί με την προσθήκη μιας κρίσιμης επέκτασης "poison extension" (OID 1.3.6.1.4.1.11129.2.4.3), στην οποία η τιμή extnValue OCTET STRING περιέχει ASN.1 NULL data (0x05 0x00)) στο τελικό υποψήφιο-προς-υπογραφή πιστοποιητικό (TBSCertificate). Αυτή η επέκταση προστίθεται για να εξασφαλίσει ότι το Precertificate δεν μπορεί να χρησιμοποιηθεί ως έγκυρο πιστοποιητικό από έναν τυπικό client X.509v3.

Ιδιωτικός Οργανισμός: Μία μη κρατική νομική οντότητα (είτε ανήκει σε ιδιωτικά συμφέροντα ή είναι δημοσίως εισηγμένη) η οποία απέκτησε νομική υπόσταση με την υποβολή (ή την πράξη) Υπηρεσίας Σύστασης ή ισοδύναμο βάσει της Δικαιοδοσίας Σύστασης

Ιδιωτικό Κλειδί: Το κλειδί από ένα Ζεύγος Κλειδιών το οποίο φυλάσσεται από τον κάτοχο του Ζεύγους κλειδιών, και χρησιμοποιείται για να δημιουργήσει Ψηφιακές Υπογραφές και/ή για να αποκρυπτογραφήσει ηλεκτρονικά αρχεία που έχουν κρυπτογραφηθεί με το αντίστοιχο Δημόσιο Κλειδί.

Δημόσιο Κλειδί: Το κλειδί ενός Ζεύγους Κλειδιών που μπορεί να δημοσιοποιηθεί από τον κάτοχο του αντίστοιχου Ιδιωτικού Κλειδιού και χρησιμοποιείται από ένα Βασιζόμενο Μέρος για την επαλήθευση Ψηφιακών Υπογραφών που δημιουργήθηκαν με το αντίστοιχο Ιδιωτικό Κλειδί του κατόχου ή/και για την κρυπτογράφηση μηνυμάτων τα οποία μπορούν να αποκρυπτογραφηθούν μόνο με το αντίστοιχο Ιδιωτικό Κλειδί.

Υποδομή Δημοσίου Κλειδιού: Ένα σύνολο από υλικό, λογισμικό, ανθρώπους, διαδικασίες, κανόνες, πολιτικές και υποχρεώσεις, που χρησιμοποιούνται για την αξιόπιστη δημιουργία, έκδοση, διαχείριση, και χρήση των Πιστοποιητικών και κλειδιών που βασίζονται στην Κρυπτογραφία Δημοσίου Κλειδιού.

Δημοσίως Έμπιστο Πιστοποιητικό: Ένα Πιστοποιητικό που θεωρείται έμπιστο λόγω του γεγονότος ότι το αντίστοιχο πιστοποιητικό της Κορυφαίας ΑΠ λειτουργεί ως σημείο εμπιστοσύνης (trust anchor) σε ευρέως διαδεδομένο λογισμικό ή εφαρμογές.

Οργανισμός Καταχώρισης: Μία Κρατική Υπηρεσία που καταχωρεί πληροφορίες επιχειρήσεων σχετικές με την έναρξη επιχειρηματικών δραστηριοτήτων ή το δικαίωμα άσκησης επαγγελματικής δραστηριότητας βάσει άδειας, καταστατικού ή άλλης πιστοποίησης. Ένας Οργανισμός Καταχώρισης μπορεί να είναι, αλλά δεν περιορίζεται σε αυτό: (i) ένα Υπουργείο με αρμοδιότητα στις Επιχειρήσεις ή μία Γραμματεία Υπουργείου, (ii) μία υπηρεσία αδειοδότησης, όπως ένα Υπουργείο Ασφαλίσεων, ή (iii) μία υπηρεσία μισθώσεων, όπως ένα κρατικό γραφείο ή τμήμα δημοσιονομικού κανονισμού, τραπεζικού ή χρηματοοικονομικού, ή ένας ομοσπονδιακός οργανισμός όπως το Γραφείο του Επιθεωρητή του Νομισματικού Ταμείου ή της Υπηρεσίας Επιτήρησης Υγείας.

Αρχή Καταχώρησης: Οποιοδήποτε Νομικό Πρόσωπο που είναι υπεύθυνο για την ταυτοποίηση και επαλήθευση των υποκειμένων των Πιστοποιητικών, αλλά δεν είναι η Αρχή Πιστοποίησης και κατά συνέπεια δεν υπογράφει ούτε εκδίδει Πιστοποιητικά. Η «ΑΚ» μπορεί να βοηθήσει στη διαδικασία αίτησης πιστοποιητικού ή στη διαδικασία ανάκλησης ή και στις δύο. Όταν ο όρος «ΑΚ» χρησιμοποιείται σαν επιθετικός προσδιορισμός για να περιγράψει ένα ρόλο ή μια διεργασία, δεν σημαίνει απαραίτητα ότι πρόκειται για ξεχωριστή οντότητα αλλά μπορεί να είναι μέρος της Αρχής Πιστοποίησης.

Αριθμός Μητρώου: Ένας μοναδικός αριθμός που έχει αποδοθεί σε έναν Ιδιωτικό Οργανισμό από την Υπηρεσία Σύστασης στην Δικαιοδοσία Σύστασης του οργανισμού.

Διαπιστευμένος Ελεγκτής: Ένα φυσικό ή νομικό πρόσωπο που πληροί τις απαιτήσεις της παραγράφου 8.2 (Ελεγκτής Προσόντων).

Εγκεκριμένο Πιστοποιητικό για ηλεκτρονική σφραγίδα: Πιστοποιητικό για Εγκεκριμένη Ηλεκτρονική Σφραγίδα που εκδόθηκε από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης και πληροί τις απαιτήσεις του Παραρτήματος ΙΙΙ του Ευρωπαϊκού Κανονισμού Νο 910/2014.

Εγκεκριμένο Πιστοποιητικό για ηλεκτρονική υπογραφή: Πιστοποιητικό για Εγκεκριμένες Ηλεκτρονικές Υπογραφές που εκδόθηκε από εγκεκριμένο πάροχο

υπηρεσιών εμπιστοσύνης και ικανοποιεί τις απαιτήσεις του Παραρτήματος Ι του Ευρωπαϊκού Κανονισμού Νο 910/2014.

Εγκεκριμένη Ηλεκτρονική Σφραγίδα: Προηγμένη Ηλεκτρονική Σφραγίδα που δημιουργήθηκε από Εγκεκριμένη Διάταξη Δημιουργίας Ηλεκτρονικής Σφραγίδας και βασίζεται σε Εγκεκριμένο Πιστοποιητικό για ηλεκτρονικές σφραγίδες, όπως ορίζεται στον Ευρωπαϊκό Κανονισμό Νο 910/2014.

Εγκεκριμένη Ηλεκτρονική Υπογραφή: Προηγμένη Ηλεκτρονική Υπογραφή που δημιουργήθηκε από Εγκεκριμένη Διάταξη Δημιουργίας Ηλεκτρονικής Υπογραφής και βασίζεται σε Εγκεκριμένο Πιστοποιητικό για ηλεκτρονικές υπογραφές, όπως ορίζεται στον Ευρωπαϊκό Κανονισμό Νο 910/2014.

Εγκεκριμένη Διάταξη Δημιουργίας Ηλεκτρονικής Υπογραφής/Σφραγίδας: Γνωστή επίσης ως ΕΔΔΥ. Μια συσκευή δημιουργίας ηλεκτρονικής υπογραφής που ικανοποιεί τις απαιτήσεις του Παραρτήματος ΙΙ του Ευρωπαϊκού Κανονισμού Νο 910/2014.

Εγκεκριμένη Ηλεκτρονική Χρονοσφραγίδα: Ηλεκτρονική Χρονοσφραγίδα που ικανοποιεί τις απαιτήσεις του Άρθρου 42 του Ευρωπαϊκού Κανονισμού Νο 910/2014.

Τυχαία Τιμή: Μια τιμή που ορίζεται από τη HARICA στον Αιτούντα που περιλαμβάνει τουλάχιστον 112 bit εντροπίας.

Κατοχυρωμένο Όνομα Χώρου: Όνομα Χώρου που έχει καταχωρηθεί σε ένα Καταχωρητή Ονομάτων Χώρου.

Αρχή Καταχώρησης (ΑΚ): Κάθε οντότητα που είναι υπεύθυνη για την αναγνώριση και ταυτοποίηση των Υποκειμένων των Πιστοποιητικών, αλλά δεν είναι μια ΑΠ, και ως εκ τούτου δεν υπογράφει ή εκδίδει Πιστοποιητικά. Μια ΑΚ μπορεί να συμβάλλει στη διαδικασία αίτησης Πιστοποιητικού ή στη διαδικασία ανάκλησης ή και στις δύο. Όταν ο όρος "ΑΚ" χρησιμοποιείται ως επίθετο για να περιγράψει έναν ρόλο ή λειτουργία, αυτό δεν σημαίνει κατ' ανάγκη μια ξεχωριστή μονάδα, αλλά μπορεί να αποτελεί μέρος της ΑΠ.

Αξιόπιστη Πηγή Δεδομένων: Ένα έγγραφο αναγνώρισης ή πηγή δεδομένων που χρησιμοποιείται για την επαλήθευση Πληροφοριών Ταυτότητας του Υποκειμένου που αναγνωρίζεται μεταξύ των εμπορικών επιχειρήσεων και των κυβερνήσεων ως αξιόπιστο, και το οποίο δημιουργήθηκε από τρίτους για σκοπό διαφορετικό από την απόκτηση Πιστοποιητικού του Αιτούντος.

Αξιόπιστη Μέθοδος Επικοινωνίας: Μέθοδος επικοινωνίας, όπως μια ταχυδρομική διεύθυνση/διεύθυνση αποστολής ταχυμεταφορών, ένας αριθμός τηλεφώνου ή μία διεύθυνση ηλεκτρονικού ταχυδρομείου, που επαληθεύτηκε χρησιμοποιώντας μια πηγή δεδομένων η οποία δεν προέρχεται από τον Αιτούντα ή Εκπρόσωπο του Αιτούντος.

Βασιζόμενο Μέρος (Relying Party): Κάθε φυσικό ή νομικό πρόσωπο που στηρίζεται σε ένα έγκυρο Πιστοποιητικό. Ένας Προμηθευτής Λογισμικού Εφαρμογών δεν θεωρείται Βασιζόμενο Μέρος όταν το λογισμικό που διανέμεται από τον εν λόγω προμηθευτή απλώς εμφανίζει πληροφορίες σχετικά με το Πιστοποιητικό.

Αποθετήριο: Μια online βάση δεδομένων που περιέχει δημοσίως διαθέσιμα έγγραφα της ΥΔΚ (Πολιτικές Πιστοποίησης και Δηλώσεις Διαδικασιών Πιστοποίησης) και πληροφορίες κατάστασης Πιστοποιητικού, είτε με τη μορφή μιας ΛΑΠ είτε απάντησης OCSP.

Τεκμήριο Αιτήματος: Μια τιμή που προκύπτει από μια μέθοδο που ορίζεται από τη HARICA η οποία συσχετίζει την έννοια του «ελέγχου» σε ένα αίτημα για έκδοση Πιστοποιητικού.

- Το Τεκμήριο Αιτήματος πρέπει να σχετίζεται με το κλειδί που θα χρησιμοποιηθεί στο αίτημα του Πιστοποιητικού.
- Ένα Τεκμήριο Αιτήματος μπορεί να περιλαμβάνει τη χρονική στιγμή για να είναι εμφανές το πότε δημιουργήθηκε.
- Ένα Τεκμήριο Αιτήματος μπορεί να περιλαμβάνει άλλες πληροφορίες προκειμένου να εξασφαλίζεται η μοναδικότητά του.
- Ένα Τεκμήριο Αιτήματος το οποίο περιλαμβάνει χρονική στιγμή, πρέπει να παραμείνει έγκυρο μέχρι 30 ημέρες από τη δημιουργία του.
- Ένα Τεκμήριο Αιτήματος το οποίο περιλαμβάνει χρονική στιγμή, πρέπει να θεωρείται άκυρο αν η χρονική του στιγμή είναι στο μέλλον.
- Ένα Τεκμήριο Αιτήματος το οποίο δεν περιλαμβάνει χρονική στιγμή, είναι έγκυρο για μία μόνο χρήση και η HARICA δεν θα το κάνει αποδεκτό για επόμενο έλεγχο.
- Η συσχέτιση πρέπει να χρησιμοποιεί αλγόριθμο ψηφιακής υπογραφής ή αλγόριθμο δημιουργίας hash, τουλάχιστον όσο ισχυρό χρησιμοποιείται για την τελική υπογραφή του αιτήματος Πιστοποιητικού.

Αιτούμενο Περιεχόμενο Ιστοχώρου: Είτε μια Τυχαία Τιμή είτε ένα Τεκμήριο Αιτήματος, μαζί με επιπλέον πληροφορία που αναγνωρίζει μοναδικά τον Συνδρομητή, όπως ορίζεται από την HARICA.

Δεσμευμένη Διεύθυνση IP: Διεύθυνση IPv4 ή IPv6 την οποία ο IANA έχει επισημάνει ως κατοχυρωμένη:

- http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml
- http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml

Κορυφαία ΑΠ: Η Αρχή Πιστοποίησης κορυφαίου επιπέδου (ένας οργανισμός) της οποίας το Πιστοποιητικό ΑΠ (ή το αντίστοιχο Δημόσιο Κλειδί) διανέμεται από εφαρμογές Προμηθευτών Λογισμικού ως σημείο εμπιστοσύνης (trust anchor).

Κορυφαίο Πιστοποιητικό: Το Πιστοποιητικό της ΑΠ στο οποίο το Δημόσιο Κλειδί έχει υπογραφεί ψηφιακά από το αντίστοιχο Ιδιωτικό Κλειδί.

Κυρίαρχο Κράτος: Μία πολιτεία ή χώρα η οποία αυτό-κυβερνάται και δεν εξαρτάται από, ή δεν υπόκειται σε άλλη δύναμη.

Ανώτερος Κυβερνητικός Φορέας: Με βάση τη δομή διακυβέρνησης είναι ο Κυβερνητικός Φορέας ή οι Φορείς που έχουν την ικανότητα να διαχειρίζονται, να κατευθύνουν και να ελέγχουν τις δραστηριότητες του Αιτούντα.

Υποκείμενο: Το φυσικό πρόσωπο, συσκευή, σύστημα, μονάδα ή νομική οντότητα που αναφέρεται στο Πιστοποιητικό ως Υποκείμενο (Subject). Το Υποκείμενο είναι είτε ο Συνδρομητής είτε μία συσκευή υπό τον έλεγχο και τη διαχείριση του Συνδρομητή.

Πληροφορίες Ταυτότητας του Υποκειμένου: Πληροφορίες που προσδιορίζουν το Υποκείμενο του Πιστοποιητικού. Στις πληροφορίες αυτές δεν περιλαμβάνεται ένα όνομα χώρου που υπάρχει στην επέκταση subjectAltName ή στο πεδίο commonName στο Υποκείμενο.

Ενδιάμεση ΑΠ: Μία Αρχή Πιστοποίησης που έχει στην κατοχή της ή υπό τον έλεγχο της το Ιδιωτικό Κλειδί που σχετίζεται με Πιστοποιητικό Ενδιάμεσης ΑΠ. Ο Διαχειριστής της Ενδιάμεσης ΑΠ μπορεί να είναι είτε μια Ενδιάμεση ΑΠ Εξωτερικής Διαχείρισης είτε μία Ενδιάμεση ΑΠ Εσωτερικής Διαχείρισης.

Πιστοποιητικό Ενδιάμεσης ΑΠ: Πιστοποιητικό ΑΠ που έχει υπογραφεί από το Ιδιωτικό Κλειδί που σχετίζεται με ένα Κορυφαίο Πιστοποιητικό ή με ένα διαφορετικό Πιστοποιητικό Ενδιάμεσης ΑΠ.

Συνδρομητής: Ένα φυσικό ή νομικό πρόσωπο στο οποίο εκδίδεται Πιστοποιητικό και ο οποίος δεσμεύεται νομικά από μία Σύμβαση Συνδρομητή ή από τους Όρους Χρήσης της υπηρεσίας.

Σύμβαση Συνδρομητή: Μία σύμβαση μεταξύ της HARICA και του Αιτούντα/Συνδρομητή που καθορίζει τα δικαιώματα και τις υποχρεώσεις των μερών.

Θυγατρική Εταιρεία: Μια εταιρεία που ελέγχεται από μία Μητρική Εταιρεία.

Ύποπτος Κώδικας: Κώδικας που περιέχει κακόβουλη λειτουργικότητα ή σοβαρή ευπάθεια και περιλαμβάνει spyware, malware και άλλου είδους κώδικα λογισμικού που εγκαθίσταται χωρίς τη συγκατάθεση του χρήστη και/ή αντιστέκεται στην αφαίρεσή του, όπως και κώδικας που μπορεί να παραβιαστεί και να εκτελεστεί με τρόπους πέρα από τις προθέσεις των δημιουργών του, προκειμένου να παραβιάσει και να υποβαθμίσει την αξιοπιστία του συστήματος στο οποίο θα εκτελεστεί.

Τεχνικά Περιορισμένο Πιστοποιητικό Ενδιάμεσης ΑΠ: Ένα Πιστοποιητικό μιας Ενδιάμεσης ΑΠ που χρησιμοποιεί ένα συνδυασμό των επεκτάσεων “Extended Key Usage” και “Name Constraints” για να περιορίσει το πεδίο εντός του οποίου η Ενδιάμεση ΑΠ μπορεί να εκδίδει Πιστοποιητικά Συνδρομητή ή άλλα Πιστοποιητικά Ενδιάμεσων ΑΠ.

Όροι Χρήσης: Διατάξεις σχετικά με τη προστασία και τις αποδεκτές χρήσεις ενός Πιστοποιητικού που εκδίδεται σύμφωνα με την παρούσα ΠΠ/ΔΔΠ, όταν ο Αιτών/Συνδρομητής αποτελεί Συνεργάτη της HARICA ή είναι η HARICA.

Χρονο-σφραγίδα: δεδομένα σε ηλεκτρονική μορφή που συνδέουν άλλα ηλεκτρονικά δεδομένα με συγκεκριμένη χρονική στιγμή παρέχοντας αποδείξεις ότι αυτά τα δεδομένα ίσχυαν τη δεδομένη χρονική στιγμή.

Τεκμήριο Χρονοσήμανσης: ένα αντικείμενο δεδομένων που συνδέει μια έκφανση του χρόνου σε μια συγκεκριμένη χρονική στιγμή με μια ψηφιακή υπογραφή, με αποτέλεσμα τη δημιουργία πειστήριου.

Αρχή Χρονοσήμανσης (ΑΧΣ): Η Αρχή που παρέχει υπηρεσίες χρονοσήμανσης χρησιμοποιώντας μια ή περισσότερες μονάδες χρονοσήμανσης.

Μονάδα Χρονοσήμανσης (ΜΧΣ): Το σύνολο του υλικού και λογισμικού που αντιμετωπίζεται ως μονάδα και έχει ενεργό ένα μοναδικό κλειδί υπογραφής χρονοσήμανσης κάθε φορά.

Δήλωση Γνωστοποίησης ΑΧΣ: το σύνολο των δηλώσεων σχετικά με τις πολιτικές και τις διαδικασίες μιας ΑΧΣ που απαιτούν ειδικότερη επισήμανση ή γνωστοποίηση στους συνδρομητές και στους βασιζόμενα μέρη, όπως για παράδειγμα η συμμόρφωση με κανονιστικές απαιτήσεις.

Αξιόπιστο Σύστημα: Ηλεκτρονικοί υπολογιστές, λογισμικό, και διαδικασίες που:

- είναι εύλογα ασφαλείς έναντι εισβολής και κακής χρήσης,
- παρέχουν ένα εύλογο επίπεδο διαθεσιμότητας, αξιοπιστίας και ορθής λειτουργίας,
- είναι κατάλληλοι για την εκτέλεση των καθηκόντων που προορίζονται και
- εφαρμόζουν τη σχετική πολιτική ασφάλειας.

Μη Εκχωρημένο Όνομα Χώρου: Ένα Όνομα Χώρου το οποίο δεν είναι Εκχωρημένο.

UTC(k): έκφανση του χρόνου όπως απεικονίζεται από το πιστοποιημένο εργαστήριο "k" και το οποίο βρίσκεται σε πολύ μεγάλη συμφωνία με την Παγκόσμια Ώρα (UTC), με στόχο την επίτευξη ακρίβειας ±100 ns.

Έγκυρο Πιστοποιητικό: Το Πιστοποιητικό που περνά τη διαδικασία επαλήθευσης που ορίζεται στο RFC 5280.

Ειδικοί Ελέγχου Εγκυρότητας: Κάποιος που εκτελεί τα καθήκοντα επαλήθευσης των πληροφοριών που καθορίζονται από αυτό το κείμενο ΠΠ/ΔΔΠ.

Περίοδος Ισχύος (ενός Πιστοποιητικού): Η χρονική περίοδος ισχύος ενός Πιστοποιητικού από την τιμή `notBefore` έως `notAfter`, συμπεριλαμβανομένων των τιμών αυτών.

Σάρωση για Ευπάθειες: Μια διαδικασία που χρησιμοποιεί χειροκίνητα ή αυτοματοποιημένα εργαλεία διερεύνησης εσωτερικών και εξωτερικών συστημάτων με σκοπό να ελέγξει την κατάσταση των λειτουργικών συστημάτων, των υπηρεσιών και των συσκευών που εκτίθενται στο δίκτυο και την παρουσία ευπαθειών κι εξάγει αναφορές.

WHOIS: Πληροφορίες που έχουν ληφθεί απευθείας από έναν Καταχωρητή Ονομάτων Χώρου μέσω του πρωτοκόλλου που ορίζεται στο RFC 3912, μέσω του Registry Data Access Protocol που ορίζεται στο RFC 7482, ή μέσω ενός ιστοχώρου με HTTPS.

Πιστοποιητικό Μπαλαντέρ: Είναι ένα πιστοποιητικό που περιέχει έναν αστερίσκο (*) στην πιο αριστερή θέση οποιουδήποτε από τα Πλήρως Πιστοποιημένα Ονόματα Χώρου (FQDN) που περιέχονται στο Πιστοποιητικό.

Όνομα Χώρου Μπαλαντέρ: Ένα Όνομα Χώρου που αποτελείται από έναν αστερίσκο που ακολουθείται από μια τελεία ("*.") και στη συνέχεια ένα Πλήρως Πιστοποιημένο Όνομα Χώρου (FQDN).

1.6.2 Ακρωνύμια

Ελληνικός όρος	Συντόμευση	Αγγλικός όρος	Συντόμευση
Όνομα Χώρου Εξουσιοδότησης		Authorization Domain Name	ADN
Αίτημα Υπογραφής Πιστοποιητικού		Certificate Signing Request	CSR
Αιτούμενος		Applicant	
Αναγνώριση		Identification	
Αναγνωριστικό Αντικειμένου	ΑΑ	Object Identifier	OID
Αποθετήριο Δεδομένων		Data Repository	
Αρχή Καταχώρισης	ΑΚ	Registration Authority	RA
Αρχή Πιστοποίησης	ΑΠ	Certification Authority	CA
Αρχή Πιστοποίησης Πολιτικής	ΑΠΠ	Policy Certification Authority	PCA
Αρχή Χρονοσήμανσης	ΑΧΣ	Time-Stamp Authority	TSA
Ασφαλής Διάταξη Δημιουργίας Υπογραφής	ΑΔΔΥ	Secure Signature Creation Device	SSCD
Αυθυπόγραφα πιστοποιητικά		Self-signed certificates	
Βασιζόμενο Μέρος		Relying Party	
Δήλωση Διαδικασιών Πιστοποίησης	ΔΔΠ	Certification Practice Statement	CPS
Δημόσιο Κλειδί		Public Key	
Διαδρομή Πιστοποίησης	ΔΠ	Certification Path	
Διακεκριμένο Όνομα	ΔΟ	Distinguished Name	DN
Διακριτικός Τίτλος		Doing Business As	DBA
Διαφάνεια Πιστοποιητικών		Certificate Transparency	CT
Εγκεκριμένη Διάταξη Δημιουργίας Υπογραφής/Σφραγίδας	ΕΔΔΥ	Qualified Signature/Seal Creation Device	QSCD
Εγκεκριμένο Πιστοποιητικό		Qualified Certificate	
Εγκεκριμένος Πάροχος Υπηρεσιών Εμπιστοσύνης	ΕΠΥΕ	Qualified Trust Service Provider	QTSP
Εξουσιοδότηση Αρχών Πιστοποίησης		Certification Authority Authorization	CAA
Επιβεβαίωση κατοχής Χώρου Ονομάτων		Domain Validation Cert. Policy	DVCP
Επιβεβαίωση Οργανισμού		Organizational Validation Cert. Policy	OVCP

Επιτροπή Διαχείρισης Πολιτικής Πιστοποίησης και Διαδικασιών	ΕΔΠΠ	Policy Management Committee	PMC
Ιδιωτικό Κλειδί		Private Key	
Κοινό Όνομα		CommonName	CN
Λίστα Ανάκλησης Πιστοποιητικών	ΛΑΠ	Certificate Revocation List	CRL
Μεσεγγύηση ιδιωτικού κλειδιού		Private Key Escrow	
Μονάδα Χρονοσήμανσης	ΜΧΣ	Time-Stamping Unit	TSU
Όνομα Οργανισμού		OrganizationName	O
Όνομα Χώρας		CountryName	C
Οργανωτική Μονάδα		Organizational Unit	OU
Πάροχος Υπηρεσιών Εμπιστοσύνης		Trust Service Provider	TSP
Πιστοποιητικά για Αρχή Πιστοποίησης		CA Certificates	
Πιστοποιητικά για Εξυπηρετητές		Server Certificates	
Πιστοποιητικά για Υπογραφή Αντικειμένων		Object-Signing Certificates	
Πιστοποιητικά Ταυτότητας		Personal Identity Certificates	
Πιστοποιητικό		Certificate	
Πολιτική Πιστοποίησης	ΠΠ	Certification Policy	CP
Προσωπικός Κωδικός Αναγνώρισης		Personal identification number	PIN
Συνδρομητής		Subscriber	
Συντονισμένη Παγκόσμια Ώρα	ΣΠΩ	Coordinated Universal Time	UTC
Ταυτοποίηση		Authentication	
Τεκμήριο Χρονοσήμανσης		Time-Stamp Token	TST
Υποδομή Δημοσίου Κλειδιού	ΥΔΚ	Public Key Infrastructure	PKI
Υποκείμενο Πιστοποιητικού		Certificate Subject	
Χαρακτηριστικό πολιτικής		Policy Qualifier	
		Extended Key Usage	EKU
		Fully Qualified Domain Name	FQDN
		Hardware Security Module	HSM
		Hyper Text Transfer Protocol	HTTP
		IETF Working Group on PKI	PKIX
		International Standards Organization's Object Identifier	OID
		International Organization for Standardization	ISO
		International Telecommunication Union	ITU
		Internet Assigned Numbers Authority	IANA
		Internet Corporation for Assigned Names and Numbers	ICANN

		Internet Engineering Task Force	IETF
		ITU Telecommunication Standardization Sector	ITU-T
		ITU-T standard for Certificates and authentication framework	X.509
		On-line Certificate Status Protocol	OCSP
		Public-Key Cryptography Standards	PKCS
		Secure Hashing Algorithm	SHA
		Secure multipurpose Internet mail extensions	S/MIME
		Secure Socket Layer	SSL
		Subordinate Certification Authority	subCA
		Transport Layer Security	TLS
		Top Level Domain	TLD
		Uniform Resource Identifier	URI
		Uniform Resource Locator	URL
		United States Federal Information Processing Standards	FIPS
		European Banking Authority	EBA[1]
		Extended Validation	EV
Εθνική Αρμόδια Αρχή	ΕΑΑ	National Competent Authority	NCA
		Payment Services Directive 2	PSD2[1]
Πάροχος Υπηρεσιών Πληρωμών	ΠΥΠ	Payment Service Provider	PSP[2]
		Account Information Service Provider	PSP_AI[2]
		Account Servicing Payment Service Provider	PSP_AS[2]
		Payment Service Provider Issuing Card-based payment instruments	PSP_IC[2]
		Payment Initiation Service Provider	PSP_PI[2]
		Qualified electronic Seal Certificate	QSealC
		Qualified Website Authentication Certificate	QWAC

[1] Βλ. Οδηγία (ΕΕ) 2015/2366
[2] Βλ. Εξουσιοδοτημένο Κανονισμό Επιτροπής (ΕΕ) 2018/389

2 Δημοσιοποίηση και Αποθετήρια

2.1 Αποθετήρια

Η ΥΔΚ HARICA διαθέτει ειδικό ιστοχώρο αποθετηρίου όπου δημοσιεύονται κείμενα πολιτικής, πιστοποιητικά Αρχών Πιστοποίησης και τελικά πιστοποιητικά συνδρομητών/συσκευών στη διεύθυνση https://repo.harica.gr. Κατά περίπτωση μπορεί να υπάρχουν κατανεμημένοι ιστοχώροι αποθετηρίων για κάθε ενδιάμεση Αρχή Πιστοποίησης/Αρχή Καταχώρισης που συμμετέχει στην ΥΔΚ.

2.2 Δημοσιοποίηση πληροφοριών της Αρχής Πιστοποίησης

Η ΥΔΚ HARICA διαθέτει ιστοχώρο αποθετηρίου διαθέσιμο μέσω Διαδικτύου όπου δημοσιεύονται τα Ψηφιακά Πιστοποιητικά των Αρχών Πιστοποίησης (τύπου X.509.v3), τα Ψηφιακά Πιστοποιητικά που εκδίδονται σύμφωνα με τη ΠΠ/ΔΔΠ, την τρέχουσα ΛΑΠ, το κείμενο της ΠΠ/ΔΔΠ και άλλα κείμενα σχετικά με τη λειτουργία της (π.χ. μνημόνιο συνεργασίας και συναντίληψης - MoU).

Η ΥΔΚ HARICA εκτελεί όλες τις ενέργειες για την αδιάλειπτη - κατά το δυνατόν- διαθεσιμότητα του ιστοχώρου αποθετηρίου.

Η ηλεκτρονική διεύθυνση του ιστοχώρου αποθετηρίου της Υποδομής Δημοσίου Κλειδιού HARICA είναι https://repo.harica.gr.

Οι προμηθευτές λογισμικών που αξιοποιούν Πιστοποιητικά SSL/TLS, μπορούν να χρησιμοποιούν την ακόλουθη λίστα ιστοχώρων για έλεγχο λειτουργικότητας:

Root CA	**Status**	**URL**
Harica Root CA 2011	Έγκυρο	https://haricarootca2011-valid.harica.gr
	Ανακλημένο	https://haricarootca2011-revoked.harica.gr
	Ληγμένο	https://haricarootca2011-expired.harica.gr
Harica Root CA 2015	Έγκυρο	https://haricarootca2015-valid-ev.harica.gr
	Ανακλημένο	https://haricarootca2015-revoked-ev.harica.gr
	Ληγμένο	https://haricarootca2015-expired-ev.harica.gr
Harica ECC Root CA 2015	Έγκυρο	https://haricaeccrootca2015-valid-ev.harica.gr
	Ανακλημένο	https://haricaeccrootca2015-revoked-ev.harica.gr
	Ληγμένο	https://haricaeccrootca2015-expired-ev.harica.gr

2.3 Συχνότητα δημοσιοποίησης

Η Λίστα Ανάκλησης Πιστοποιητικών ενημερώνεται σύμφωνα με την παράγραφο 4.9.7.

2.4 Έλεγχος πρόσβασης στον ιστοχώρο αποθετηρίου

Η πρόσβαση στο τμήμα του αποθετηρίου που περιέχει τα πιστοποιητικά που έχουν εκδοθεί είναι διαθέσιμη μέσω ιστοσελίδας αναζήτησης. Η αναζήτηση γίνεται είτε με το σειριακό αριθμό του πιστοποιητικού (οπότε προβάλλεται μία εγγραφή), ή εισάγοντας τμήμα του διακεκριμένου ονόματος του υποκειμένου του πιστοποιητικού, οπότε είναι πιθανό να επιστραφεί λίστα πιστοποιητικών.

Ενδέχεται να επιβάλλεται περιορισμός στην πρόσβαση στο αποθετήριο για λόγους προστασίας από επιθέσεις απαρίθμησης (προσπάθεια άντλησης όλων των εγγραφών).

3 Αναγνώριση και ταυτοποίηση

3.1 Ονοματολογία

3.1.1 Τύποι ονομάτων

Τα ονόματα που χρησιμοποιούνται στην έκδοση του πιστοποιητικού εξαρτώνται από την κλάση του πιστοποιητικού και είναι σύμφωνα με το πρότυπο ITU X.500 για τα Διακεκριμένα Ονόματα.

3.1.1.1 Συμμόρφωση του ονόματος Πιστοποιητικού με Baseline Requirements

Η HARICA δεν εκδίδει πιστοποιητικά που περιέχουν Εσωτερικό Όνομα και/ή δεσμευμένες διευθύνσεις IP.

3.1.2 Υποχρέωση τα ονόματα να έχουν συγκεκριμένο νόημα

Τα ονόματα που περιλαμβάνονται στα πιστοποιητικά χρηστών, πρέπει με κάποιο τρόπο να συσχετίζονται με το Συνδρομητή. Θα πρέπει επίσης να έχουν νόημα , να είναι σαφή και να παράγουν μοναδικά DNs ανά εκδούσα ΑΠ. Σε περιπτώσεις όπου το Common Name (CN) ή οποιοδήποτε άλλο στοιχείο θα μπορούσε να παράγει ένα διφορούμενο ή μη μοναδικό ΔΟ, ή εάν για οποιοδήποτε λόγο απουσιάζει ένα CN, η HARICA θα χρησιμοποιεί ένα μοναδικό αναγνωριστικό ή/και ένα σειριακό αριθμό στο ΔΟ του Υποκειμένου για να προσδιορίσει με μοναδικό τρόπο ένα Πιστοποιητικό.

3.1.3 Δυνατότητα έκδοσης ανώνυμων πιστοποιητικών ή πιστοποιητικών με ψευδώνυμα

Βλ. παράγραφο 3.2.2.2.

3.1.4 Κανόνες ερμηνείας διαφόρων τύπων 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).

Χαρακτηριστικό DN	Ερμηνεία
CN or common name (OID: 2.5.4.3)	Αν υπάρχει αυτό το πεδίο, για πιστοποιητικά χρήσης SSL/TLS, πρέπει να περιέχει ένα FQDN ή μια Διεύθυνση IP που είναι μια από τις τιμές που περιέχονται στην επέκταση subjectAltName του Πιστοποιητικού. Για πιστοποιητικά

	S/MIME ή πιστοποιητικά Υπογραφής Κώδικα αυτό το πεδίο πρέπει να περιέχει στοιχεία του ονόματος του Υποκειμένου. Για Πιστοποιητικά Χρήστη, το "common name" χρησιμοποιείται για την φιλική εκδοχή του ονόματος του Υποκειμένου ώστε να εκπροσωπήσει τον εαυτό του. Αυτό το όνομα δεν είναι απαραίτητο να ταιριάζει απόλυτα με το πλήρες καταχωρισμένο όνομα ενός οργανισμού ή το επίσημο ονοματεπώνυμο ενός προσώπου.
G or givenName (OID: 2.5.4.42)	Το επίσημο όνομα του Υποκειμένου
SN or surname (OID: 2.5.4.4)	Το επίσημο επίθετο του Υποκειμένου
E or emailAddress	Η διεύθυνση email του Υποκειμένου
streetAddress (OID: 2.5.4.9)	Η διεύθυνση κατοικίας του Υποκειμένου
postalCode (OID: 2.5.4.17)	Ο ταχυδρομικός κώδικας της διεύθυνσης κατοικίας
L or Locality (OID: 2.5.4.7)	Η πόλη της ταχυδρομικής διεύθυνσης
ST for State or Province Name (OID: 2.5.4.8)	Ο Δήμος ή η Περιοχή της ταχυδρομικής διεύθυνσης
C or Country (OID: 2.5.4.6)	Η Χώρα του Υποκειμένου
O or Organization (OID: 2.5.4.10)	Το πλήρες καταχωρισμένο Όνομα του Οργανισμού του Υποκειμένου. Για τα **Πιστοποιητικά QCP-w, QCP-w-psd2 και EV**, η ερμηνεία αυτού του χαρακτηριστικού εξηγείται στην παράγραφο 9.2.1 των Οδηγιών EV.
OU or Organizational Unit	Η Μονάδα του Οργανισμού του Υποκειμένου ή η υπο-Μονάδα του, ή ειδικό χαρακτηριστικό του υπογράφοντα που σχετίζεται με τον σκοπό χρήσης ή τα χαρακτηριστικά του πιστοποιητικού
serialNumber (OID: 2.5.4.5)	Μοναδικό αναγνωριστικό που διακρίνει το Όνομα του Υποκειμένου σύμφωνα με το πλαίσιο της Εκδούσας ΑΠ. Για τα **Πιστοποιητικά QCP-w, QCP-w-psd2 και EV**, η ερμηνεία αυτού του χαρακτηριστικού εξηγείται στην παράγραφο 9.2.6 των Οδηγιών EV.
OrganizationIdentifier (OID: 2.5.4.97)	Μοναδικό αναγνωριστικό του Οργανισμού
Business Category (OID: 2.5.4.15)	**Μόνο για τα Πιστοποιητικά QCP-w, QCP-w-psd2 και EV.** Αυτό το πεδίο ΠΡΕΠΕΙ να περιέχει μία από τις εξής ακολουθίες: "Private Organization", "Government Entity", "Business Entity" ή "Non-Commercial Entity" ανάλογα με το

	αν το Υποκείμενο πληροί τις προϋποθέσεις της Ενότητας 8.5.2, 8.5.3 , 8.5.4 ή 8.5.5 των Οδηγιών EV, αντιστοίχως.
jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3) **jurisdictionStateOrProvinceName** (OID: 1.3.6.1.4.1.311.60.2.1.2) **jurisdictionLocalityName** (OID: 1.3.6.1.4.1.311.60.2.1.1)	**Μόνο για τα Πιστοποιητικά QCP-w, QCP-w-psd2 και EV.** Αυτά τα πεδία ΔΕΝ ΠΡΕΠΕΙ να περιέχουν πληροφορίες που δεν σχετίζονται με το επίπεδο της Υπηρεσίας που διενεργεί τη Σύσταση ή του Οργανισμού Καταχώρισης. Η ερμηνεία αυτού του χαρακτηριστικού εξηγείται στην παράγραφο 9.2.5 των Οδηγιών EV.

3.1.4.1 Τελικά Πιστοποιητικά για ηλεκτρονικές υπογραφές

Τα Πιστοποιητικά για Προηγμένες ή Εγκεκριμένες ηλεκτρονικές υπογραφές εκδίδονται σε φυσικά πρόσωπα και περιλαμβάνουν στο subject DN του Πιστοποιητικού τουλάχιστον τα ακόλουθα χαρακτηριστικά:

- "countryName"
- "givenName" και "surname"
- "countryName"

3.1.4.2 Τελικά Πιστοποιητικά για ηλεκτρονικές σφραγίδες

Τα Πιστοποιητικά για Προηγμένες ή Εγκεκριμένες ηλεκτρονικές σφραγίδες εκδίδονται σε νομικά πρόσωπα και περιλαμβάνουν στο subject DN του Πιστοποιητικού τουλάχιστον τα ακόλουθα χαρακτηριστικά:

- "commonName"
- "organizationName"
- "countryName"
- "organizationIdentifier"

3.1.4.3 Πιστοποιητικά συσκευών για χρήση SSL/TLS

Τα πιστοποιητικά για χρήση SSL/TLS σύμφωνα με την πολιτική DVCP, πρέπει να περιέχουν το FQDN της συσκευής ή μία Διεύθυνση IP στην επέκταση “Subject Alternative Name – SAN”. Το πεδίο “Common Name” είναι προαιρετικό αλλά σε περίπτωση που υπάρχει, πρέπει να περιλαμβάνει τουλάχιστον ένα FQDN ή μία Διεύθυνση IP που είναι μια από τις τιμές που υπάρχουν στην επέκταση subjectAltName.

Τα πιστοποιητικά για χρήση SSL/TLS σύμφωνα με την πολιτική OVCP, επιπρόσθετα με τα παραπάνω πεδία, πρέπει να περιλαμβάνουν στο subject DN του Πιστοποιητικού τουλάχιστον τα ακόλουθα χαρακτηριστικά :

- "organizationName"
- "countryName"
- "localityName" ή "stateOrProvinceName"

Τα Πιστοποιητικά για SSL / TLS σύμφωνα με τις πολιτικές των EV Guidelines, εκτός από τα παραπάνω πεδία, πρέπει να περιλαμβάνουν τουλάχιστον τα ακόλουθα πρόσθετα χαρακτηριστικά στο πεδίο subject DN του Πιστοποιητικού:

- “serialNumber”
- “businessCategory”

- “jurisdictionCountryName” ή/και “jurisdictionStateOrProvinceName” ή/και “jurisdictionLocalityName”.

Τα Πιστοποιητικά για SSL / TLS σύμφωνα με τις πολιτικές EVCP και QCP-w σύμφωνα με το ETSI EN 319 411-1 και 319 411-2, εκτός από τα παραπάνω πεδία, πρέπει να περιλαμβάνουν τουλάχιστον τα ακόλουθα επιπλέον χαρακτηριστικά στο πεδίο subject DN του πιστοποιητικού:

- “organizationIdentifier”

και θα περιέχουν την επέκταση πιστοποιητικού QCStatement σύμφωνα με το πρότυπο ETSI TS 119 412-1.

Τα Πιστοποιητικά για SSL / TLS σύμφωνα με τις πολιτικές QCP-w-psd2 και QCP-l-psd2, εκτός από τα παραπάνω πεδία, πρέπει να περιλαμβάνουν τουλάχιστον τα ακόλουθα επιπλέον χαρακτηριστικά στο πεδίο subject DN του πιστοποιητικού:

- “organizationIdentifier”

και θα περιέχουν την επέκταση πιστοποιητικού PSD2 QCStatement που περιλαμβάνει το αναγνωριστικό της ΕΑΑ και τους ρόλους ΠΥΠ του υποκειμένου σύμφωνα με το πρότυπο ETSI TS 119 495.

3.1.4.4 Πιστοποιητικά Υπογραφής Κώδικα

Τα Πιστοποιητικά Υπογραφής Κώδικα όπως ορίζει η πολιτική IVCP ή OVCP, που εκδίδονται σε φυσικά ή νομικά πρόσωπα αντίστοιχα, περιλαμβάνουν στο subject DN του Πιστοποιητικού τουλάχιστον τα ακόλουθα χαρακτηριστικά:

- "commonName"
- "organizationName". Επειδή τα χαρακτηριστικά που αφορούν στο όνομα του Υποκειμένου φυσικών προσώπων, "givenName" και "surname", δεν υποστηρίζονται από λογισμικά εφαρμογών, η HARICA μπορεί να χρησιμοποιεί το πεδίο subject:organizationName field για να εκφράσει το όνομα του Υποκειμένου ή το όνομα με το οποίο είναι ευρέως γνωστό.
- "countryName"

Τα Πιστοποιητικά EV για Υπογραφή Κώδικα σύμφωνα με την πολιτική EVCP, επιπλέον των παραπάνω πεδίων, θα πρέπει να περιλαμβάνουν τουλάχιστον τα ακόλουθα επιπρόσθετα χαρακτηριστικά στο πεδίο subject DN του Πιστοποιητικού:

- “serialNumber”
- “businessCategory”
- “jurisdictionCountryName” or “jurisdictionStateOrProvinceName” or “jurisdictionLocalityName”,
- “streetAddress”, “postalCode”, “localityName”, “stateOrProvinceName”, “countryName” σύμφωνα με την ενότητα 9.2.7 των Οδηγιών EV.

3.1.4.5 Πιστοποιητικά για επαλήθευση ταυτότητας Web Client

Τα Πιστοποιητικά για επαλήθευση ταυτότητας web client που εκδίδονται σε φυσικά ή νομικά πρόσωπα, περιλαμβάνουν τουλάχιστον τα ακόλουθα χαρακτηριστικά στο subject DN του Πιστοποιητικού:

- "commonName"
- "organizationName". Επειδή τα χαρακτηριστικά που σχετίζονται με το όνομα του Υποκειμένου για τα φυσικά πρόσωπα, "givenName" και "surname", δεν

υποστηρίζονται ευρέως από τα λογισμικά εφαρμογών, η HARICA μπορεί να χρησιμοποιεί το πεδίο subject:organizationName για να εκφράσει το όνομα του Υποκειμένου φυσικού προσώπου ή Διακριτικό Τίτλο (DBA)
- "countryName"

3.1.5 Μοναδικότητα ονομάτων

Το Διακεκριμένο Όνομα σε κάθε Πιστοποιητικό Συνδρομητή πρέπει να είναι μοναδικό για κάθε Εκδούσα ΑΠ, ενώ είναι επιθυμητό να είναι μοναδικό και σε ολόκληρη την ιεραρχία πιστοποίησης της HARICA. Το Διακεκριμένο Όνομα ενός Συνδρομητή δεν πρέπει ποτέ να αντιστοιχισθεί με άλλη οντότητα από την ίδια Εκδούσα ΑΠ.

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

Οι Αιτούντες, υποβάλλοντας αίτημα για πιστοποιητικό, δηλώνουν και διαβεβαιώνουν εγγυώμενοι προς τούτο ότι το αίτημα είναι ελεύθερο από οποιαδήποτε δικαιώματα πνευματικής ή διανοητικής ιδιοκτησίας τρίτου μέρους και δεν περιέχει δεδομένα τα οποία με οποιονδήποτε τρόπο παρεμποδίζουν ή παραβιάζουν τα δικαιώματα οποιουδήποτε τρίτου, σε οποιαδήποτε δικαιοδοσία, σε σχέση με διπλώματα ευρεσιτεχνίας, εμπορικά σήματα, σήματα υπηρεσιών, εμπορικές επωνυμίες, επωνυμίες εταιρειών, διακριτικούς τίτλους και άλλα εμπορικά δικαιώματα, και ότι δε παρουσιάζουν τα δεδομένα για οποιονδήποτε παράνομο σκοπό. Τα δεδομένα που αφορά αυτή η δήλωση και διαβεβαίωση, έχουσα χαρακτήρα εγγυήσεως περιλαμβάνουν, χωρίς να περιορίζονται σε αυτά, οποιοδήποτε όνομα χώρου, περιοχή χώρου ονομάτων, Διακεκριμένο Όνομα, ή Πλήρως Πιστοποιημένο Όνομα Χώρου (FQDN), και/ή κανένα εμπορικό όνομα ή διακριτικό τίτλο, που περιέχεται σε οποιοδήποτε τμήμα της αίτησης για πιστοποιητικό.
Αρμόδιο όργανο για θέματα επίλυσης διαφορών σχετικά με την κυριότητα ονομάτων ή σχετικά με την παροχή των υπηρεσιών ή οτιδήποτε άλλο σχετικό, είναι η ΕΔΠΠ της HARICA. Δείτε επίσης, την παράγραφο 9.13.

3.2 Αρχική Επαλήθευση ταυτότητας

Σύμφωνα με την τρέχουσα πολιτική επαλήθευσης, η HARICA θα ζητά μόνο στοιχεία ταυτότητας που ικανοποιούν τις απαιτήσεις του σκοπούμενου τύπου πιστοποιητικού. Η ΥΔΚ HARICA εκδίδει διάφορα είδη ψηφιακών πιστοποιητικών, τα οποία προορίζονται για SSL/TLS, S/MIME, Υπογραφή Κώδικα, Ψηφιακές Υπογραφές. Κάθε τύπος πιστοποιητικού έχει διαφορετικά επίπεδα διασφάλισης, ανάλογα με το επίπεδο πολιτικής του ελέγχου εγκυρότητας, το οποίο ξεκινά από την πολιτική LCP μέχρι την Εκτεταμένη Επαλήθευση (Extended Validation) και την πολιτική QCP.

Η ΥΔΚ HARICA εξετάζει για αλλοίωση ή πλαστογράφηση οποιοδήποτε έγγραφο χρησιμοποιείται για επιβεβαίωση στοιχείων. Η ΥΔΚ HARICA επαληθεύει την ταυτότητα και την κατάσταση οποιουδήποτε Αιτούντος ανάλογα με την περίπτωση και όπως απαιτείται για τον εκάστοτε τύπο πιστοποιητικού και το ζητούμενο επίπεδο διασφάλισης. Αλλοίωση ή πλαστογράφηση οποιουδήποτε εγγράφου χρησιμοποιήθηκε σε αυτή τη διαδικασία, παραποίηση της ταυτότητας ή της κατάστασης οποιουδήποτε Αιτούντος που σχετίζεται με τη διαδικασία, συνιστά λόγο για την απόρριψη αίτησης πιστοποιητικού ή / και άμεσης ανάκλησης τυχόν υπάρχοντος πιστοποιητικού που βασίζεται σε αλλοιωμένα ή πλαστογραφημένα έγγραφα ή ψευδή ή παραποιημένη ταυτότητα ή κατάσταση σύμφωνα με την ενότητα 4.9.1.1.

Για τα πιστοποιητικά EV SSL/TLS, η HARICA λαμβάνει όλα τα απαραίτητα μέτρα επαλήθευσης ώστε να ικανοποιηθούν οι Απαιτήσεις Επαλήθευσης EV όπως καθορίζονται από τις Οδηγίες EV SSL/TLS του CA/Browsers Forum.

Για τα πιστοποιητικά EV Code Signing, η HARICA λαμβάνει όλα τα απαραίτητα μέτρα επαλήθευσης ώστε να ικανοποιηθούν οι Απαιτήσεις Επαλήθευσης EV όπως καθορίζονται από τις Οδηγίες EV Code Signing του CA/Browsers Forum.

3.2.1 Τρόπος απόδειξης κατοχής ιδιωτικού κλειδιού

Επαληθεύεται η ταυτότητα του Αιτούντα και υποβάλλεται το CSR που περιέχει το Δημόσιο Κλειδί του αντίστοιχου Ιδιωτικού Κλειδιού. Το CSR διασφαλίζει ότι ο Αιτούντας κατέχει το Ιδιωτικό Κλειδί που αντιστοιχεί στο Δημόσιο Κλειδί το οποίο θα εισαχθεί στο αιτούμενο πιστοποιητικό, καθώς το CSR περιλαμβάνει υπογραφή που έχει δημιουργηθεί από το Ιδιωτικό Κλειδί.

Αναφορικά με τα Εγκεκριμένα Πιστοποιητικά που σχετίζονται με ιδιωτικά κλειδιά σε Εγκεκριμένες Διατάξεις Δημιουργίας Υπογραφής/Σφραγίδας (ΕΔΔΥ) , σύμφωνα με τη σχετική Ευρωπαϊκή/Ελληνική νομοθεσία για την Ηλεκτρονική Υπογραφή (QCP+), τα ιδιωτικά κλειδιά δημιουργούνται απευθείας στις Εγκεκριμένες Διατάξεις Δημιουργίας Υπογραφής παρουσία του δικαιούχου του Πιστοποιητικού και ενός εξουσιοδοτημένου προσωπικού της ΑΚ που πιστοποιεί ότι το ιδιωτικό κλειδί δημιουργήθηκε στην ΕΔΔΥ. Η παρουσία εξουσιοδοτημένου προσωπικού της ΑΚ μπορεί αποφευχθεί αν υπάρχει αξιόπιστη διαδικασία που εξασφαλίζει με τεχνικά μέσα, ότι το ιδιωτικό κλειδί δημιουργείται μόνο εντός της ΕΔΔΥ. Ο κάτοχος του Πιστοποιητικού είναι υπεύθυνος για την προστασία της ΕΔΔΥ με Προσωπικό Αριθμό Αναγνώρισης (Personal Identification Number - PIN).

Η απαίτηση αυτή δεν ισχύει όταν ένα Ζεύγος Κλειδί παράγεται από την HARICA για λογαριασμό ενός Συνδρομητή για Εγκεκριμένες υπογραφές/σφραγίδες, Πιστοποιητικά Υπογραφής κώδικα και Πιστοποιητικά Υπογραφής Κώδικα EV. Σε αυτές τις περιπτώσεις, η HARICA θα εφαρμόσει ελέγχους για τη δημιουργία των κλειδιών σε ειδικού σκοπού κρυπτογραφικές συσκευές που πληρούν τις απαιτήσεις της ενότητας 6.2.1 και θα παραδώσει αυτές τις συσκευές με ασφάλεια στον Συνδρομητή.

3.2.2 Επαλήθευση ταυτότητας οργανισμού

Η Αρχή Καταχώρισης πρέπει να επιβεβαιώνει ότι ο Αιτών ανήκει στον Οργανισμό, το όνομα του οποίου περιλαμβάνεται στο πιστοποιητικό. Όταν ένας Αιτών ζητά ένα Πιστοποιητικό με βάση τη δυνατότητα νόμιμης εκπροσώπησης ενός Νομικού Προσώπου (σύμφωνα με την πολιτική QCP-l ή QCP-l-qscd), τότε ο Αιτών θα πρέπει να παρέχει όλα τα απαραίτητα έγγραφα συμπεριλαμβάνοντας το πλήρες όνομα του Νομικού Προσώπου, το νομικό καθεστώς καθώς επίσης και τα σχετικά στοιχεία καταχώρισης (σε επίπεδο Χώρας/Νομού ή Πολιτείας/Πόλης).

Κάθε Νομικό πρόσωπο πρέπει να έχει τους δικούς του εξουσιοδοτημένους αιτούντες και μία Μητρική Εταιρεία δεν μπορεί να εξουσιοδοτεί αιτήσεις Πιστοποιητικών για Θυγατρικές Εταιρείες.

Όταν μία ΑΚ λαμβάνει ένα «Αίτημα για Πιστοποιητικό Υψηλού Κινδύνου» το οποίο ταιριάζει με Όνομα Χώρου ή Οργανισμό που έχει επισημανθεί ως «Υψηλού

Κινδύνου», τότε πριν από την έκδοση πραγματοποιείται πρόσθετος ενδελεχής έλεγχος στη διαδικασία επαλήθευσης. Για τα Πιστοποιητικά Υπογραφής Κώδικα και Πιστοποιητικά Υπογραφής Κώδικα EV, η HARICA πρέπει να προσδιορίσει εάν είναι αντιληπτό ότι η οντότητα ζητεί Πιστοποιητικό Υπογραφής Κώδικα από μια Περιοχή που θεωρείται Υψηλού Κινδύνου και να την επισημάνει ως "υψηλού κινδύνου".

Η επαλήθευση της ταυτότητας ενός Οργανισμού σε οποιοδήποτε αίτημα για EV πιστοποιητικό (Extended Validation) θα πρέπει να ακολουθεί τις διαδικασίες επαλήθευσης EV που περιγράφονται στις Οδηγίες EV. Η HARICA δημοσιεύει τις Υπηρεσίες Σύστασης και Οργανισμούς Καταχώρισης στο Αποθετήριο όπως περιγράφεται στην ενότητα 2.1.

3.2.2.1 Ταυτότητα

Αν οι Πληροφορίες Ταυτότητας του Υποκειμένου πρέπει να περιλαμβάνουν το όνομα ή τη διεύθυνση ενός οργανισμού, η ΑΚ επαληθεύει την ταυτότητα και τη διεύθυνση του οργανισμού, καθώς και ότι η διεύθυνση αυτή είναι η διεύθυνση κατοικίας/έδρας του Αιτούντα. Η HARICA επαληθεύει την ταυτότητα και τη διεύθυνση του Αιτούντα, χρησιμοποιώντας τεκμηρίωση που παρέχεται, ή επικοινωνώντας, με τουλάχιστον ένα από τα ακόλουθα :

1. Μία Κρατική Υπηρεσία στην περιοχή δικαιοδοσίας της νομικής υπόστασης , ή αναγνώρισης του Αιτούντα
2. Μία τρίτη βάση δεδομένων που ενημερώνεται περιοδικά και θεωρείται Αξιόπιστη Πηγή Δεδομένων, όπως ορίζεται στην ενότητα 3.2.2.7
3. Μία επίσκεψη στον ίδιο τον χώρο από την ΑΠ ή τρίτο που ενεργεί ως αντιπρόσωπος της ΑΠ, ή
4. Ένα Έγγραφο Βεβαίωσης

Η HARICA μπορεί να επαληθεύει τη **διεύθυνση του Αιτούντα** (αλλά όχι την ταυτότητα του Αιτούντα) μέσω ενός λογαριασμού υπηρεσιών κοινής ωφέλειας, δήλωσης τραπεζικού λογαριασμού, δήλωσης πιστωτικής κάρτας, φορολογικού στοιχείου, ή άλλου αξιόπιστου εγγράφου αναγνώρισης ταυτότητας.

3.2.2.2 Διακριτικός Τίτλος (DBA) / Επωνυμία / Ρόλοι

Η HARICA δεν επιτρέπει την έκδοση πιστοποιητικού για ανώνυμους χρήστες. Η έκδοση πιστοποιητικού για ψευδώνυμα, π.χ. «Πρύτανης» ή «Πρόεδρος», δεν προβλέπεται στην παρούσα Δήλωση Διαδικασιών Πιστοποίησης, όμως δεν απαγορεύεται. Αυτά τα ψευδώνυμα θα πρέπει να περιλαμβάνονται ως πρόσθετες πληροφορίες στα ψηφιακά πιστοποιητικά μετά την κατάλληλη διαδικασία επιβεβαίωσης τους που επαληθεύει ότι το πραγματικό πρόσωπο κατέχει το αντίστοιχο ψευδώνυμο/ρόλο. Για παράδειγμα, για το ρόλο του «Επόπτη», πρέπει να υπάρχει ένα έγγραφο που να αποδεικνύει ότι το υποκείμενο του πιστοποιητικού δικαιούται αυτό το ρόλο.

Αν οι Πληροφορίες Αναγνώρισης Ταυτότητας του Υποκειμένου πρέπει να περιλαμβάνουν ένα Διακριτικό τίτλο (DBA) ή μια εμπορική επωνυμία, η HARICA θα επαληθεύει το δικαίωμα του Αιτούντα, χρησιμοποιώντας τουλάχιστον μία από τις ακόλουθες μεθόδους:

1. Έγγραφα που παρέχονται από, ή επικοινωνώντας με, Κυβερνητική Οντότητα που έχει την αρμοδιότητα της δημιουργίας νομικής υπόστασης, ή αναγνώρισης του Αιτούντα

2. Μία Αξιόπιστη Πηγή Δεδομένων
3. Επικοινωνία με Κυβερνητική Οντότητα υπεύθυνη για τη διαχείριση τέτοιων ευρέως γνωστών ονομάτων ή επωνυμιών
4. Ένα Έγγραφο Βεβαίωσης που συνοδεύεται από επιπλέον αποδεικτικά τεκμηρίωσης ή
5. Ένας λογαριασμός υπηρεσιών κοινής ωφέλειας, τραπεζική δήλωση, δήλωση πιστωτικής κάρτας, φορολογικό στοιχείο, ή άλλο αξιόπιστο έγγραφο αναγνώρισης ταυτότητας που ορίζει η HARICA.

3.2.2.3 **Επαλήθευση της Χώρας**

Αν υπάρχει το πεδίο του υποκειμένου subject:countryName, η HARICA επαληθεύει τη χώρα που συνδέεται με το υποκείμενο χρησιμοποιώντας ένα από τα παρακάτω:

- την ανάθεση εύρους IP διευθύνσεων ανά χώρα είτε για
  - τη διεύθυνση IP του δικτυακού τόπου, όπως προκύπτει από την εγγραφή DNS για την ιστοσελίδα είτε
  - τη διεύθυνση IP του Αιτούντα,
- το ccTLD του αιτούμενου Ονόματος Χώρου,
- τις πληροφορίες που παρέχονται από τον Καταχωρητή Χώρου Διευθύνσεων, ή
- μια μέθοδο που προσδιορίζεται στις παραγράφους 3.2.2.1 ή 3.2.3.1.

3.2.2.4 **Επιβεβαίωση Κατοχής ή Ελέγχου Ονόματος Χώρου**

Αυτή η παράγραφος ορίζει τις διαδικασίες και πρακτικές που προβλέπονται για την επιβεβαίωση της κατοχής ή του ελέγχου ονόματος χώρου (domain) από τον Αιτούντα.

Η HARICA επιβεβαιώνει ότι, πριν την ημερομηνία έκδοσης Πιστοποιητικού έχει επικυρώσει κάθε Πλήρως Πιστοποιημένο Όνομα Χώρου (FQDN) ως εξής:

1. Όταν ένα FQDN **δεν περιλαμβάνει την τιμή "onion"** στην πιο δεξί όνομα-ετικέτα (label), η HARICA θα επαληθεύσει το FQDN χρησιμοποιώντας τουλάχιστον μία από τις μεθόδους αυτής της παραγράφου, και

Όταν ένα FQDN **περιλαμβάνει την τιμή "onion"** στην πιο δεξί όνομα-ετικέτα (label), η HARICA θα επαληθεύσει το FQDN σύμφωνα με τα οριζόμενα στο

2. ΠΑΡΑΡΤΗΜΑ Ε ΕΚΔΟΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΓΙΑ .ONION DOMAIN NAMES.

Ολοκληρωμένες επιβεβαιώσεις του ελέγχου του FQDN από τον Αιτούντα μπορεί να ισχύουν για την έκδοση πολλών πιστοποιητικών σε βάθος χρόνου. Σε όλες τις περιπτώσεις η επιβεβαίωση πρέπει να έχει ξεκινήσει μέσα στο χρονικό διάστημα που ορίζεται στην παράγραφο 4.2.1, πριν την έκδοση του πιστοποιητικού. Για λόγους ελέγχου εγκυρότητας του χώρου ονομάτων (domain), ο όρος Αιτών περιλαμβάνει τη Μητρική Εταιρεία του Αιτούντα, τη Θυγατρική Εταιρεία, τον Συνεργάτη ή τον ίδιο τον Αιτούντα ως μεμονωμένο Φυσικό Πρόσωπο.

Η HARICA καταγράφει τη μέθοδο ελέγχου που χρησιμοποιείται για κάθε χώρο ονομάτων που ελέγχεται ως προς την εγκυρότητα, συμπεριλαμβανομένης της έκδοσης των “Baseline Requirements” της σύμπραξης CA/B Forum που είναι σε ισχύ όταν πραγματοποιείται ο έλεγχος.

Σημείωση: Τα FQDNs πρέπει να καταγράφονται στα Πιστοποιητικά του Συνδρομητή χρησιμοποιώντας εγγραφές *dNSNames* στην επέκταση *subjectAltName* ή στα Πιστοποιητικά των Υφιστάμενων ΑΠ μέσω εγγραφών *dNSNames* στο πεδίο *permittedSubtrees* στην επέκταση *Name Constraints*.

3.2.2.4.1 Διαδικασία επιβεβαίωσης Αιτούντα ως Επαφή Ονόματος Χώρου

Δεν χρησιμοποιείται.

3.2.2.4.2 Αποστολή Email, Fax, SMS, ή Ταχυδρομικής Αλληλογραφίας στο Επαφή Ονόματος Χώρου

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο του FQDN με αποστολή Τυχαίας Τιμής μέσω email, fax, SMS ή ταχυδρομείου και λήψη επιβεβαιωτικής απάντησης που χρησιμοποιεί την Τυχαία Τιμή. Η Τυχαία Τιμή πρέπει να έχει αποσταλεί σε διεύθυνση email, αριθμό fax/SMS, ή ταχυδρομική διεύθυνση που αντιστοιχεί σε Επαφή Χώρου.

Κάθε email, fax, SMS, ή ταχυδρομική αλληλογραφία μπορεί να επιβεβαιώνει τον έλεγχο για πολλαπλά Ονόματα Χώρου Εξουσιοδότησης.

Η HARICA μπορεί να στέλνει το email, το fax, το SMS ή την ταχυδρομική αλληλογραφία που αναφέρεται σε αυτήν παράγραφο, σε περισσότερους από έναν παραλήπτες υπό την προϋπόθεση ότι κάθε παραλήπτης αναγνωρίζεται από τον Καταχωρητή Ονόματος Χώρου ως εκπρόσωπος Καταχωρίζοντα Ονόματος Χώρου για κάθε FQDN που έχει επαληθευτεί μέσω email, fax, SMS ή ταχυδρομικής αλληλογραφίας.

Η Τυχαία Τιμή είναι μοναδική σε κάθε email, fax, SMS ή ταχυδρομική αλληλογραφία.

Η HARICA μπορεί να στείλει ξανά το email, το fax, το SMS ή την ταχυδρομική αλληλογραφία στο ακέραιο, συμπεριλαμβανομένης της Τυχαίας Τιμής, εφόσον τα στοιχεία επικοινωνίας και ο παραλήπτης(ες) παραμένουν τα ίδια.

Η Τυχαία Τιμή παραμένει έγκυρη για χρήση σε επιβεβαιωτική απάντηση μέχρι τριάντα (30) μέρες από τη δημιουργία της.

Σημείωση: Από τη στιγμή που το FQDN έχει ελεγχθεί για την εγκυρότητά του χρησιμοποιώντας αυτή τη μέθοδο, η HARICA ΜΠΟΡΕΙ επίσης, να εκδίδει Πιστοποιητικά για άλλα FQDN που έχουν κατάληξη τις διάφορες τιμές (labels) του FQDN που έχει ελεγχθεί και είναι έγκυρο. Αυτή η μέθοδος είναι κατάλληλη για έλεγχο εγκυρότητας Ονομάτων Χώρου Μπαλαντέρ.

3.2.2.4.3 Τηλεφωνική επικοινωνία με την Επαφή Ονόματος Χώρου

Δεν χρησιμοποιείται.

3.2.2.4.4 Δομημένο Email σε Επαφή Ονόματος Χώρου

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο του FQDN που περιέχεται στην αίτηση, ως εξής:

1. αποστολή email σε μία ή περισσότερες διευθύνσεις που περιέχουν το πρόθεμα “admin”, “administrator”, “webmaster”, “hostmaster” ή “postmaster”, και ακολουθούνται από το σύμβολο ‘@’ και το Όνομα Χώρου Εξουσιοδότησης (Authorization Domain Name),
2. το οποίο email περιέχει μία Τυχαία Τιμή, και
3. λήψη επιβεβαιωτικής απάντησης στην οποία χρησιμοποιείται η Τυχαία Τιμή.

Κάθε email μπορεί να επιβεβαιώνει πολλά FQDNs, δεδομένου ότι το Όνομα Χώρου Εξουσιοδότησης που χρησιμοποιείται σε καθένα είναι το Όνομα Χώρου Εξουσιοδότησης για κάθε FQDN που έχει επιβεβαιωθεί.

Η Τυχαία Τιμή είναι μοναδική σε κάθε email.

Το email μπορεί να αποσταλεί εκ νέου ακέραιο, με την Τυχαία Τιμή, δεδομένου ότι τα περιεχόμενα και ο παραλήπτης παραμένουν τα ίδια.

Η Τυχαία Τιμή παραμένει έγκυρη για χρήση σε μια επιβεβαιωτική απάντηση έως τριάντα (30) μέρες από τη δημιουργία της.

Σημείωση: Από τη στιγμή που ελέγχεται για την εγκυρότητά του το FQDN με τη χρήση αυτής της μεθόδου, η HARICA ΜΠΟΡΕΙ επίσης, να εκδίδει Πιστοποιητικά για άλλα FQDN που έχουν κατάληξη τις διάφορες τιμές (labels) του FQDN που έχει ελεγχθεί και είναι έγκυρο. Αυτή η μέθοδος είναι κατάλληλη για τον έλεγχο εγκυρότητας Ονομάτων Χώρου Μπαλαντέρ.

3.2.2.4.5 Έγγραφο Ονόματος Χώρου Εξουσιοδότησης

Δεν χρησιμοποιείται

3.2.2.4.6 Συμφωνημένη Αλλαγή σε Ιστοχώρο

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο του FQDN που περιέχεται στην αίτηση με επιβεβαίωση της παρουσίας ενός Τεκμηρίου Αιτήματος ή Τυχαίας Τιμής που περιλαμβάνεται:

1. μέσα σε ένα αρχείο, ή
2. σε μια ιστοσελίδα σε μορφή “meta tag” (όπως ορίζεται στη γλώσσα HTML) α

Αυτό το αρχείο ή ιστοσελίδα πρέπει να είναι προσβάσιμη σε μια διαδρομή κάτω από τον κατάλογο "/.well-known/pki-validation", ή άλλο μονοπάτι καταχωρισμένο στον οργανισμό IANA ειδικά για λόγους Ελέγχου Εγκυρότητας Ονομάτων Χώρου, στο Όνομα Χώρου Εξουσιοδότησης που είναι προσβάσιμο από την HARICA μέσω HTTP/HTTPS πάνω από Εξουσιοδοτημένη Θύρα.

1. Η ύπαρξη του Απαιτούμενου Στοιχείου Ιστοσελίδας στα περιεχόμενα ενός αρχείου της ιστοσελίδας. Όλο το Απαιτούμενο Περιεχόμενο πρέπει να ΜΗΝ εμφανίζεται σε αίτημα που χρησιμοποιείται για να ανακτήσει το αρχείο ή την ιστοσελίδα, ή
2. Η παρουσία του Τεκμηρίου Αιτήματος ή Τυχαίας Τιμής που βρίσκεται στο περιεχόμενο ενός αρχείου όπου το Τεκμήριο Αιτήματος ή η Τυχαία Τιμή πρέπει να ΜΗΝ εμφανίζονται στο αίτημα.

Αν χρησιμοποιείται η Τυχαία Τιμή, η HARICA παρέχει μια Τυχαία Τιμή μοναδική για το αίτημα πιστοποιητικού και δεν χρησιμοποιεί την Τυχαία Τιμή:

(i) Μετά το πέρας των τριάντα (30) ημερών ή
(ii) Αν ο Αιτών υπέβαλε αίτημα πιστοποιητικού, μετά από το επιτρεπόμενο χρονικό διάστημα επαναχρησιμοποίησης της επιβεβαιωμένης πληροφορίας που σχετίζεται με το πιστοποιητικό (όπως ορίζεται στην παράγραφο 4.2.1).

Σημείωση: Αυτή η μέθοδος ΔΕΝ ΕΙΝΑΙ κατάλληλη για τον έλεγχο εγκυρότητας Ονομάτων Χώρου Μπαλαντέρ.

Η HARICA θα σταματήσει να χρησιμοποιεί αυτή τη μέθοδο επαλήθευσης μετά τις 2020-06-03. Η HARICA μπορεί να επαναχρησιμοποιεί πληροφορίες επαλήθευσης για ονόματα χώρου που επαληθεύθηκαν μέσω αυτής της μεθόδου, σύμφωνα με την προβλεπόμενη περίοδο επαναχρησιμοποίησης.

3.2.2.4.7 Αλλαγή στο DNS

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο του FQDN που περιέχεται στην αίτηση με επιβεβαίωση της παρουσίας μίας Τυχαίας Τιμής ή ενός Τεκμηρίου Αιτήματος σε ένα πεδίο CNAME, TXT ή CAA του DNS είτε:

1. του Ονόματος Χώρου Εξουσιοδότησης είτε
2. του Ονόματος Χώρου Εξουσιοδότησης που έχει πρόθεμα με τίτλο που ξεκινά με τον χαρακτήρα της κάτω παύλας (underscore).

Αν χρησιμοποιείται η Τυχαία Τιμή, η HARICA παρέχει μια Τυχαία Τιμή που είναι μοναδική για το αίτημα πιστοποιητικού και δεν χρησιμοποιεί την Τυχαία Τιμή:

(i) μετά από τριάντα (30) μέρες
(ii) Αν ο Αιτών υπέβαλε αίτημα πιστοποιητικού, μετά από το επιτρεπόμενο χρονικό διάστημα επαναχρησιμοποίησης της επαληθευμένης πληροφορίας που σχετίζεται με το πιστοποιητικό (όπως ορίζεται στην παράγραφο 4.2.1).

Σημείωση: Από τη στιγμή που το FQDN ελέγχεται για την εγκυρότητά του με τη χρήση αυτής της μεθόδου, η HARICA ΜΠΟΡΕΙ επίσης να εκδίδει Πιστοποιητικά για άλλα FQDN που έχουν κατάληξη τις διάφορες τιμές (labels) του επαληθευμένου

FQDN. Αυτή η μέθοδος είναι κατάλληλη για τον έλεγχο εγκυρότητας Ονομάτων Χώρου Μπαλαντέρ.

3.2.2.4.8 Διεύθυνση IP

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο του FQDN με επιβεβαίωση ότι ο Αιτών ελέγχει μία διεύθυνση IP που επιστρέφεται από μία αναζήτηση στο DNS για εγγραφές A ή AAAA του FQDN σύμφωνα με την παράγραφο Επαλήθευση ταυτότητας για μία Διεύθυνση IP3.2.2.5.

Σημείωση: Από τη στιγμή που ελέγχεται για την εγκυρότητά του το FQDN με τη χρήση αυτής της μεθόδου, η HARICA ΔΕΝ ΜΠΟΡΕΙ να εκδίδει επίσης Πιστοποιητικά για άλλα FQDNs που έχουν κατάληξη τις διάφορες τιμές (labels) του επιβεβαιωμένου FQDN εκτός αν η HARICA πραγματοποιήσει ξεχωριστή διαδικασία επαλήθευσης για εκείνα τα FQDN με τη χρήση άλλης επιτρεπόμενης μεθόδου σύμφωνα με όσα περιγράφονται στην παράγραφο 3.2.2.4. Η συγκεκριμένη μέθοδος ΔΕΝ είναι κατάλληλη για τον έλεγχο εγκυρότητας Ονομάτων Χώρου Μπαλαντέρ.

3.2.2.4.9 Δοκιμαστικό Πιστοποιητικό

Δεν χρησιμοποιείται

3.2.2.4.10 TLS με χρήση Τυχαίας Τιμής

Αυτή η μέθοδος έχει αποσυρθεί και ΔΕΝ ΠΡΕΠΕΙ να χρησιμοποιείται.

3.2.2.4.11 Οποιαδήποτε Άλλη Μέθοδος

Αυτή η μέθοδος έχει αποσυρθεί και ΔΕΝ ΠΡΕΠΕΙ να χρησιμοποιείται.

3.2.2.4.12 Έλεγχος εγκυρότητας Αιτούντα ως Επαφή Ονόματος Χώρου

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο στο FQDN με επαλήθευση ότι ο Αιτών είναι η Επαφή Χώρου. Αυτή η μέθοδος μπορεί να χρησιμοποιηθεί μόνο αν η HARICA είναι και ο Καταχωρητής Ονόματος Χώρου, ή Συνεργάτης του Καταχωρητή του Ονόματος Χώρου Βάσης.

Σημείωση: Από τη στιγμή που το FQDN έχει ελεγχθεί για την εγκυρότητά του με τη χρήση αυτής της μεθόδου, η HARICA μπορεί να εκδίδει Πιστοποιητικά για άλλα FQDNs που έχουν κατάληξη τις διάφορες τιμές του FQDN που έχει ελεγχθεί και είναι έγκυρο. Αυτή η μέθοδος είναι κατάλληλη για τον έλεγχο εγκυρότητας Ονομάτων Χώρου Μπαλαντέρ.

3.2.2.4.13 Email στην Επαφή DNS CAA

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο του FQDN με αποστολή μίας Τυχαίας Τιμής με μήνυμα ηλεκτρονικού ταχυδρομείου και κατόπιν λήψης μίας επιβεβαιωτικής απάντησης που χρησιμοποιεί την Τυχαία Τιμή. Η Τυχαία Τιμή πρέπει να έχει αποσταλεί σε Email Επαφής DNS CAA. Το σχετικό CAA Resource Record Set ΠΡΕΠΕΙ να βρεθεί χρησιμοποιώντας τον αλγόριθμο αναζήτησης όπως περιγράφεται στο RFC 8659 στην ενότητα 3.

Κάθε email ΜΠΟΡΕΙ να επιβεβαιώνει έλεγχο για πολλά FQDNs, δεδομένου ότι κάθε διεύθυνση email είναι ένα Email Επαφής DNS CAA για κάθε Όνομα Χώρου Εξουσιοδότησης που καλείται να επιβεβαιωθεί. Το ίδιο email ΜΠΟΡΕΙ να σταλεί σε

πολλαπλούς παραλήπτες εφόσον όλοι οι παραλήπτες είναι τα Email Επαφής DNS CAA για κάθε Ονόμα Χώρου Εξουσιοδότησης που καλείται να επιβεβαιωθεί.

Η Τυχαία Τιμή ΕΙΝΑΙ μοναδική σε κάθε email. Το email μπορεί να ξανασταλεί στο ακέραιο του, συμπεριλαμβάνοντας την ίδια Τυχαία Τιμή, με την προϋπόθεση ότι όλο το περιεχόμενο και οι παραλήπτες του παραμένουν αμετάβλητα. Η Τυχαία Τιμή παραμένει έγκυρη για χρήση σε μια επιβεβαιωτική απάντηση έως 30 μέρες από τη δημιουργία της.

Σημείωση: Από τη στιγμή που το FQDN έχει ελεγχθεί για την εγκυρότητά του με τη χρήση αυτής της μεθόδου, η HARICA ΜΠΟΡΕΙ να εκδίδει Πιστοποιητικά για άλλα FQDNs που έχουν κατάληξη τις διάφορες τιμέστου επαληθευμένουFQDN. Αυτή η μέθοδος είναι κατάλληλη για τον έλεγχο εγκυρότητας Ονομάτων Χώρου Μπαλαντέρ.

3.2.2.4.14 Email στην Επαφή DNS TXT

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο του FQDN με αποστολή μίας Τυχαίας Τιμής με μήνυμα ηλεκτρονικού ταχυδρομείου και κατόπιν λήψης μίας επιβεβαιωτικής απάντησης που χρησιμοποιεί την Τυχαία Τιμή. Η Τυχαία Τιμή ΠΡΕΠΕΙ να έχει αποσταλεί σε ένα Email Επαφής DNS TXT για το Όνομα Χώρου Εξουσιοδότησης που επιλέχθηκε να επαληθεύσει το FQDN.

Κάθε email μπορεί να επιβεβαιώνει έλεγχο για πολλά FQDNs, δεδομένου ότι κάθε διεύθυνση email είναι το Email Επαφής DNS TXT για κάθε Εξουσιοδότηση του Ονόματος Χώρου που καλείται να ελεγχθεί. Το ίδιο email ΜΠΟΡΕΙ να σταλεί σε πολλαπλούς παραλήπτες εφόσον όλοι οι παραλήπτες είναι Email Επαφής DNS TXT για κάθε Ονόμα Χώρου Εξουσιοδότησης που καλείται να ελεγχθεί.

Η Τυχαία Τιμή ΕΙΝΑΙ μοναδική σε κάθε email. Το email μπορεί να ξανασταλεί στο ακέραιο του, συμπεριλαμβάνοντας την χρήση της ίδιας Τυχαίας Τιμής, με την προϋπόθεση ότι όλο το περιεχόμενο και οι παραλήπτες του παραμένουν αμετάβλητα. Η Τυχαία Τιμή παραμένει έγκυρη για χρήση σε μια επιβεβαιωτική απάντηση έως 30 μέρες από τη δημιουργία της.

Σημείωση: Από τη στιγμή που το FQDN έχει ελεγχθεί για την εγκυρότητά του με τη χρήση αυτής της μεθόδου, η HARICA ΜΠΟΡΕΙ να εκδίδει Πιστοποιητικά για άλλα FQDNs που έχουν κατάληξη τις διάφορες τιμές του επαληθευμένου FQDN . Αυτή η μέθοδος είναι κατάλληλη για τον έλεγχο εγκυρότητας Ονομάτων Χώρου Μπαλαντέρ.

3.2.2.4.15 Τηλεφωνική επικοινωνία με την Επαφή Χώρου Ονομάτων

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο του FQDN μέσω τηλεφωνικής επικοινωνίας στον αριθμό τηλεφώνου της Επαφής Χώρου Ονομάτων και λήψης επιβεβαιωτικής απόκρισης που επαληθεύει την Εξουσιοδότηση του Χώρου Ονομάτων. Κάθε κλήση ΜΠΟΡΕΙ να επιβεβαιώνει τον έλεγχο πολλαπλών Εξουσιοδοτήσεων Χώρου Ονομάτων με την προϋπόθεση ότι καταγράφεται ο ίδιος αριθμός τηλεφώνου Επαφής Χώρου Ονομάτων για την κάθε Εξουσιοδότηση Χώρου Ονομάτων που καλείται να επιβεβαιωθεί και παρέχεται μία επιβεβαιωτική απάντηση για κάθε Εξουσιοδότηση Χώρου Ονομάτων.

Σε περίπτωση που απαντήσει κάποιος άλλος εκτός της Επαφής Χώρου Ονομάτων, η HARICA μπορεί να ζητήσει να τη μεταβιβάσουν στην Επαφή Χώρου Ονομάτων.

Σε περίπτωση που απαντήσει τηλεφωνητής, η HARICA μπορεί να αφήσει με μήνυμα την Τυχαία Τιμή και την Εξουσιοδότηση Χώρου Ονομάτων που καλείται να επιβεβαιωθεί. Η Τυχαία Τιμή ΠΡΕΠΕΙ να επιστραφεί στη HARICA για να εγκρίνει το αίτημα.

Η Τυχαία Τιμή παραμένει έγκυρη για χρήση σε μια επιβεβαιωτική απάντηση έως τριάντα (30) ημέρες από τη δημιουργία της.

Σημείωση: Από τη στιγμή που το FQDN έχει ελεγχθεί για την εγκυρότητά του με τη χρήση αυτής της μεθόδου, η HARICA ΜΠΟΡΕΙ να εκδίδει Πιστοποιητικά για άλλα FQDNs που τελειώνουν με όλα τα ονόματα του FQDN που έχει ελεγχθεί και είναι έγκυρο. Αυτή η μέθοδος είναι κατάλληλη για τον έλεγχο εγκυρότητας Ονομάτων Χώρου Μπαλαντέρ.

3.2.2.4.16 Τηλεφωνική επικοινωνία στον αριθμό τηλεφώνου της Επαφής DNS TXT

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο του FQDN μέσω κλήσης στον αριθμό τηλεφώνου της Επαφής της εγγραφής DNS TXT και λήψης επιβεβαιωτικής απόκρισης προκειμένου να επαληθευθεί η Εξουσιοδότηση του Χώρου Ονομάτων. Κάθε κλήση ΜΠΟΡΕΙ να επιβεβαιώνει τον έλεγχο πολλαπλών Εξουσιοδοτήσεων Χώρου Ονομάτων με την προϋπόθεση ότι καταγράφεται ο ίδιος αριθμός τηλεφώνου Επαφής της εγγραφής DNS TXT για την κάθε Εξουσιοδότηση Χώρου Ονομάτων που καλείται να επιβεβαιωθεί και παρέχεται μία επιβεβαιωτική απάντηση για κάθε Εξουσιοδότηση Χώρου Ονομάτων.

Η HARICA ΔΕΝ ΜΠΟΡΕΙ να μεταφερθεί εν γνώση της ή να ζητήσει να μεταφερθεί σε άλλο αριθμό τηλεφώνου, καθώς αυτός ο αριθμός τηλεφώνου έχει καταγραφεί αποκλειστικά για σκοπούς Ελέγχου Εγκυρότητας Χώρου Ονομάτων.

Σε περίπτωση που απαντήσει τηλεφωνητής, η HARICA μπορεί να αφήσει με μήνυμα την Τυχαία Τιμή και την Εξουσιοδότηση Χώρου Ονομάτων που καλείται να ελεγχθεί. Η Τυχαία Τιμή ΠΡΕΠΕΙ να επιστραφεί στη HARICA για να εγκριθεί το αίτημα.

Η Τυχαία Τιμή παραμένει έγκυρη για χρήση σε μια επιβεβαιωτική απάντηση έως τριάντα (30) ημέρες από τη δημιουργία της.

Σημείωση: Από τη στιγμή που το FQDN έχει ελεγχθεί για την εγκυρότητά του με τη χρήση αυτής της μεθόδου, η HARICA ΜΠΟΡΕΙ να εκδίδει Πιστοποιητικά για άλλα FQDNs που τελειώνουν με όλα τα ονόματα του FQDN που έχει ελεγχθεί και είναι έγκυρο. Αυτή η μέθοδος είναι κατάλληλη για τον έλεγχο εγκυρότητας Ονομάτων Χώρου Μπαλαντέρ.

3.2.2.4.17 Τηλεφωνική επικοινωνία στον αριθμό τηλεφώνου της Επαφής DNS CAA

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο του FQDN μέσω κλήσης στον αριθμό τηλεφώνου της Επαφής της εγγραφής DNS CAA και λήψης επιβεβαιωτικής απόκρισης προκειμένου να επαληθευθεί η Εξουσιοδότηση του Χώρου Ονομάτων. Κάθε κλήση ΜΠΟΡΕΙ να επιβεβαιώνει τον έλεγχο πολλαπλών Εξουσιοδοτήσεων Χώρου Ονομάτων με την προϋπόθεση ότι καταγράφεται ο ίδιος αριθμός τηλεφώνου Επαφής

της εγγραφής DNS CAA για την κάθε Εξουσιοδότηση Χώρου Ονομάτων που καλείται να επιβεβαιωθεί και παρέχεται μία επιβεβαιωτική απάντηση για κάθε Εξουσιοδότηση Χώρου Ονομάτων. Η σχετική εγγραφή CAA ΠΡΕΠΕΙ να βρίσκεται χρησιμοποιώντας τον αλγόριθμο αναζήτησης όπως περιγράφεται στο RFC 8659 Section 3.

Η HARICA ΔΕΝ ΠΡΕΠΕΙ να μεταφερθεί εν γνώση της ή να ζητήσει να μεταφερθεί σε άλλο αριθμό τηλεφώνου, καθώς αυτός ο αριθμός τηλεφώνου έχει καταγραφεί αποκλειστικά για σκοπούς Ελέγχου Εγκυρότητας Χώρου Ονομάτων.

Σε περίπτωση που απαντήσει τηλεφωνητής, η HARICA μπορεί να αφήσει με μήνυμα την Τυχαία Τιμή και την Εξουσιοδότηση Χώρου Ονομάτων που καλείται να ελεγχθεί. Η Τυχαία Τιμή ΠΡΕΠΕΙ να επιστραφεί στη HARICA για να εγκριθεί το αίτημα.

Η Τυχαία Τιμή παραμένει έγκυρη για χρήση σε μια επιβεβαιωτική απάντηση έως τριάντα (30) ημέρες από τη δημιουργία της.

Σημείωση: Από τη στιγμή που το FQDN έχει ελεγχθεί για την εγκυρότητά του με τη χρήση αυτής της μεθόδου, η HARICA ΜΠΟΡΕΙ να εκδίδει Πιστοποιητικά για άλλα FQDNs που τελειώνουν με όλα τα ονόματα του FQDN που έχει ελεγχθεί και είναι έγκυρο. Αυτή η μέθοδος είναι κατάλληλη για τον έλεγχο εγκυρότητας Ονομάτων Χώρου Μπαλαντέρ.

3.2.2.4.18 Συμφωνημένη Αλλαγή σε Ιστοχώρο v2

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο του FQDN που περιέχεται στην αίτηση με επιβεβαίωση της παρουσίας ενός Τεκμηρίου Αιτήματος ή Τυχαίας Τιμής που περιλαμβάνεται μέσα σε ένα αρχείο.

1. Το πλήρες Τεκμήριο Αιτήματος ή η Τυχαία Τιμή ΔΕΝ ΠΡΕΠΕΙ να εμφανίζεται στο αίτημα που θα γίνει για την ανάκτηση του αρχείου, και
2. Η HARICA ΠΡΕΠΕΙ να λάβει μια HTTP response επιτυχούς συναλλαγής για το συγκεκριμένο αίτημα (δηλαδή πρέπει να ληφθεί μια απάντηση κατάστασης HTTP τύπου 2xx).

Το αρχείο που περιλαμβάνει το Τεκμήριο Αιτήματος ή Τυχαία Τιμή:

1. ΠΡΕΠΕΙ να βρίσκεται σε ένα Χώρο Ονομάτων Εξουσιοδότησης, και
2. ΠΡΕΠΕΙ να βρίσκεται κάτω από τη διαδρομή "/.well-known/pki-validation", και
3. ΠΡΕΠΕΙ να ανακτάται είτε μέσω του "http" ή του "https" σχήματος, και
4. ΠΡΕΠΕΙ να ανακτάται μέσω μιας Εξουσιοδοτημένης Θύρας.

Αν χρησιμοποιείται η Τυχαία Τιμή, τότε

1. Η HARICA παρέχει μια Τυχαία Τιμή μοναδική για το αίτημα πιστοποιητικού
2. Η Τυχαία Τιμή παραμένει έγκυρη για χρήση σε μια επιβεβαιωτική απάντηση έως τριάντα (30) ημέρες από τη δημιουργία της

Σημείωση: Αυτή η μέθοδος ΔΕΝ είναι κατάλληλη για τον έλεγχο εγκυρότητας Ονομάτων Χώρου Μπαλαντέρ.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο του FQDN χρησιμοποιώντας μια μέθοδο “ACME HTTP Challenge” όπως ορίζεται στην ενότητα 8.3 του RFC 8555. Τα παρακάτω είναι επιπλέον απαιτήσεις σε σχέση με το RFC 8555.

Η HARICA πρέπει να λάβει μια επιτυχημένη HTTP απάντηση σε ένα αίτημα (δηλαδή, πρέπει να λάβει μια απάντηση με HTTP status code 2xx).

Το τεκμήριο (token, όπως ορίζεται στην ενότητα 8.3 του RFC 8555), δεν επιτρέπεται να χρησιμοποιηθεί για διάστημα μεγαλύτερο των τριάντα (30) ημερών από τη δημιουργία του.

Η HARICA επιτρέπει τις ανακατευθύνσεις, και ισχύουν τα ακόλουθα:

1. Ανακατευθύνσεις ΠΡΕΠΕΙ να ξεκινούν στο επίπεδο πρωτοκόλλου HTTP (π.χ. με χρήση status code 3xx)
2. Ανακατευθύνσεις ΠΡΕΠΕΙ να είναι το αποτέλεσμα ενός HTTP status code εντός της κλάσης ανακατεύθυνσης 3xx, όπως ορίζεται στην ενότητα 6.4 του RFC 7231
3. Ανακατευθύνσεις ΠΡΕΠΕΙ να είναι για resource URLs είτε για το “http” είτε για το “https” σχήμα
4. Ανακατευθύνσεις ΠΡΕΠΕΙ να είναι για resource URLs μέσω μιας Εξουσιοδοτημένης Θύρας

Σημείωση: Αυτή η μέθοδος ΔΕΝ είναι κατάλληλη για τον έλεγχο εγκυρότητας Ονομάτων Χώρου Μπαλαντέρ.

3.2.2.4.20 TLS Using ALPN

Δεσμευμένο.

3.2.2.5 Επαλήθευση ταυτότητας για μία Διεύθυνση IP

Αυτή η ενότητα ορίζει τις διεργασίες και τις διαδικασίες που επιτρέπονται για τον έλεγχο εγκυρότητας της κατοχής ή του ελέγχου από τον Αιτών μίας Διεύθυνσης IP καταγράφεται σε ένα Πιστοποιητικό.

Η HARICA επιβεβαιώνει ότι, πριν από την έκδοση, κάθε Διεύθυνση IP που καταγράφεται στο Πιστοποιητικό έχει επικυρωθεί χρησιμοποιώντας τουλάχιστον μία από τις μεθόδους που καθορίζονται στην παρούσα ενότητα.

Οι έλεγχοι εγκυρότητας που πραγματοποιήθηκαν αναφορικά με την ευθύνη του Αιτούντα μπορούν να ισχύουν με την πάροδο του χρόνου για την έκδοση πολλαπλών Πιστοποιητικών. Σε όλες τις περιπτώσεις, ο έλεγχος εγκυρότητας πρέπει να έχει ξεκινήσει εντός της χρονικής περιόδου που καθορίζεται στη σχετική απαίτηση (όπως στην παράγραφο 4.2.1 αυτής της ΠΠ/ΔΔΠ) πριν από την έκδοση του Πιστοποιητικού. Για τους σκοπούς ελέγχου εγκυρότητας Διεύθυνσης IP, ο όρος Αιτών συμπεριλαμβάνει τη Μητρική Εταιρεία, τη Θυγατρική Εταιρεία ή Συνεργάτη του Αιτούντα.

Μετά την 31η Ιουλίου 2019, η HARICA διατηρεί ένα πεδίο για τη μέθοδο ελέγχου εγκυρότητας IP που χρησιμοποιήθηκε για κάθε Διεύθυνση IP, συμπεριλαμβανομένου του αντίστοιχου αριθμού έκδοσης BR.

Σημείωση: Οι Διευθύνσεις IP που επαληθεύονται σύμφωνα με αυτήν την ενότητα μπορούν να αναγράφονται στα Πιστοποιητικά Συνδρομητών όπως ορίζεται στην παράγραφο 7.1.4 ή στα Πιστοποιητικά Ενδιάμεσων ΑΠ μέσω του iPAddress στο

permittedSubtrees της επέκτασης Name Constraints. Η HARICA δεν υποχρεούται να επαληθεύει τις Διευθύνσεις IP που παρατίθενται στα Πιστοποιητικά Υφιστάμενων ΑΠ μέσω του iPAddress στο excludedSubtrees της επέκτασης Name Constraints πριν από την προσθήκη στο Πιστοποιητικό Υφιστάμενης ΑΠ.

3.2.2.5.1 Συμφωνημένη Αλλαγή σε Ιστοχώρο

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο της Διεύθυνση IP που περιέχεται στην αίτηση με επιβεβαίωση της παρουσίας ενός Τεκμηρίου Αιτήματος ή Τυχαίας Τιμής που περιλαμβάνεται μέσα σε ένα αρχείο, ή σε μια ιστοσελίδα σε μορφή “meta tag” κάτω από την τοποθεσία "/.well-known/pki-validation", ή άλλη που έχει καταχωρηθεί στον οργανισμό ΙΑΝΑ ειδικά για λόγους ελέγχου εγκυρότητας Διεύθυνσης IP, σε Διεύθυνση IP που είναι προσβάσιμη από την HARICA μέσω HTTP/HTTPS πάνω από Εξουσιοδοτημένη Θύρα.

Αν χρησιμοποιείται η Τυχαία Τιμή, η HARICA παρέχει μια Τυχαία Τιμή μοναδική για το αίτημα πιστοποιητικού και ΔΕΝ χρησιμοποιεί την Τυχαία Τιμή:

(i) μετά το πέρας των τριάντα (30) ημερών ή
(ii) αν ο Αιτών υπέβαλε αίτημα πιστοποιητικού, μετά από το επιτρεπόμενο χρονικό διάστημα επαναχρησιμοποίησης της επιβεβαιωμένης πληροφορίας που σχετίζεται με το πιστοποιητικό (όπως ορίζεται στην παράγραφο 4.2.1 της ΠΠ/ΔΔΠ).

3.2.2.5.2 Αποστολή Email, Fax, SMS, ή Ταχυδρομικής αλληλογραφίας σε Επαφή Διεύθυνσης IP

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο της Διεύθυνσης IP που περιέχεται στην αίτηση με αποστολή μίας Τυχαίας Τιμής μέσω email, fax, SMS ή ταχυδρομείου και κατόπιν λήψης επιβεβαιωτικής απόκρισης που χρησιμοποιεί την Τυχαία Τιμή. Η Τυχαία Τιμή ΠΡΕΠΕΙ να σταλεί στην διεύθυνση email, στον αριθμό fax/SMS ή στην ταχυδρομική διεύθυνση που είναι γνωστή ως Επαφή Διεύθυνσης IP.

Κάθε email, fax, SMS ή ταχυδρομική διεύθυνση ΜΠΟΡΕΙ να επιβεβαιώνει τον έλεγχο πολλαπλών Διευθύνσεων IP.

Η HARICA ΜΠΟΡΕΙ να στείλει το email, το fax, το SMS ή την ταχυδρομική αλληλογραφία που προσδιορίζεται σε αυτήν την ενότητα σε περισσότερους από έναν παραλήπτες, υπό την προϋπόθεση ότι κάθε παραλήπτης αναγνωρίζεται από την Αρχή Καταχώρησης της Διεύθυνσης IP ότι εκπροσωπεί την Επαφή Διεύθυνσης IP για κάθε Διεύθυνση IP που επαληθεύεται χρησιμοποιώντας το email, το fax, το SMS ή την ταχυδρομική αλληλογραφία.

Η Τυχαία Τιμή ΠΡΕΠΕΙ να είναι μοναδική σε κάθε email, fax, SMS ή ταχυδρομική αλληλογραφία.

Η HARICA ΜΠΟΡΕΙ να αποστείλει εκ νέου στο ακέραιο του το email, το fax, το SMS ή την ταχυδρομική αλληλογραφία, συμπεριλαμβανομένης της ίδιας Τυχαίας Τιμής, υπό την προϋπόθεση ότι τα περιεχόμενα και οι παραλήπτες της επικοινωνίας παραμένουν αμετάβλητα.

Η τυχαία τιμή παραμένει έγκυρη για χρήση σε επιβεβαιωτική απάντηση έως τριάντα (30) ημέρες από τη δημιουργία της.

3.2.2.5.3 Αναζήτηση της Διεύθυνσης Reverse IP

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο της Διεύθυνσης IP μέσω ενός Ονόματος Χώρου που σχετίζεται με τη Διεύθυνση IP και προκύπτει από αναζήτηση της reverse-IP για τη Διεύθυνση IP και στη συνέχεια επαληθεύοντας τον έλεγχο του FQDN χρησιμοποιώντας μία επιτρεπόμενη μέθοδο σύμφωνα με την παράγραφο 3.2.2.4.

3.2.2.5.4 Οποιαδήποτε άλλη μέθοδος

Δεν χρησιμοποιείται.

3.2.2.5.5 Τηλεφωνική επικοινωνία με την Επαφή Διεύθυνσης IP

Επιβεβαίωση ότι ο Αιτών έχει τον έλεγχο της Διεύθυνσης IP με κλήση στον αριθμό τηλεφώνου της Επαφής της Διεύθυνσης IP και λήψη απάντησης που επιβεβαιώνει το αίτημα του Αιτούντα για επιβεβαίωση της Διεύθυνσης IP. Η HARICA ΠΡΕΠΕΙ να πραγματοποιήσει την κλήση σε έναν αριθμό τηλεφώνου που αναγνωρίζεται από την Αρχή Καταχώρησης της Διεύθυνσης IP ως Επαφή Διεύθυνσης IP. Κάθε κλήση γίνεται σε έναν αριθμό τηλεφώνου.

Σε περίπτωση που απαντήσει κάποιος άλλος εκτός της Επαφής της Διεύθυνσης IP, η HARICA ΜΠΟΡΕΙ να ζητήσει να μεταβιβασθεί στην Επαφή της Διεύθυνσης IP.

Σε περίπτωση που απαντήσει τηλεφωνητής, η HARICA μπορεί να αφήσει με μήνυμα την Τυχαία Τιμή και την/τις Διεύθυνση/Διευθύνσεις (ες) IP που καλούνται να επιβεβαιωθούν. Η Τυχαία τιμή ΠΡΕΠΕΙ να επιστραφεί στην HARICA για να εγκρίνει το αίτημα.

Η Τυχαία Τιμή ΠΡΕΠΕΙ να παραμείνει έγκυρη για χρήση σε επιβεβαιωτική απάντηση έως τριάντα (30) ημέρες από τη δημιουργία της.

3.2.2.5.6 Μέθοδος ACME “http-01” για Διευθύνσεις IP

Δεσμευμένο.

3.2.2.5.7 Μέθοδος ACME “ tls-alpn-01” για Διευθύνσεις IP

Δεσμευμένο.

3.2.2.6 Έλεγχος εγκυρότητας Ονομάτων Χώρου Μπαλαντέρ

Πριν από την έκδοση πιστοποιητικού με χαρακτήρα μπαλαντέρ (*) στο CN ή στο SubjectAltName της κατηγορίας DNS-ID, η HARICA ακολουθεί μία τεκμηριωμένη διαδικασία που καθορίζει εάν ο χαρακτήρας μπαλαντέρ εμφανίζεται στην πρώτη θέση στα αριστερά ενός ονόματος "ελεγχόμενου από μητρώο" ή "δημόσιου επιθέματος" (π.χ. "* .com", "* .co.uk"). Για να γίνει αυτό διερευνά και συμβουλεύεται μία "λίστα δημόσιων επιθεμάτων" όπως η http://publicsuffix.org/ (PSL).

Εάν ένας χαρακτήρας μπαλαντέρ βρίσκεται ακριβώς αριστερά από ένα όνομα "ελεγχόμενου από μητρώο" ή "δημόσιου επιθέματος", η HARICA αρνείται την έκδοση, εκτός εάν ο αιτών αποδείξει ότι έχει τον νόμιμο έλεγχο όλης της Περιοχής

Χώρου Ονομάτων (π.χ. η HARICA ΔΕΝ εκδίδει για τα "* .co.uk" ή "* .local", αλλά ΜΠΟΡΕΙ να εκδώσει για τα "* .example.com" στο παράδειγμα Co.).

Πιστοποιητικά Μπαλαντέρ δεν επιτρέπονται για Πιστοποιητικά EV SSL/TLS εκτός από ότι ορίζεται στο Παράρτημα F των Οδηγιών EV.

3.2.2.7 **Ακρίβεια Πηγής δεδομένων**

Πριν από τη χρήση οποιασδήποτε πηγής δεδομένων ως Αξιόπιστη Πηγή Δεδομένων, η HARICA αξιολογεί την πηγή για την αξιοπιστία της, την ακρίβεια και την αντοχή της σε παραποίηση ή πλαστογράφηση. Η HARICA εξετάζει τα ακόλουθα κριτήρια για την απόφασή της εάν θα πρέπει ή όχι να αποδέχεται πληροφορίες από μία Πηγή Δεδομένων:

1. Η παλαιότητα των πληροφοριών που παρέχονται,
2. Η συχνότητα των ενημερώσεων της πηγής πληροφοριών,
3. Ο πάροχος δεδομένων και ο σκοπός της συλλογής δεδομένων,
4. Η δυνατότητα πρόσβασης του κοινού σχετικά με τη διαθεσιμότητα των δεδομένων, και
5. Η σχετική δυσκολία στην παραποίηση ή τροποποίηση των δεδομένων.

Η HARICA χρησιμοποιεί Επίσημες Υπηρεσίες Καταλόγου Ακαδημαϊκών / Ερευνητικών Φορέων για να επαληθεύσει τις ταυτότητες και τους ρόλους μέσα στην Ακαδημαϊκή / Ερευνητική κοινότητα.

Από 1 Οκτωβρίου 2020, η HARICA θα εξασφαλίσει ότι, πριν την αξιοποίηση ενός Incorporating Agency ή Registration Agency για απαιτήσεις επαλήθευσης δεδομένων, οι πηγές δεδομένων των Incorporating Agency ή Registration Agency που θα χρησιμοποιούνται για EV Πιστοποιητικά θα έχουν δημοσιευθεί στο αποθετήριο που περιγράφεται στην ενότητα 2.1.

Οι πληροφορίες κάθε Agency θα περιλαμβάνουν τουλάχιστον τα ακόλουθα:

- Ικανή πληροφορία για να αναγνωριστεί αναμφίσημα το Incorporating Agency ή Registration Agency (όπως το όνομα, περιοχή δικαιοδοσίας και ιστοχώρος),
- Την αποδεκτή ή αποδεκτές τιμές για κάθε ένα από τα πεδία `subject:jurisdictionLocalityName` (OID: 1.3.6.1.4.1.311.60.2.1.1), `subject:jurisdictionStateOrProvinceName` (OID: 1.3.6.1.4.1.311.60.2.1.2), και `subject:jursidictionCountryName` (OID: 1.3.6.1.4.1.311.60.2.1.3), όταν ένα πιστοποιητικό EV εκδίδεται χρησιμοποιώντας πληροφορία από το συγκεκριμένο Incorporating Agency ή Registration Agency, εμφανίζοντας την περιοχή (ή περιοχές) δικαιοδοσίας όπου το Agency είναι κατάλληλο,
- Το ιστορικό αλλαγών αυτής της πληροφορίας, χρησιμοποιώντας ένα μοναδικό αριθμό έκδοσης και ημερομηνία δημοσίευσης για κάθε προσθήκη, αλλαγή ή/και αφαίρεση από τη συγκεκριμένη λίστα.

3.2.2.7.1 Εγκεκριμένη Ανεξάρτητη Πηγή Πληροφοριών

Μία Εγκεκριμένη Ανεξάρτητη Πηγή Πληροφοριών (ΕΑΠΠ) είναι μία συστηματικά ενημερωμένη και δημόσια διαθέσιμη βάση δεδομένων που γενικά αναγνωρίζεται ως

αξιόπιστη πηγή βασικών πληροφοριών. Μία βάση δεδομένων πληροί τις προϋποθέσεις ως ΕΑΠΠ αν η HARICA καθορίζει ότι:

1. Οι Επιχειρήσεις εκτός του κλάδου των πιστοποιητικών βασίζονται στη βάση δεδομένων για την ακριβή τοποθεσία, τα στοιχεία επικοινωνίας και άλλες πληροφορίες, και
2. Ο πάροχος της βάσης δεδομένων ενημερώνει τα δεδομένα του σε τουλάχιστον ετήσια βάση.

Η HARICA χρησιμοποιεί μία τεκμηριωμένη διαδικασία για να ελέγξει την ακρίβεια της βάσης δεδομένων και εξασφαλίζει ότι τα δεδομένα αυτής είναι αποδεκτά, συμπεριλαμβανομένου του ελέγχου των όρων χρήσης του παρόχου της βάσης δεδομένων. Η HARICA ΔΕΝ χρησιμοποιεί κανένα στοιχείο της ΕΑΠΠ που γνωρίζει ότι είναι (i) αυτο-δηλούμενο και (ii) δεν έχει επαληθευτεί από την ΕΑΠΠ για την ακρίβειά του. Βάσεις δεδομένων στις οποίες η HARICA ή οι ιδιοκτήτες της ή θυγατρικές εταιρείες διατηρούν πλειοψηφικό έλεγχο, ή στις οποίες οι όποιες Αρχές Καταχώρησης ή οι υπεργολάβοι, όπου η HARICA έχει αναθέσει τμήμα της διαδικασίας εξέτασης (ή οι ιδιοκτήτες τους ή θυγατρικές εταιρείες) διατηρούν οποιαδήποτε κυριότητα ή ωφέλιμο συμφέρον, δεν πληρούν τις προϋποθέσεις ως ΕΑΠΠ.

3.2.2.7.2 Εγκεκριμένη Κρατική Πηγή Πληροφοριών

Μία Εγκεκριμένη Κρατική Πηγή Πληροφοριών (ΕΚΠΠ) είναι μία συστηματικά ενημερωμένη και δημόσια διαθέσιμη βάση δεδομένων που έχει σχεδιαστεί να παρέχει με ακρίβεια τις πληροφορίες για τις οποίες κάποιος τη συμβουλεύεται, και η οποία αναγνωρίζεται γενικά ως αξιόπιστη πηγή αυτών των πληροφοριών με την προϋπόθεση ότι συντηρείται από έναν Κρατικό Φορέα, η διαδικασία αναφοράς των δεδομένων ορίζεται από το νόμο και η ψευδή ή παραπλανητική αναφορά δεδομένων τιμωρείται με ποινικές ή αστικές κυρώσεις. Η χρήση τρίτων προμηθευτών για την απόκτηση των πληροφοριών από τον Κρατικό Φορέα επιτρέπεται, υπό την προϋπόθεση ότι ο τρίτος προμηθευτής λαμβάνει τις πληροφορίες απευθείας από τον Κρατικό Φορέα.

3.2.2.7.3 Εγκεκριμένη Κρατική Πηγή Φορολογικών Στοιχείων

Μία Εγκεκριμένη Κρατική Πηγή Φορολογικών Στοιχείων είναι μία Εγκεκριμένη Κρατική Πηγή Πληροφοριών που περιέχει φορολογικά στοιχεία που σχετίζονται με Ιδιωτικούς Οργανισμούς, Επιχειρήσεις ή Φυσικά Πρόσωπα. (π.χ. το TAXIS στην Ελλάδα, το IRS στις Η.Π.Α.).

3.2.2.8 **Εγγραφές CAA**

Η HARICA πρέπει να ελέγχει για DNS εγγραφές τύπου CAA για κάθε dNSName στην επέκταση subjectAltName του πιστοποιητικού που πρόκειται να εκδοθεί, σύμφωνα με τη διαδικασία που περιγράφεται στο RFC 8659. Αν η HARICA αποφασίσει να εκδώσει ένα πιστοποιητικό εξυπηρετητή που περιλαμβάνει ένα dNSName, ΠΡΕΠΕΙ να το κάνει μέσα στη διάρκεια ζωής (TTL) του πεδίου CAA, ή σε 8 ώρες, όποιο είναι μεγαλύτερο

Όταν η HARICA επεξεργάζεται μία εγγραφή CAA, πρέπει να επεξεργάζεται τα property tags “issue”, “issuewild” και “iodef” όπως ορίζεται στο RFC 8659, αλλά δεν υποχρεούται να προχωρά σε ενέργειες με βάση το property tag “iodef”. Επιπρόσθετα property tags ΜΠΟΡΕΙ να υποστηρίζονται αλλά ΔΕΝ ΠΡΕΠΕΙ να αντικρούονται με τα υποχρεωτικά property tags ή να τα αντικαθιστούν όπως ορίζεται σε αυτό το έγγραφο. Η HARICA σέβεται το flag “critical” στην εγγραφή CAA και δεν εκδίδει

πιστοποιητικό αν δεν γνωρίζει πώς να χειριστεί ένα property tag που θα έχει το συγκεκριμένο flag.

Η HARICA ΜΠΟΡΕΙ να αντιμετωπίζει ένα CAA RR set που δεν είναι κενό και το οποίο δεν περιλαμβάνει κανένα είδος property tag του τύπου "issue" (και επίσης δεν περιλαμβάνει property tags "issuewild" όταν γίνεται έλεγχος CAA για Όνομα Χώρου Μπαλαντέρ) ως άδεια για να εκδώσει, δεδομένου ότι άλλες εγγραφές στο CAA RR set δεν απαγορεύουν την έκδοση.

Ο έλεγχος του CAA είναι προαιρετικός:

- για πιστοποιητικά για τα οποία έχουν εκδοθεί pre-certificates σύμφωνα με τη Διαφάνεια Πιστοποιητικών και είναι καταγεγραμμένα σε δύο τουλάχιστον δημόσια προσβάσιμους εξυπηρετητές καταγραφής CT, για τα οποία έχει πραγματοποιηθεί ο έλεγχος CAA
- για πιστοποιητικά που έχουν εκδοθεί από μία Τεχνικά Περιορισμένη Ενδιάμεση ΑΠ όπως καταγράφεται στην παράγραφο 7.1.5, όπου η μη υποχρέωση ελέγχου CAA ορίζεται ρητά σε συμφωνητικό με τον Αιτούντα.
- αν ένας Συνεργάτης της HARICA είναι ο Διαχειριστής DNS (όπως ορίζεται στο RFC 7719) της Υπηρεσίας Ονομάτων Χώρου (DNS) του Ονόματος Χώρου.

3.2.3 Επαλήθευση ταυτότητας φυσικού προσώπου

Αν ένας Αιτών είναι φυσικό πρόσωπο, η HARICA ΕΠΑΛΗΘΕΥΕΙ το όνομα του Αιτούντα, τη διεύθυνσή του και τη γνησιότητα του αιτήματος πιστοποιητικού.

Όταν ένα Πιστοποιητικό έχει δυνατότητα να χρησιμοποιηθεί για ψηφιακή υπογραφή ή κρυπτογράφηση μηνυμάτων email (Πιστοποιητικά S/MIME), η HARICA θα λάβει πρόνοια να επαληθεύσει ότι ο Αιτούμενος ελέγχει την διεύθυνση email που σχετίζεται με την διεύθυνση email που βρίσκεται μέσα στο πιστοποιητικό *ή* έχει εξουσιοδοτηθεί από τον δικαιούχο του λογαριασμού email για να τον εκπροσωπήσει. Η HARICA ελέγχει αυτή τη κατοχή:

α) ζητώντας από τον Αιτούμενο να συμπληρώσει την διεύθυνση email σε μια φόρμα αιτήματος πιστοποιητικού. Στη συνέχεια στέλνεται ένα email επιβεβαίωσης στη διεύθυνση αυτή μαζί με μια Τυχαία Τιμή. Όταν ο Αιτούμενος επιστρέψει την Τυχαία Τιμή πίσω στη HARICA, η διεύθυνση email θεωρείται επιβεβαιωμένη, ή

β) ζητώντας από τον Αιτούμενο να επιβεβαιώσει έλεγχο ή κατοχή του domain μέρους της email διεύθυνσης (domain portion) ως Ονόματος Χώρου Εξουσιοδότησης χρησιμοποιώντας κάποια από τις αποδεκτές μεθόδους ελέγχου όπως περιγράφονται στην ενότητα 3.2.2.4.

Η HARICA μπορεί να βασισθεί σε επαληθεύσεις που πραγματοποιήθηκαν σε Εξουσιοδοτημένα Ονόματα Χώρου ως έγκυρα για υποκείμενα Ονόματα Χώρου (subdomains), χρησιμοποιώντας τις μεθόδους ελέγχου κατοχής ονομάτων χώρου που περιγράφονται στην ενότητα 3.2.2.4.

3.2.3.1 Πρόσωπο που αιτείται πιστοποιητικό χρήστη

Όλα τα πιστοποιητικά φυσικών προσώπων που εκδίδονται από την 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 Εγκεκριμένης Διάταξης Δημιουργίας Υπογραφής (ΕΔΔΥ) και εκδίδονται παρουσία εξουσιοδοτημένου προσωπικού της Αρχής Καταχώρισης που επιβεβαιώνει ότι το ιδιωτικό κλειδί δημιουργήθηκε στην ΕΔΔΥ.

Πιθανά Αναγνωριστικά Πολιτικών για Πιστοποιητικά Class A είναι:

- NCP+
- QCP-n-qscd
- QCP-l-qscd
- QCP-l-psd2-qscd
- Code Signing
- EV Code Signing

Η κλάση Β, αφορά πιστοποιητικά των οποίων το ιδιωτικό κλειδί δημιουργείται με χρήση κάποιου λογισμικού. Πιθανά Αναγνωριστικά Πολιτικών για Πιστοποιητικά «Class B» είναι:

- LCP
- NCP
- QCP-n
- QCP-l
- QCP-l-psd2

Η Κεντρική Αρχή Καταχώρισης μπορεί να βασίζεται σε συνεργαζόμενα Ιδρύματα για τον έλεγχο ταυτότητας που γίνεται για Αιτούντες που σχετίζονται με τα Ελληνικά Ακαδημαϊκά και Ερευνητικά Ιδρύματα. Αυτά τα Ιδρύματα ενεργούν ως Εταιρικές ΑΚ και χρησιμοποιούν ασφαλείς μεθόδους για να επαληθεύουν την ταυτότητα των Αιτούντων. Οι συνεργαζόμενες μονάδες είναι υποχρεωμένες να έχουν πιστοποιήσει την ταυτότητα του χρήστη με φυσική παρουσία, χρησιμοποιώντας κάποιο επίσημο έγγραφο που φέρει τη φωτογραφία του δικαιούχου (π.χ. αστυνομική ταυτότητα, διαβατήριο, δίπλωμα οδήγησης). Εναλλακτικά, η ίδια η ΑΚ κάθε ιδρύματος μπορεί να εκτελέσει την παραπάνω διαδικασία ταυτοποίησης του Αιτούντος για κάθε αίτημα προσωπικού πιστοποιητικού.

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 email) 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 τις παρακάτω μεθόδους ελέγχου πιστοποίησης της κυριότητας μίας διεύθυνσης email:

i. Απλή επιβεβαίωση μέσω email. Ο Αιτών εισάγει τη διεύθυνση email στην αρχική φόρμα αιτήσεως για πιστοποιητικό και αποστέλλεται στη διεύθυνση αυτή ένα μήνυμα επιβεβαίωσης με ένα σύνδεσμο σε μοναδική ιστοσελίδα. Μετά την επίσκεψη αυτού του συνδέσμου, αποστέλλεται ένα email στον εξουσιοδοτημένο “Validator” του αντίστοιχου Ιδρύματος που απαιτεί έγκριση με βάση το ονοματεπώνυμο που συμπλήρωσε ο Αιτών και τη διεύθυνση email του. Αυτή η έγκριση απαιτεί την ταυτοποίηση του χρήστη με την φυσική του παρουσία και την επίδειξη επίσημου αποδεικτικού

ταυτότητας. Αν αυτή η διαδικασία έγινε παλιότερα (π.χ. κατά τη δημιουργία του λογαριασμού email) δεν υπάρχει λόγος να επαναληφθεί.

ii. Εξυπηρετητής LDAP. Ο Αιτών εισάγει την ιδρυματική διεύθυνση email και τον αντίστοιχο κωδικό στην αίτηση πιστοποιητικού. Οι πληροφορίες επαληθεύονται μέσω του ιδρυματικού εξυπηρετητή LDAP. Εφόσον είναι αληθείς, αντλείται το ονοματεπώνυμο του αιτούντα από τον ιδρυματικό κατάλογο LDAP και υποβάλλεται η αίτηση πιστοποιητικού. 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.

iii. Single Sign On (SSO) που βασίζεται στο πρότυπο SAML. Ο Αιτών δίνει το ιδρυματικό email του σε ειδική ιστοσελίδα και στη συνέχεια ανακατευθύνεται στην ιστοσελίδα του Παρόχου Ταυτοποίησης του οικείου Ιδρύματος. Ο Πάροχος Ταυτοποίησης επαληθεύει τον αιτούντα κι επιστρέφει το ονοματεπώνυμο και τη διεύθυνση email του Αιτούντα. 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.

iv. Φυσική παρουσία. Εάν ένα άτομο αδυνατεί να χρησιμοποιήσει τις προηγούμενες μεθόδους, αυτός/αυτή μπορεί να εμφανιστεί στην ΑΚ. Η ΑΚ πρέπει να ελέγχει το όνομα του Αιτούντα, τη διεύθυνση και την αυθεντικότητα της αίτησης πιστοποιητικού. Η HARICA επαληθεύει το όνομα του Αιτούντα, χρησιμοποιώντας τουλάχιστον ένα ευανάγνωστο αντίγραφο επίσημου αποδεικτικού ταυτότητας (διαβατήριο, δίπλωμα οδήγησης, ακαδημαϊκή ταυτότητα, εθνική ταυτότητα ή άλλο αντίστοιχο δημόσιο έγγραφο) το οποίο δείχνει ευδιάκριτα το πρόσωπο του Αιτούντα. Η HARICA ελέγχει το αντίγραφο για οποιαδήποτε ένδειξη αλλοίωσης ή παραποίησης. Η HARICA επαληθεύει τη διεύθυνση του Αιτούντα, χρησιμοποιώντας ένα αξιόπιστο έγγραφο ταυτοποίησης, όπως μια αστυνομική ταυτότητα, λογαριασμό κοινής ωφελείας, δήλωση τραπεζικού λογαριασμού ή πιστωτικής κάρτας. Η HARICA επαληθεύει την κατοχή διεύθυνσης ηλεκτρονικού ταχυδρομείου εφαρμόζοντας διαδικασία πρόκλησης - απόκρισης σύμφωνα με τη μέθοδο "Απλή επιβεβαίωση μέσω email " (i) που αναφέρθηκε παραπάνω.

Τα πιστοποιητικά κλάσης Α συνίσταται να περιέχουν ένα επιπλέον πεδίο οργανωτικής μονάδας (OU) στο πεδίο του υποκειμένου με τιμή ”Class A – Private Key created and stored in hardware CSP”. Επιπλέον, όσον αφορά τα Πιστοποιητικά για Εγκεκριμένες ηλεκτρονικές υπογραφές/σφραγίδες, αυτά πρέπει να περιέχουν το αναγνωριστικό (OID) id-etsi-qcs-QcSSCD στην επέκταση qcStatements. Τα πιστοποιητικά κλάσης Α, πληρούν τους όρους και προϋποθέσεις του Ευρωπαϊκού Κανονισμού 2014/910 σε ό,τι αφορά τις Εγκεκριμένες Διατάξεις Δημιουργίας Υπογραφής (ΕΔΔΥ).

Τα πιστοποιητικά κλάσης Β συνίσταται να περιέχουν ένα επιπλέον πεδίο οργανωτικής μονάδας (OU) στο πεδίο του υποκειμένου με τιμή “Class B – Private Key created and stored in software CSP”.
Ειδικά για την έκδοση Εγκεκριμένων Πιστοποιητικών σύμφωνα με τον Κανονισμό (ΕΕ) 2014/910, η εξακρίβωση της ταυτότητας φυσικών ή νομικών προσώπων θα γίνεται σύμφωνα με τις διατάξεις του Άρθρου 24, παράγραφος 1 του Κανονισμού. Σήμερα η HARICA χρησιμοποιεί τις μεθόδους εξακρίβωσης (α), (β) και (γ) από τη συγκεκριμένη παράγραφο.

3.2.3.2 Πρόσωπο που αιτείται πιστοποιητικό συσκευής

Ένας Αιτών που ελέγχει τη λειτουργία μιας συσκευής/εξυπηρετητή, πρέπει να έχει στην κατοχή του πιστοποιητικό που εκδόθηκε από την HARICA ή το όνομα χρήστη/κωδικό πρόσβασης που απέκτησε κατά την αρχική εγγραφή.

Ο Αιτών υποβάλλει την αίτηση για πιστοποιητικό συσκευής σε ασφαλή ιστοσελίδα όπου ταυτοποιείται παρουσιάζοντας είτε το προσωπικό πιστοποιητικό του ή το συνδυασμό ονόματος χρήστη/κωδικού πρόσβασης.

Η Κεντρική Αρχή Καταχώρησης της HARICA επαληθεύει τον έλεγχο κυριότητας της πιστοποιούμενης συσκευής. Για πιστοποιητικά SSL/TLS που χρησιμοποιούνται για ονόματα χώρου που ανήκουν σε Ακαδημαϊκά / Εκπαιδευτικά ιδρύματα, αποστέλλεται ένα μήνυμα email σε εξουσιοδοτημένο Διαχειριστή της ΥΔΚ του Ιδρύματος ο οποίος ελέγχει το FQDN του αιτήματος αν είναι έγκυρο. Ο διαχειριστής δικτύου του Ιδρύματος επίσης, επαληθεύει αν ο χρήστης που αιτείται το πιστοποιητικό είναι διαχειριστής του συγκεκριμένου εξυπηρετητή που χρησιμοποιεί το FQDN μέσω του μητρώου χρηστών/υπολογιστών που τηρείται στο ίδρυμα.

Επιπλέον με την προαναφερόμενη διαδικασία, η Κεντρική ΑΚ της HARICA ακολουθεί τις μεθόδους επαλήθευσης που αναφέρθηκαν στην παράγραφο 3.2.2.4.

3.2.4 Μη επιβεβαιωμένα στοιχεία του συνδρομητή

Τα πιστοποιητικά που εκδίδονται δεν περιλαμβάνουν μη επιβεβαιωμένα στοιχεία του συνδρομητή. Η HARICA μπορεί να συμπεριλάβει κάποιες πληροφορίες στο πεδίο OU για να υποδείξει κάποιες αξιόπιστες πληροφορίες (για παράδειγμα, το κείμενο που δείχνει πως ένα ιδιωτικό κλειδί αντιστοιχεί στο πιστοποιητικό που έχει δημιουργηθεί σε ΕΔΔΥ).

3.2.5 Επιβεβαίωση της Εξουσιοδότησης

Η Κεντρική ΑΚ της HARICA ακολουθεί διαδικασία για να καθορίσει τα εξουσιοδοτημένα πρόσωπα που μπορούν να ζητήσουν πιστοποιητικά για λογαριασμό ενός οργανισμού. Κάθε οργανισμός μπορεί να περιορίσει τους εξουσιοδοτημένους αιτούντες για πιστοποιητικό.

Οι Αρχές Καταχώρισης διαθέτουν διαδικασίες με τις οποίες επαληθεύεται η σχέση κάθε Αιτούντα με το ίδρυμα και η κατάσταση αυτής. Αυτό γίνεται είτε με ηλεκτρονικές λίστες που συγκεντρώνει η κάθε ΑΚ από τις αρμόδιες -για κάθε κατηγορία- πηγές (π.χ. γραμματείες τμημάτων/σχολών, δ/νση μηχανοργάνωσης διοίκησης κ.α.), είτε με προσκόμιση επικυρωμένων έγγραφων βεβαιώσεων όπου πιστοποιείται η σχέση του ενδιαφερόμενου με το ίδρυμα.

Η HARICA χρησιμοποιεί πληροφορίες από πηγές δεδομένων σύμφωνα με την παράγραφο 3.2.2.7 για τη δημιουργία μιας αξιόπιστης μεθόδου επικοινωνίας.

Για αιτήματα Πιστοποιητικών με Εκτεταμένο Έλεγχο εγκυρότητας (είτε EV SSL/TLS είτε Υπογραφής Κώδικα EV), η HARICA ακολουθεί τις διαδικασίες που περιγράφονται στην ενότητα 11.8 των Οδηγιών EV για να επιβεβαιώσει την αρμοδιότητα για το αίτημα.

3.2.6 Κριτήρια για διαλειτουργικότητα

Η HARICA μπορεί να εκδίδει πιστοποιητικά δια-πιστοποίησης, προκειμένου να βοηθήσει τις διεργασίες μετάβασης σε νέα Κεντρική ΑΠ. Η HARICA παρέχει επίσης, υπηρεσίες δια-πιστοποίησης για να δια-πιστοποιήσει μια ΑΠ που δεν ανήκει στην HARICA. Για να παρέχονται αυτές οι υπηρεσίες, πρέπει να ισχύουν τα ακόλουθα κριτήρια:

- Η περίοδος διασύνδεσης περιορίζεται το μέγιστο στα οκτώ (8) χρόνια με δικαίωμα ανανέωσης
- Ο φορέας που θα δια-πιστοποιηθεί, θα υπογράψει συμβόλαιο με τη HARICA που θα περιλαμβάνει «δικαίωμα ελέγχου» από την HARICA προς τον φορέα και
- Η ΑΠ πρέπει να λειτουργεί σύμφωνα με μία ΠΠ/ΔΔΠ που είναι τουλάχιστον όσο αυστηρό είναι και η ΠΠ/ΔΔΠ της HARICA.

3.3 Επαλήθευση ταυτότητας για επανέκδοση πιστοποιητικών με νέο κλειδί

Με τον όρο επανέκδοση πιστοποιητικού με νέο κλειδί, περιγράφεται η δημιουργία νέου πιστοποιητικού, που χρησιμοποιεί ένα μέρος ή όλες τις πληροφορίες που υπάρχουν για ένα ισχύον πιστοποιητικό χρησιμοποιώντας ένα νέο Ζεύγος Κλειδιού. Οι Συνδρομητές μπορούν να ζητούν επανέκδοση πιστοποιητικού μόνο πριν τη λήξη του. Η διαδικασία επανέκδοσης περιγράφεται στην ενότητα 4.7.

3.3.1 Επαλήθευση ταυτότητας και εξουσιοδότηση για αίτηση έκδοσης νέου κλειδιού-πιστοποιητικού

Ο Συνδρομητής μπορεί να αιτηθεί την επανέκδοση για ένα πιστοποιητικό που δεν έχει λήξει και δεν έχει ανακληθεί, οποιαδήποτε στιγμή πριν την λήξη του, ακολουθώντας τη διαδικασία που περιγράφεται στην παράγραφο 3.2.

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

Ο Συνδρομητής μπορεί να αιτηθεί την επανέκδοση αμέσως μετά την ανάκληση του αρχικού πιστοποιητικού του, ακολουθώντας την διαδικασία που περιγράφεται στην παράγραφο 3.2.

3.4 Επαλήθευση ταυτότητας και εξουσιοδότηση για αιτήματα ανάκλησης

Η HARICA μπορεί να ανακαλεί οποιοδήποτε πιστοποιητικό (Πιστοποιητικό Ενδιάμεσης ΑΠ ή Πιστοποιητικό χρήστη/συσκευής) κατά την απόλυτη διακριτική της ευχέρεια.

Η επαλήθευση ταυτότητας κι εξουσιοδότηση για αιτήματα ανάκλησης γίνονται σύμφωνα με τις μεθόδους που περιγράφονται στην παράγραφο 3.2.3. Επιπλέον, η HARICA και ο Συνδρομητής, κατά την παραλαβή του πιστοποιητικού, συμφωνούν σε ένα μυστικό κωδικό ανάκλησης του πιστοποιητικού, ο οποίος είναι απαραίτητος για την ανάκληση του πιστοποιητικού από το Συνδρομητή.

Κρατικές αρχές επαληθεύονται μέσω ασφαλούς κλήσης στους επίσημους αριθμούς τηλεφώνου τους ή στις επίσημες διευθύνσεις ηλεκτρονικού ταχυδρομείου.

Η πλήρης διαδικασία ανάκλησης περιγράφεται στην παράγραφο 4.9.3.

3.4.1 Αίτημα ανάκλησης από Εκδούσα Αρχή

Η Εκδούσα ΑΠ οφείλει να ανακαλεί πιστοποιητικά εφόσον έχει ισχυρές ενδείξεις ότι το ιδιωτικό κλειδί ή το πιστοποιητικό κάποιου Συνδρομητή έχει διαρρεύσει. Μπορεί επίσης, να ανακαλέσει ένα πιστοποιητικό χωρίς τη συγκατάθεση του Συνδρομητή αν έχει εκδοθεί με λάθος παραμέτρους/πληροφορίες. Για την ειδική περίπτωση των Εγκεκριμένων Πιστοποιητικών, η ανάκληση γίνεται:

- μετά από αίτημα της Εποπτεύουσας Αρχής
- αν κατά τη διαδικασία ελέγχου/επιθεώρησης βρεθεί ότι περιέχει λάθος ή ανακριβείς πληροφορίες
- αν υπάρχει σχετική δικαστική απόφαση
- αν παραβιάζεται η Εθνική και Ευρωπαϊκή Νομοθεσία.

3.4.2 Αίτημα ανάκλησης από Συνδρομητή

Ο Συνδρομητής μπορεί να αιτηθεί την ανάκληση του πιστοποιητικού μέσω ασφαλούς ιστοσελίδας της HARICA, με τη χρήση εγκεκριμένων μεθόδων ταυτοποίησης ή με την χρήση του μυστικού κωδικού ανάκλησης. Εναλλακτικά, ο Συνδρομητής μπορεί να ζητήσει ανάκληση πιστοποιητικού με τηλεφωνική επικοινωνία στην αντίστοιχη ΑΠ και κατά τη διαδικασία αυτή πρέπει να γίνει επαλήθευση της ταυτότητάς του βάσει πληροφοριών που είναι γνωστές μεταξύ Αρχής Καταχώρισης και Συνδρομητή.

3.4.3 Αίτημα ανάκλησης από μη-Συνδρομητή

Αιτήματα Ανάκλησης Πιστοποιητικών από μη-Συνδρομητές που αιτούνται ανάκληση ενός πιστοποιητικού της HARICA, πρέπει να γίνονται σύμφωνα με τις διαδικασίες που περιγράφονται στην παράγραφο 4.9.3.2

4 Λειτουργικές Απαιτήσεις Κύκλου ζωής Πιστοποιητικού

4.1 Αίτηση για Πιστοποιητικό

4.1.1 Ποιος δικαιούται να καταθέσει αίτηση για πιστοποιητικό

Αιτήσεις για έκδοση πιστοποιητικού μπορούν να καταθέσουν μόνο οι Αιτούντες που περιγράφονται στην παράγραφο 1.3.3. Η HARICA χαρακτηρίζει όλα τα ανακλημένα και/ή απορριφθέντα αιτήματα πιστοποιητικών και μπορεί να χρησιμοποιήσει αυτή την πληροφορία για να αναγνωρίσει επόμενες αιτήσεις πιστοποιητικών που θεωρούνται ύποπτες.

Η HARICA ενδέχεται να αξιοποιεί τη μηχανή Google Safe Browsing για ανίχνευση ύποπτων ιστοχώρων, προκειμένου να αποτρέψει έκδοση πιστοποιητικών για τα αντίστοιχα Ονόματα Χώρου.

Η HARICA εκδίδει Πιστοποιητικά QCP-w, QCP-w-psd2, EV SSL και Υπογραφής Κώδικα EV σε Αιτούντες μόνο εφόσον υποβάλλουν ένα πλήρες Αίτημα Πιστοποιητικού και πληρούν τις απαιτήσεις που ορίζονται στις παραγράφους 8.5 και 10.2 των Οδηγιών EV, επιπλέον των απαιτήσεων που ορίζονται σε αυτή την ΠΠ/ΔΔΠ.

4.1.2 Διαδικασία ένταξης και ευθύνες

Πριν την έκδοση ενός Πιστοποιητικού, η HARICA λαμβάνει την ακόλουθη τεκμηρίωση από τον Αιτούντα:

1. Μία αίτηση για πιστοποιητικό, η οποία μπορεί να είναι ηλεκτρονική και
2. Μία υπογεγραμμένη Σύμβαση Συνδρομητή ή αποδοχή Όρων Χρήσης, που μπορεί να διατίθενται ηλεκτρονικά.

Ένα αίτημα για πιστοποιητικό μπορεί να είναι αρκετό για πολλά Πιστοποιητικά που πρέπει να εκδοθούν στον ίδιο Αιτούντα που υπόκειται στους χρονικούς περιορισμούς και τους περιορισμούς επαναχρησιμοποίησης υφιστάμενων τεκμηρίων όπως περιγράφεται στην παράγραφο 4.2.1, υπό την προϋπόθεση ότι κάθε Πιστοποιητικό υποστηρίζεται από ένα έγκυρο, ισχύον αίτημα για πιστοποιητικό που υπογράφηκε από τον κατάλληλο Εκπρόσωπο Αιτούντα εκ μέρους του Αιτούντα. Το αίτημα για πιστοποιητικό μπορεί να έχει γίνει, να έχει υποβληθεί και /ή να έχει υπογραφεί ηλεκτρονικά.

Η αίτηση πιστοποιητικού πρέπει να περιλαμβάνει δήλωση του Αιτούντα, ή του Εκπροσώπου του Αιτούντα, ότι όλες οι πληροφορίες είναι ορθές.

Οι Αιτούντες μπορούν να υποβάλουν την αίτηση για έκδοση του πιστοποιητικού στην ασφαλή ιστοσελίδα https://app.harica.gr/, https://cm.harica.gr ή στην Αρχή Καταχώρισης του οικείου ιδρύματος, ή σε Αρχή Καταχώρισης Εξουσιοδοτημένου Τρίτου Εταίρου, ή στην Κεντρική Αρχή Καταχώρισης. Η διαδικασία αίτησης θα έχει ως αποτέλεσμα την ασφαλή υποβολή ενός κατάλληλα διαμορφωμένου Αιτήματος Υπογραφής Πιστοποιητικού (CSR) και τεκμήρια εξακρίβωσης ταυτότητας τα οποία στη συνέχεια ελέγχονται από Ειδικό Ελέγχου Εγκυρότητας.

4.1.2.1 Διαδικασία ένταξης για EV Πιστοποιητικά

Οι παρακάτω ρόλοι Αιτούντα είναι απαραίτητοι για την έκδοση πιστοποιητικού EV.

1. **Αιτών πιστοποιητικού**: Το Αίτημα EV Πιστοποιητικού πρέπει να υποβληθεί από εξουσιοδοτημένο Αιτούντα Πιστοποιητικού. Ο Αιτών Πιστοποιητικού είναι φυσικό πρόσωπο που είναι είτε ο Αιτών, είτε εργάζεται στον αιτούντα, είτε είναι ένας εξουσιοδοτημένος αντιπρόσωπος που έχει ρητή εξουσιοδότηση να εκπροσωπεί τον Αιτούντα, ή κάποιος τρίτος (όπως ένας ISP ή μία εταιρεία παροχής υπηρεσίας φιλοξενίας) που συμπληρώνει και υποβάλλει το Αίτημα EV Πιστοποιητικού εξ ονόματος του Αιτούντος.
2. **Υπεύθυνος Έγκρισης Πιστοποιητικού**. Το Αίτημα EV Πιστοποιητικού πρέπει να εγκριθεί από εξουσιοδοτημένο Υπεύθυνο Έγκρισης Πιστοποιητικού. Ο Υπεύθυνος Έγκρισης Πιστοποιητικού είναι ένα φυσικό πρόσωπο που είναι είτε ο Αιτών, είτε εργάζεται στον αιτούντα, είτε είναι ένας εξουσιοδοτημένος αντιπρόσωπος που έχει ρητή εξουσιοδότηση να εκπροσωπεί τον Αιτούντα (i) να ενεργεί ως Αιτών Πιστοποιητικού και να εξουσιοδοτεί άλλους υπαλλήλους ή τρίτους να ενεργούν ως Αιτούντες Πιστοποιητικού, και (ii) να εγκρίνουν τα Αιτήματα EV Πιστοποιητικών που υποβάλλονται από άλλους Αιτούντες Πιστοποιητικών.
3. **Υπογράφων Σύμβασης**: Η Σύμβαση Συνδρομητή που ισχύει για το αιτούμενο EV Πιστοποιητικό πρέπει να υπογράφεται από εξουσιοδοτημένο Υπογράφοντα Σύμβασης. Ο Υπογράφων Σύμβασης είναι φυσικό πρόσωπο, το οποίο είναι είτε ο Αιτών, είτε εργάζεται στον Αιτούντα, είτε είναι ο εξουσιοδοτημένος αντιπρόσωπος που έχει ρητή εξουσιοδότηση να εκπροσωπεί τον Αιτούντα και ο οποίος έχει την αρμοδιότητα εξ ονόματος του Αιτούντος να υπογράψει Συμβάσεις Συνδρομητή.
4. **Αντιπρόσωπος Αιτούντα**: Σε περίπτωση που η HARICA και ο Συνδρομητής συνεργάζονται, οι Όροι Χρήσης που ισχύουν για το αιτούμενο EV Πιστοποιητικό πρέπει να αναγνωρίζονται και να συμφωνούνται από εξουσιοδοτημένο Αντιπρόσωπο Αιτούντος. Ο Αντιπρόσωπος Αιτούντος είναι ένα φυσικό πρόσωπο που είναι είτε ο Αιτών, είτε εργάζεται στον Αιτούντα, είτε είναι ο εξουσιοδοτημένος αντιπρόσωπος που έχει ρητή εξουσιοδότηση να εκπροσωπεί τον Αιτούντα και ο οποίος έχει την αρμοδιότητα εξ ονόματος του Αιτούντα να αναγνωρίσει και να συμφωνήσει με τους Όρους Χρήσης.

Ο Αιτών μπορεί να εξουσιοδοτήσει ένα πρόσωπο να έχει δύο ή περισσότερους από αυτούς τους ρόλους και / ή να επιτρέψει σε περισσότερα από ένα άτομα να έχουν οποιονδήποτε από αυτούς τους ρόλους.

4.2 Επεξεργασία Αίτησης Πιστοποιητικού

4.2.1 Διαδικασίες εξακρίβωσης ταυτότητας Συνδρομητή

Η επεξεργασία των αιτήσεων βασίζεται σε όσα αναγράφονται στην παράγραφο 3.2. Όλα τα αιτήματα πρέπει να ελέγχονται ως προς την εγκυρότητά τους.

Η παράγραφος 6.3.2 περιορίζει την διάρκεια ισχύος των Πιστοποιητικών Συνδρομητή. Η HARICA μπορεί να χρησιμοποιεί έγγραφα και δεδομένα που αναφέρονται στην παράγραφο 3.2 για να επαληθεύσει τις πληροφορίες του πιστοποιητικού ή μπορεί να επαναχρησιμοποιήσει προηγούμενες επαληθεύσεις, δεδομένου ότι απέκτησε αυτά τα στοιχεία ή έγγραφα από πηγή που ορίζεται στην παράγραφο 3.2 ή ολοκλήρωσε την επαλήθευση, όχι πριν από οκτακόσιες εικοσιπέντε (825) ημέρες από την έκδοση του Πιστοποιητικού.

Από 2021-04-01, ειδικά για τα δεδομένα επαλήθευσης Domain Name ή Διεύθυνση IP τα οποία αποκτήθηκαν ως τεκμήρια βάσει των ενοτήτων 3.2.2.4, 3.2.2.5 και ΠΑΡΑΡΤΗΜΑ Ε ΕΚΔΟΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΓΙΑ .ONION DOMAIN NAMES, η HARICA μπορεί να επαναχρησιμοποιήσει προηγούμενα δεδομένα επαλήθευσης μέχρι **τριακόσιες ενενήντα επτά (397) ημέρες** πριν την έκδοση του Πιστοποιητικού.

Για τα Πιστοποιητικά EV, εκτός από την περίπτωση της επανέκδοσης Πιστοποιητικού EV σύμφωνα με την ενότητα 11.14.2 των Οδηγιών EV και εκτός εάν επιτρέπεται διαφορετικά στην ενότητα 11.14.1 των Οδηγιών EV, η παλαιότητα όλων των στοιχείων που χρησιμοποιήθηκαν προκειμένου να εκδοθεί ένα EV πιστοποιητικό (πριν απαιτηθεί επανέλεγχος) ΔΕΝ υπερβαίνει τα ακόλουθα όρια:

(Α) Νομική ισχύ και ταυτότητα - **δεκατρείς (13) μήνες**.
(Β) Φερόμενο όνομα - **δεκατρείς (13) μήνες**.
(Γ) Διεύθυνση του Τόπου Επιχείρησης - **δεκατρείς (13) μήνες**.
(Δ) Επαληθευμένη Μέθοδος Επικοινωνίας - **δεκατρείς (13) μήνες**.
(Ε) Λειτουργική ισχύ - **δεκατρείς (13) μήνες**.
(Στ) Όνομα Χώρου - **δεκατρείς (13) μήνες**.
(Ζ) Ονοματεπώνυμο, Τίτλος, Οργανισμός και Αρχή - **δεκατρείς (13) μήνες,**

εκτός εάν η σύμβαση μεταξύ της HARICA και του Αιτούντα ορίζει έναν διαφορετικό όρο, στην περίπτωση που ο όρος ορίζεται στους ελέγχους της σύμβασης. Για παράδειγμα, η σύμβαση ΜΠΟΡΕΙ να περιλαμβάνει τη διαρκή ανάθεση των ρόλων EV έως ότου ανακληθεί από τον Αιτούντα ή τη HARICA ή έως ότου λήξει ή τερματιστεί η σύμβαση.

Η προθεσμία των δεκατριών μηνών που αναφέρεται παραπάνω ξεκινά από την ημερομηνία συλλογής των στοιχείων από τη HARICA.

Η HARICA ΜΠΟΡΕΙ να χρησιμοποιήσει ξανά ένα Αίτημα Πιστοποιητικού EV που έχει υποβληθεί, τη Σύμβαση Συνδρομητή ή τους Όρους Χρήσης, συμπεριλαμβανομένης της μοναδικής Αίτησης Πιστοποιητικού EV για την υποστήριξη πολλαπλών Πιστοποιητικών EV που περιέχουν το ίδιο Subject, στο βαθμό που επιτρέπεται από τις ενότητες 11.9 και 11.10 των Οδηγιών EV.

Η HARICA ΠΡΕΠΕΙ να επαναλάβει τη διαδικασία επαλήθευσης για τυχόν πληροφορίες που αποκτήθηκαν εκτός των χρονικών ορίων που καθορίζονται παραπάνω, εκτός εάν επιτρέπεται διαφορετικά σύμφωνα με την ενότητα 11.14.1 των Οδηγιών EV.

Σε καμία περίπτωση δεν μπορεί να επανα-χρησιμοποιηθεί έλεγχος εγκυρότητας που είχε προηγηθεί, αν έχει παρέλθει το επιτρεπόμενο χρονικό διάστημα επαναχρησιμοποίησης πληροφορίας ή εγγράφων που χρησιμοποιήθηκαν σε παλαιότερο έλεγχο εγκυρότητας για την έκδοση Πιστοποιητικού.

4.2.2 Έγκριση ή απόρριψη αιτήσεων πιστοποιητικών

Μετά από όλους τους ελέγχους ταυτότητας και των υπόλοιπων στοιχείων του Αιτούντα, ελέγχεται και το περιεχόμενο της αίτησης για ψηφιακό πιστοποιητικό. Σε περίπτωση που ο Αιτών δεν δικαιούται ψηφιακό πιστοποιητικό ή η αίτηση περιέχει σφάλματα, η αίτηση απορρίπτεται.

Η HARICA θα απορρίπτει αιτήσεις για Πιστοποιητικά σε περίπτωση που τα υποχρεωτικά βήματα επαλήθευσης δεν μπορούν να ολοκληρωθούν επιτυχώς.

Η HARICA μπορεί να απορρίψει μία αίτηση για οποιοδήποτε πιστοποιητικό του οποίου η έκδοση μπορεί να βλάψει, να υποβαθμίσει ή να έχει αρνητική επίδραση με οιονδήποτε τρόπο στην ίδια τη HARICA, συμπεριλαμβανόμενων των Βασιζόμενων Μερών.

Η HARICA δεν θα εκδώσει νέα Πιστοποιητικά Υπογραφής Κώδικα ούτε θα αντικαταστήσει, για μια οντότητα που θεωρεί ότι σκόπιμα υπέγραψε Ύποπτο Κώδικα. Η HARICA διατηρεί τα μετα-δεδομένα που αφορούν το λόγο ανάκλησης Πιστοποιητικού Υπογραφής Κώδικα, ως απόδειξη ότι το Πιστοποιητικό Υπογραφής Κώδικα ανακλήθηκε επειδή ο Αιτών σκόπιμα υπέγραφε ύποπτο κώδικα.

Εγκρίνονται αιτήσεις πιστοποιητικού που είναι σύμφωνες με τα κριτήρια του αιτούμενου πιστοποιητικού, οι οποίες επαληθεύτηκαν κι επικυρώθηκαν επιτυχώς.

Συνδρομητές που ζητούν ή χρησιμοποιούν Πιστοποιητικά Υπογραφής Κώδικα πρέπει να παρακολουθούν τις απαιτήσεις της δημιουργίας Ιδιωτικού Κλειδιού και της προστασίας του όπως ορίζεται στην παράγραφο 6.2.1.

Τα αιτήματα Πιστοποιητικών EV απαιτούν έγκριση από τουλάχιστον δύο (2) διαφορετικούς Ειδικούς Ελέγχου Εγκυρότητας. Ο δεύτερος Ειδικός Ελέγχου Εγκυρότητας ζητά πρόσθετη τεκμηρίωση ή / και επαλήθευση πριν εγκρίνει την έκδοση Πιστοποιητικού EV. Σε καμία περίπτωση δεν ελέγχεται ως προς την εγκυρότητα, εγκρίνεται ή εκδίδεται EV πιστοποιητικό από ένα άτομο. Δείτε επίσης την ενότητα 5.2.4.

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 ελέγχει τις εγγραφές CAA σύμφωνα με το RFC 6844 πριν εκδώσει Πιστοποιητικά Συνδρομητών για χρήση SSL/TLS ή Πιστοποιητικά Υφιστάμενων ΑΠ που μπορούν να εκδίδουν Πιστοποιητικά Συνδρομητών για χρήση SSL/TLS, εκτός από τις προαιρετικές περιπτώσεις τις παραγράφου 3.2.2.8.

Οι Συνδρομητές που επιθυμούν να εξουσιοδοτήσουν την HARICA να εκδίδει Πιστοποιητικά για τα δικά τους FQDNs θα πρέπει να συμπεριλάβουν στην δική τους αντίστοιχη ζώνη DNS μια εγγραφή CAA “issue” ή “issuewild” με τιμή “**harica.gr**”.

Οι Συνδρομητές που έχουν ήδη εγγραφές CAA στη δική τους ζώνη DNS και χρειάζονται ένα Πιστοποιητικό από την HARICA πρέπει να προσθέσουν μία εγγραφή CAA “issue” ή “issuewild”, με τιμή “**harica.gr**”.

4.3 Έκδοση πιστοποιητικών

4.3.1 Διαδικασίες Αρχών Πιστοποίησης κατά την έκδοση Πιστοποιητικών

Τα πιστοποιητικά Συνδρομητών δημοσιεύονται μετά την επιτυχή επαλήθευση των περιεχομένων του Πιστοποιητικού από τον Συνδρομητή.

Η έκδοση Πιστοποιητικού από Κορυφαία ΑΠ απαιτεί ένα εξουσιοδοτημένο πρόσωπο (δηλαδή ο διαχειριστής του συστήματος της ΑΠ, υπάλληλος ή διαχειριστής της ΥΔΚ) να δώσει ρητά και με εσκεμμένα εντολή στην Κορυφαία ΑΠ να προχωρήσει σε υπογραφή πιστοποιητικού.

Η HARICA δημοσιεύει όλα τα Πιστοποιητικά των Υφιστάμενων ΑΠ μέσω του επίσημου αποθετηρίου της και αποθετηρίων που παρέχονται από Προμηθευτές Λογισμικού Εφαρμογών.

Αναφορικά με τα Πιστοποιητικά SSL/TLS που απαιτείται να τα εμπιστεύονται συγκεκριμένοι Πάροχοι Λογισμικού, η HARICA μπορεί να καταγράφει στοιχεία που αφορούν αυτά τα πιστοποιητικά σε τουλάχιστον δύο εξυπηρετητές καταγραφής στοιχείων (log servers) Διαφάνειας Πιστοποιητικού. Αυτοί οι εξυπηρετητές καταγραφής πρέπει να είναι πιστοποιημένοι και να έχουν χαρακτηριστεί «αξιόπιστοι» από τους συγκεκριμένους Παρόχους Λογισμικού.

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

Η HARICA ενημερώνει τον Αιτούντα για την αποδοχή ή απόρριψη της Αίτησης Πιστοποιητικού μέσω ηλεκτρονικού ταχυδρομείου.

4.4 Αποδοχή Πιστοποιητικού

4.4.1 Δεοντολογία που διέπει τη διαδικασία αποδοχής πιστοποιητικού

Οι Αιτούντες πρέπει να αποδεχθούν (να παραλάβουν και να εγκαταστήσουν μέσω ασφαλούς ιστοσελίδας) το νέο τους πιστοποιητικό μέσα σε **τριάντα (30) ημέρες**, διαφορετικά, το Πιστοποιητικό ανακαλείται και ο Αιτών πρέπει να κάνει εκ νέου αίτηση. Οι Αιτούντες, προτείνεται να επιβεβαιώνουν ότι έχουν ελέγξει όλα τα στοιχεία του πιστοποιητικού και ότι είναι αυτά είναι ορθά, προκειμένου να παραλάβουν το πιστοποιητικό τους. Τέλος, πρέπει να αποδέχονται τους όρους και προϋποθέσεις της παρούσας ΠΠ/ΔΔΠ, και κατόπιν παραλαμβάνουν το πιστοποιητικό και γίνονται Συνδρομητές.

4.4.2 Δημοσίευση πιστοποιητικού από την ΑΠ

Όλες οι ΑΠ δημοσιεύουν τα πιστοποιητικά μόνο εφόσον έχει γίνει η αποδοχή τους από τους Αιτούντες σύμφωνα με την παράγραφο 4.4.1.

4.4.3 Ενημέρωση άλλων οντοτήτων για την έκδοση πιστοποιητικού από την ΑΠ

Δεν προβλέπεται ενημέρωση άλλων οντοτήτων για τα νέα πιστοποιητικά πέραν των όσων περιγράφονται στην παράγραφο 4.3.1.

4.5 Ζεύγος Κλειδιών και Χρήση Πιστοποιητικού

4.5.1 Χρήση ιδιωτικού κλειδιού και πιστοποιητικού Συνδρομητή

Οι Συνδρομητές επιτρέπεται να χρησιμοποιούν τα ιδιωτικά κλειδιά και τα πιστοποιητικά τους για χρήσεις που περιγράφονται στην παράγραφο 6.1.7. Πρέπει επίσης, να ακολουθούν τις Εγγυήσεις Συνδρομητή όπως περιγράφονται στην παράγραφο 9.6.3, ειδικά αυτές που σχετίζονται με την «Προστασία του Ιδιωτικού Κλειδιού» και τη «Χρήση του Πιστοποιητικού».

4.5.2 Χρήση του δημόσιου κλειδιού και πιστοποιητικού από Βασιζόμενα Μέρη

Τα Βασιζόμενα μέρη μπορούν να χρησιμοποιούν τα δημόσια κλειδιά και τα πιστοποιητικά των Συνδρομητών ακολουθώντας τα όσα αναγράφονται στην παράγραφο 1.3.4. Οι λειτουργίες που μπορούν να εκτελέσουν (η λίστα αυτή δεν είναι περιοριστική) είναι:

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

4.6 Ανανέωση πιστοποιητικού

4.6.1 Συνθήκες κατά τις οποίες μπορεί να γίνει ανανέωση πιστοποιητικού

Η ανανέωση Πιστοποιητικού επιτρέπεται όταν πλησιάζει η λήξη ενός μη ανακληθέντος πιστοποιητικού. Ορισμένα πιστοποιητικά μπορούν να ανανεωθούν με χρήση του ίδιου ζεύγους κλειδιού εφόσον δεν έχει ξεπεραστεί το χρονικό όριο ισχύος των κλειδιών που συνοδεύουν τα πιστοποιητικά. Επιπλέον, 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

Ο Συνδρομητής που επιθυμεί ανανέωση μέσω ασφαλούς ιστοσελίδας της HARICA, καταθέτει το αίτημα ανανέωσης μετά από τον κατάλληλο έλεγχο ταυτότητας. Συνιστάται οι Συνδρομητές 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.

4.6.3 Επεξεργασία αιτημάτων ανανέωσης πιστοποιητικού

- 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 Συνδρομητή όπως για παράδειγμα το ονοματεπώνυμο ή το email, αλλάξουν, ακολουθούνται διαδικασίες έκδοσης νέου πιστοποιητικού.
- Για το υπόλοιπο επιτρεπόμενο χρονικό διάστημα εκδίδεται νέο πιστοποιητικό χρησιμοποιώντας το αρχικό certificate request (CSR) που βρίσκεται αποθηκευμένο στην Αρχή Καταχώρισης.

Για παράδειγμα, ένας Συνδρομητής 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 πάνω από ένα έτος (σύμφωνα με την ενότητα 6.3.2). Αν ο Συνδρομητής ανακαλέσει ένα Πιστοποιητικό με λόγο ανάκλησης `keyCompromise`, το Δημόσιο Κλειδί που σχετίζεται με αυτό το Πιστοποιητικό δεν μπορεί να χρησιμοποιηθεί ξανά σε νέα Αίτηση Πιστοποιητικού.

4.6.4 Ενημέρωση Συνδρομητή για έκδοση νέου πιστοποιητικού

Ακολουθείται η διαδικασία που περιγράφεται στην παράγραφο 4.3.2.

4.6.5 Δεοντολογία που διέπει την αποδοχή ανανεωμένου πιστοποιητικού

Ακολουθείται η διαδικασία που περιγράφεται στην παράγραφο 4.4.1.

4.6.6 Δημοσίευση του ανανεωμένου πιστοποιητικού από την ΑΠ

Ακολουθείται η διαδικασία που περιγράφεται στην παράγραφο 4.4.2.

4.6.7 Ενημέρωση άλλων οντοτήτων για την έκδοση πιστοποιητικού

Ακολουθείται η διαδικασία που περιγράφεται στην παράγραφο 4.4.3.

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. Επιπλέον, ισχύουν όλα όσα αναφέρονται στην παράγραφο 1.3.3. Λόγοι αλλαγής κλειδιών μπορεί να είναι (η λίστα δεν είναι περιοριστική):

- Διαπίστωση ευπάθειας στον αλγόριθμο δημιουργίας κλειδιού ή στο μέγεθος του κλειδιού
- Απώλεια ή παραβίαση ή υποψία για παραβίαση ιδιωτικού κλειδιού
- Αμφισβήτηση του αλγορίθμου δημιουργίας κλειδιού ή του μεγέθους του κλειδιού

4.7.2 Ποιος μπορεί να αιτηθεί πιστοποίηση νέου δημόσιου κλειδιού

Οι Συνδρομητές έχουν τη δυνατότητα να καταθέτουν αίτημα αλλαγής κλειδιών πιστοποιητικού μέσω ασφαλούς ιστοσελίδας μετά από κατάλληλο έλεγχο ταυτότητας. Το προηγούμενο πιστοποιητικό συνήθως ανακαλείται.

4.7.3 Διαδικασίες για αιτήματα αλλαγής κλειδιών

Ακολουθείται η διαδικασία που περιγράφεται στην παράγραφο 4.3.

4.7.4 Ενημέρωση Συνδρομητή για τα πιστοποιητικό στο οποίο πραγματοποιήθηκε αλλαγή κλειδιού

Ακολουθείται η διαδικασία που περιγράφεται στην παράγραφο 4.3.2.

4.7.5 Δεοντολογία που διέπει την διαδικασία αποδοχής πιστοποιητικού στο οποίο έγινε αλλαγή κλειδιού

Ακολουθείται η διαδικασία που περιγράφεται στην παράγραφο 4.4.1.

4.7.6 Δημοσίευση πιστοποιητικών στα οποία έγινε αλλαγή κλειδιού από την ΑΠ

Ακολουθείται η διαδικασία που περιγράφεται στην παράγραφο 4.4.2.

4.7.7 Ενημέρωση από την ΑΠ άλλων οντοτήτων για την έκδοση πιστοποιητικών με νέο κλειδί

Ακολουθείται η διαδικασία που περιγράφεται στην παράγραφο 4.4.3.

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 για αιτήματα μεταβολής πιστοποιητικών

Μεταβολή στοιχείων πιστοποιητικών δεν επιτρέπεται.

4.8.4 Ενημέρωση Συνδρομητή για το νέο πιστοποιητικά που μεταβλήθηκε

Μεταβολή στοιχείων πιστοποιητικών δεν επιτρέπεται.

4.8.5 Δεοντολογία που διέπει τη διαδικασία αποδοχή πιστοποιητικών που μεταβλήθηκαν

Μεταβολή στοιχείων πιστοποιητικών δεν επιτρέπεται.

4.8.6 Δημοσίευση πιστοποιητικών που μεταβλήθηκαν από την ΑΠ

Μεταβολή στοιχείων πιστοποιητικών δεν επιτρέπεται.

4.8.7 Ενημέρωση από την ΑΠ άλλων οντοτήτων για την έκδοση πιστοποιητικών που μεταβλήθηκαν

Μεταβολή στοιχείων πιστοποιητικών δεν επιτρέπεται.

4.9 Αναστολή και ανάκληση πιστοποιητικών

4.9.1 Συνθήκες για ανάκληση

4.9.1.1 Λόγοι για την Ανάκληση Πιστοποιητικού Συνδρομητή

Ένα πιστοποιητικό ανακαλείται όταν τα στοιχεία που περιέχει έχουν αλλάξει ή υπάρχει υποψία ότι έχει εκτεθεί ή χαθεί το ιδιωτικό κλειδί ή υπάρχει υποψία ότι έχει εκτεθεί ή χαθεί. Στην τελευταία περίπτωση, όλα τα πιστοποιητικά που περιλαμβάνουν το Δημόσιο Κλειδί που αντιστοιχεί στο Ιδιωτικό Κλειδί που έχει παραβιαστεί ανακαλούνται από την HARICA και το Δημόσιο Κλειδί δεν μπορεί να χρησιμοποιηθεί ξανά σε Αίτηση Υπογραφής Πιστοποιητικού.

Επίσης, το πιστοποιητικό 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 την παρούσα ΠΠ/ΔΔΠ. Τέλος, ανακαλείται εάν το πιστοποιητικό περιέχει λανθασμένες πληροφορίες.

Η HARICA πρέπει να ανακαλεί οποιοδήποτε Πιστοποιητικό Συνδρομητή μέσα σε είκοσι τέσσερεις (24) ώρες, εάν συμβεί ένα ή περισσότερα από τα ακόλουθα:

1. Ο Συνδρομητής αιτείται εγγράφως να ανακληθεί το Πιστοποιητικό από την HARICA.
2. Ο Συνδρομητής ειδοποιεί την HARICA ότι η αρχική αίτηση πιστοποιητικού δεν έχει εγκριθεί και δεν του χορηγήθηκε αναδρομικά η άδεια. Αυτό ισχύει, επίσης, για Εγκεκριμένα Πιστοποιητικά ηλεκτρονικών σφραγίδων όπου υπάρχει κάποια αλλαγή στη Νόμιμη εκπροσώπηση και ο πρώην Νόμιμος εκπρόσωπος δεν είναι εξουσιοδοτημένος πλέον να δημιουργεί Ηλεκτρονικές Σφραγίδες.
3. Η HARICA αποκτά στοιχεία που αποδεικνύουν ότι το Ιδιωτικό Κλειδί του Συνδρομητή που αντιστοιχεί στο Δημόσιο Κλειδί του Πιστοποιητικού υπέστη Παραβίαση.
4. Η HARICA αποκτά στοιχεία που αποδεικνύουν ότι η διαδικασία επιβεβαίωσης κατοχής ή ελέγχου κάποιου FQDN ή Διεύθυνσης IP που περιλαμβάνεται στο Πιστοποιητικό, δεν ήταν αξιόπιστη.

Η HARICA ΜΠΟΡΕΙ να ανακαλεί ένα Πιστοποιητικό Εξυπηρετητή SSL/TLS μέσα σε είκοσι τέσσερεις (24) ώρες και ΠΡΕΠΕΙ να το ανακαλέσει εντός πέντε (5) ημερών, εάν συμβεί ένα ή περισσότερα από τα ακόλουθα:

5. Το Πιστοποιητικό δεν συμμορφώνεται πλέον με τις απαιτήσεις που περιγράφονται στις παραγράφους 6.1.5 και 6.1.6.
6. Η HARICA έχει ενδείξεις ότι το Πιστοποιητικό χρησιμοποιήθηκε καταχρηστικά.
7. Η HARICA αντιλαμβάνεται ότι ο Συνδρομητής έχει παραβιάσει μία ή περισσότερες ουσιώδεις υποχρεώσεις από αυτές που ορίζονται στη Σύμβαση Συνδρομητή ή τους Όρους Χρήσης.
8. Η HARICA έχει ενημερωθεί για οποιαδήποτε περίσταση που δείχνει ότι η χρήση ενός Πλήρους Πιστοποιημένου Ονόματος Χώρου (FQDN) που υπάρχει στο Πιστοποιητικό δεν έχει πλέον νόμιμη άδεια (π.χ. θα μπορούσε να προκύπτει από απόφαση δικαστηρίου ή υπεύθυνου που ανακαλεί το δικαίωμα ενός Καταχωρίζοντα Ονόματος Χώρου να χρησιμοποιεί το Όνομα Χώρου, τη λήξη μιας σχετικής αδειοδότησης ή συμφωνίας παροχής υπηρεσιών μεταξύ του Καταχωρίζοντα Ονόματος Χώρου και του Αιτούντα, ή την αποτυχία του

Καταχωρίζοντα Ονόματος Χώρου να ανανεώσει το Όνομα Χώρου. Ομοίως ισχύει αν το φυσικό πρόσωπο του οποίου οι πληροφορίες περιέχονται στο πεδίο Υποκείμενο του Πιστοποιητικού, δε συνδέονται πλέον με τον οργανισμό που αναφέρεται στο πεδίο «Οργανισμός» του Πιστοποιητικού.

9. Η HARICA έχει ενημερωθεί ότι ένα Πιστοποιητικό «Μπαλαντέρ» έχει χρησιμοποιηθεί για παραπλανητικό FQDN.
10. Η HARICA έχει ενημερωθεί για ουσιώδη αλλαγή στις πληροφορίες που περιέχει το Πιστοποιητικό.
11. Η HARICA έχει ενημερωθεί ότι το Πιστοποιητικό δεν εκδόθηκε σύμφωνα με την παρούσα ΠΠ / ΔΔΠ της HARICA.
12. Η HARICA κρίνει ή έχει ενημερωθεί ότι οποιαδήποτε από τις πληροφορίες που περιλαμβάνονται στο Πιστοποιητικό είναι ανακριβείς.
13. Το δικαίωμα της HARICA να εκδίδει Πιστοποιητικά ακολουθώντας τις παρούσες Απαιτήσεις εξαντλείται ή ανακαλείται ή παύει, εκτός αν η HARICA έχει φροντίσει να συνεχίσει να διατηρεί το Αποθετήριο ΛΑΠ/OCSP.
14. Η Ανάκληση απαιτείται από την Πολιτική Πιστοποίησης και/ή Δήλωση Διαδικασιών Πιστοποίησης της HARICA, ή
15. Η HARICA έχει ενημερωθεί για πρακτικές ή εξακριβωμένες μεθόδους που εκθέτουν το Ιδιωτικό Κλειδί Συνδρομητή, μεθόδους που έχουν αναπτυχθεί και μπορεί με εύκολο τρόπο να υπολογιστεί το Ιδιωτικό Κλειδί με βάση το Δημόσιο Κλειδί (όπως τα ευάλωτα Κλειδιά Debian, βλ. http://wiki.debian.org/SSLkeys), ή υπάρχει σαφής ένδειξη ότι μια συγκεκριμένη μέθοδος δημιουργίας Ιδιωτικού Κλειδιού είναι ελαττωματική.

Η HARICA ΠΡΕΠΕΙ να ανακαλεί ένα Πιστοποιητικό S/MIME εάν συμβεί οποιοδήποτε από τα ακόλουθα γεγονότα:

16. Η HARICA αποκτά ικανοποιητικά στοιχεία ότι το πιστοποιητικό χρησιμοποιήθηκε πέρα από τους σκοπούς που έχουν ορισθεί στο συγκεκριμένο τύπο πιστοποιητικού ή στη Σύμβαση συνδρομητή ή στους Όρους Χρήσης
17. Η HARICA αντιλαμβάνεται ότι ο Συνδρομητής έχει παραβιάσει μία ή περισσότερες ουσιώδεις υποχρεώσεις από αυτές που ορίζονται στη Σύμβαση Συνδρομητή ή τους Όρους Χρήσης
18. Η HARICA έχει ενημερωθεί για οποιαδήποτε περίσταση που δείχνει ότι η χρήση μιας διεύθυνσης email που υπάρχει στο Πιστοποιητικό δεν έχει πλέον νόμιμη άδεια
19. Η HARICA έχει ενημερωθεί για ουσιώδη αλλαγή στις πληροφορίες που περιέχει το Πιστοποιητικό.
20. Η HARICA διαπιστώνει ότι το Πιστοποιητικό δεν εκδόθηκε σύμφωνα με την παρούσα ΠΠ / ΔΔΠ της HARICA.
21. Η HARICA διαπιστώνει ότι οι πληροφορίες που περιέχει το Πιστοποιητικό δεν είναι ακριβείς.

Για Πιστοποιητικά Υπογραφής Κώδικα, οι Συνδρομητές δε θα πρέπει να συμπεριλάβουν εσκεμμένα Ύποπτο Κώδικα στο λογισμικό που υπογράφουν. Εσκεμμένη υπογραφή Ύποπτου Κώδικα σημαίνει παραβίαση της παρούσας ΠΠ/ΔΔΠ. Αν κάποιο Βασιζόμενο Μέρος δώσει την πληροφορία ότι το πιστοποιητικό έχει παραβιαστεί ή έχει χρησιμοποιηθεί για να υπογράψει Ύποπτο Κώδικα, η HARICA διερευνάει το αίτημα και ανακαλεί το Πιστοποιητικό Υπογραφής Κώδικα.

Επιπλέον με τους λόγους που προαναφέρθηκαν, η HARICA ανακαλεί ένα **Εγκεκριμένο Πιστοποιητικό/Σφραγίδα** αν ισχύει κάποιο από τα ακόλουθα:

22. Ο Εθνικός Φορέα Εποπτείας (ΕΕΤΤ), κατά την εκτέλεση των καθηκόντων της, συμπεράνει ότι ένα Εγκεκριμένο Πιστοποιητικό/Σφραγίδα περιέχει λανθασμένες ή ανακριβείς πληροφορίες, μη συμμορφωμένες με τον Κανονισμό eIDAS, ή
23. Η HARICA αναγγέλλει παύση των υπηρεσιών χωρίς διάδοχη λύση, ή
24. Γνωστοποιείται στην HARICA ότι ο Συνδρομητής δεν έχει πλέον δικαίωμα υπογραφής, είναι γνωστό ότι δεν υπάρχει, έχει πεθάνει, λαμβάνοντας υπόψη ότι τα Εγκεκριμένα Πιστοποιητικά για ηλεκτρονικές υπογραφές σε όλες τις περιπτώσεις δεν μεταφέρονται, ή
25. Η HARICA λαμβάνει τελεσίδικη απόφαση δικαστηρίου που δίνει την εντολή στην HARICA να ανακαλέσει το Εγκεκριμένο Πιστοποιητικό/Σφραγίδα, ή
26. Η HARICA διαθέτει ενδείξεις ότι το Ιδιωτικό Κλειδί που αντιστοιχεί σε ένα Εγκεκριμένο Πιστοποιητικό/Σφραγίδα έχει παραβιαστεί και έχει χρησιμοποιηθεί από τρίτο που δεν έχει καμία σχέση με τον Συνδρομητή.

Ειδικά για τα Πιστοποιητικά PSD2, η HARICA ακολουθεί τις διατάξεις της παραγράφου 6.2.6 του προτύπου ETSI TS 119 495 και ανακαλεί το πιστοποιητικό εφόσον το ζητήσει η Αρμόδια Εθνική Αρχή ως κάτοχος των συγκεκριμένων πληροφοριών PSD2, εάν

27. έχει ανακληθεί η εξουσιοδότηση του ΠΥΠ,
28. έχει ανακληθεί οποιοσδήποτε ρόλος ΠΥΠ που περιλαμβάνεται στο πιστοποιητικό.

4.9.1.2 Λόγοι για την ανάκληση Πιστοποιητικού Ενδιάμεσης ΑΠ

Η HARICA ανακαλεί ένα Πιστοποιητικό Υφιστάμενης ΑΠ που έχει τεχνικά δυνατότητα έκδοσης Πιστοποιητικών Εξυπηρετητών (SSL/TLS) και υπογραφής κώδικα (Code Signing) μέσα σε επτά (7) ημέρες εάν συμβαίνει ένα ή περισσότερα από τα ακόλουθα:

1. Μια Ενδιάμεση ΑΠ Εξωτερικής Διαχείρισης αιτείται ανάκληση γραπτώς,
2. Μια Ενδιάμεση ΑΠ Εξωτερικής Διαχείρισης γνωστοποιεί στην Εκδούσα ΑΠ ότι το αρχικό αίτημα πιστοποιητικού δεν είχε εγκριθεί και δεν του χορηγήθηκε αναδρομικά η άδεια,
3. Η Εκδούσα ΑΠ διαθέτει στοιχεία ότι το Ιδιωτικό Κλειδί που αντιστοιχεί στο Δημόσιο Κλειδί του Πιστοποιητικού της Ενδιάμεσης ΑΠ έχει εκτεθεί ή δεν συμμορφώνεται πλέον με τις απαιτήσεις της παραγράφου 6.1.5 και 6.1.6.,
4. Η Εκδούσα ΑΠ διαθέτει στοιχεία ότι το Ιδιωτικό Κλειδί που αντιστοιχεί στο Δημόσιο Κλειδί του Πιστοποιητικού της Ενδιάμεσης ΑΠ έχει χρησιμοποιηθεί καταχρηστικά,
5. Γνωστοποιείται στην Εκδούσα ΑΠ ότι το Πιστοποιητικό της Ενδιάμεσης ΑΠ δεν εκδόθηκε σύμφωνα με την τρέχουσα Πολιτική Πιστοποίησης ή Δήλωση Διαδικασιών Πιστοποίησης, ή ότι η Ενδιάμεση ΑΠ Εξωτερικής Διαχείρισης δεν έχει συμμορφωθεί με αυτήν,
6. Η Εκδούσα ΑΠ αποφασίσει ότι οποιαδήποτε πληροφορία που εμφανίζεται στο Πιστοποιητικό της Ενδιάμεσης ΑΠ είναι ανακριβής ή παραπλανητική,
7. Η Εκδούσα ΑΠ ή η Ενδιάμεση ΑΠ σταματά τις λειτουργίες της για οποιονδήποτε λόγο και δεν έχει προβλέψει μια άλλη ΑΠ να παρέχει υποστήριξη σε θέματα ανάκλησης για το Πιστοποιητικό της Ενδιάμεσης ΑΠ,

8. Το δικαίωμα της Εκδούσας ΑΠ ή της Ενδιάμεσης ΑΠ να εκδίδει Πιστοποιητικά σύμφωνα με την παρούσα ΠΠ/ΔΔΠ, λήγει ή ανακαλείται ή παύει, εκτός αν η Εκδούσα ΑΠ έχει προβλέψει να συνεχιστεί η διατήρηση του αποθετηρίου ΛΑΠ/OCSP, ή
9. Η ανάκληση επιβάλλεται από την Πολιτική Πιστοποίησης/Δήλωση Διαδικασιών Πιστοποίησης της Εκδούσας ΑΠ.

Η HARICA θα ανακαλέσει το Πιστοποιητικό Υφιστάμενης ΑΠ που έχει τεχνικά δυνατότητα έκδοσης Πιστοποιητικών για Αυθεντικοποίηση χρήστη (client authentication), ηλεκτρονικό ταχυδρομείο (S/MIME), ηλεκτρονικές υπογραφές και σφραγίδες, αν συμβεί κάποιο από τα παραπάνω γεγονότα.

4.9.2 Ποιος μπορεί να αιτηθεί ανάκληση

Ο Συνδρομητής, η ΑΚ ή η Εκδούσα ΑΠ μπορούν να ξεκινήσουν διαδικασία ανάκλησης. Επιπλέον, Συνδρομητές, Έμπιστα μέρη, Προμηθευτές Λογισμικού και άλλοι τρίτοι συμπεριλαμβανομένων κυβερνητικών αρχών και δικαστηρίων της Ελλάδας και της Ευρωπαϊκής Ένωσης, μπορούν να υποβάλουν Αναφορές Προβλημάτων Πιστοποιητικών ενημερώνοντας την Εκδούσα ΑΠ για την εύλογη αιτία ανάκλησης του πιστοποιητικού.

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 την παράγραφο 3.4. Μετά την ανάκληση, ο Συνδρομητής του εν λόγω πιστοποιητικού θα ενημερώνεται για την αλλαγή της κατάστασης του Πιστοποιητικού και το πιστοποιητικό δεν αποκαθίσταται.

4.9.3.2 Ανάκληση του πιστοποιητικού από άλλη οντότητα

Οποιαδήποτε άλλη οντότητα μπορεί να υποβάλει Αναφορά Προβλήματος Πιστοποιητικού, που μπορεί να εμπεριέχει αίτημα ανάκλησής του, μέσω email στη διεύθυνση **cert-problem-report AT harica.gr** παραθέτοντας απόδειξη ότι:

α) έχει εκτεθεί το ιδιωτικό κλειδί του πιστοποιητικού, ή
β) η χρήση του πιστοποιητικού δεν είναι σύμφωνη με τη πολιτική πιστοποίησης, ή
γ) έχει πάψει να υφίσταται η συμβατική σχέση του κατόχου του πιστοποιητικού με το φορέα του.

Κάθε άλλο αίτημα ανάκλησης πιστοποιητικού από τρίτο εξετάζεται από την HARICA πριν γίνουν ενέργειες ανάκλησης του πιστοποιητικού.

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.

Σε περίπτωση Αναφοράς Προβλήματος Πιστοποιητικού με υψηλή προτεραιότητα, χρησιμοποιήστε τις πληροφορίες επικοινωνίας της παραγράφου 1.5.2.

4.9.3.3 Αίτημα Ανάκλησης από Προμηθευτή Εφαρμογής Λογισμικού

Αν ένας Προμηθευτής Λογισμικού πιστεύει ότι ένα χαρακτηριστικό (attribute) του Πιστοποιητικού είναι παραπλανητικό ή, ότι το Πιστοποιητικό χρησιμοποιήθηκε για να υπογράψει Ύποπτο Κώδικα ή άλλο παράνομο σκοπό, τότε μπορεί να αιτηθεί από την HARICA την ανάκληση του Πιστοποιητικού.

Σε αυτή την περίπτωση, μέσα σε δύο (2) εργάσιμες μέρες από τη λήψη του αιτήματος, η HARICA πρέπει είτε να ανακαλέσει το πιστοποιητικό ή να ενημερώσει τον Προμηθευτή Εφαρμογής Λογισμικού ότι διεξάγει έρευνα. Αν η HARICA αποφασίσει να διεξάγει έρευνα, πρέπει να πληροφορήσει τον Προμηθευτή Λογισμικού Εφαρμογής αν θα ανακαλέσει το Πιστοποιητικό, μέσα σε δύο (2) εργάσιμες μέρες. Αν η HARICA αποφασίσει ότι η ανάκληση θα έχει σημαντικές επιπτώσεις στον Συνδρομητή, τότε θα προτείνει στον Προμηθευτή Λογισμικού εναλλακτικές ενέργειες σύμφωνα με τη διερεύνηση του περιστατικού.

Σε κάθε περίπτωση, ο Συνδρομητής θα ενημερωθεί πριν από οποιαδήποτε αλλαγή στην κατάσταση του Πιστοποιητικού.

4.9.3.4 Αίτημα Ανάκλησης από τον Εθνικό Φορέα Εποπτείας eIDAS

Εάν ο Εθνικός Φορέα Εποπτείας (ΕΕΤΤ) θεωρεί ότι ένα Εγκεκριμένο Πιστοποιητικό περιλαμβάνει εσφαλμένες ή παραπλανητικές πληροφορίες ή ότι το Πιστοποιητικό έχει παραβιαστεί ή χρησιμοποιείται για υπογραφή πλαστών δεδομένων ή για κάποιο άλλο παράνομο σκοπό, τότε ο Φορέας Εποπτείας μπορεί να ζητήσει από την HARICA να αναστείλει ή να ανακαλέσει το Εγκεκριμένο Πιστοποιητικό. Ο Φορέας Εποπτείας πρέπει να προσδιορίσει έναν λόγο ανάκλησης βάσει του άρθρου 11 του Εθνικού κανονισμού για τους Παρόχους Υπηρεσιών Εμπιστοσύνης (ΦΕΚ 4396-Β, 2017).

Σε αυτή την περίπτωση, η HARICA πρέπει να εγκρίνει την αίτηση ανάκλησης και να εκτελέσει το αίτημα εντός δύο (2) εργάσιμων ημερών. Σε όλες τις περιπτώσεις, ο Συνδρομητής ενημερώνεται πριν από οποιαδήποτε αλλαγή της κατάστασης του Πιστοποιητικού του.

4.9.3.5 Αίτημα Ανάκλησης από Αρμόδια Εθνική Αρχή

Εάν μια Αρμόδια Εθνική Αρχή PSD2 πιστεύει ότι ένα Εγκεκριμένο Πιστοποιητικό PSD2 περιλαμβάνει πληροφορίες για ένα ΠΥΠ που είναι εσφαλμένες ή παραπλανητικές ή ότι το Πιστοποιητικό έχει παραβιαστεί ή χρησιμοποιείται για να υπογράψει πλαστά δεδομένα ή για κάποιο άλλο παράνομο σκοπό, τότε η ΑΕΑ μπορεί να ζητήσει από την HARICA να αναστείλει ή να ανακαλέσει το Εγκεκριμένο Πιστοποιητικό PSD2. Η ΑΕΑ πρέπει να προσδιορίσει έναν λόγο ανάκλησης, ο οποίος πρέπει να είναι περιγραφικός και όχι τυποποιημένος. Έγκυροι λόγοι ανάκλησης μπορεί να περιλαμβάνουν τα ακόλουθα σενάρια:

- οι πληροφορίες στο Δημόσιο Μητρώο έχουν αλλάξει ώστε να επηρεάζουν σημαντικά την εγκυρότητα των χαρακτηριστικών PSD2 στο πιστοποιητικό.
- το καθεστώς εξουσιοδότησης που έχει χορηγηθεί από αυτήν την ΑΕΑ έχει αλλάξει (π.χ. ο ΠΥΠ δεν είναι πλέον εγκεκριμένος).

Σε αυτή την περίπτωση, η HARICA πρέπει να εγκρίνει την αίτηση ανάκλησης και να εκτελέσει το αίτημα εντός δύο (2) εργάσιμων ημερών. Σε όλες τις περιπτώσεις, ο

Συνδρομητής ενημερώνεται πριν από οποιαδήποτε αλλαγή της κατάστασης του Πιστοποιητικού του.

4.9.4 Χρονική περίοδος στην οποία μπορεί να γίνει αίτημα ανάκλησης

Ο Συνδρομητής μπορεί να καταθέσει αίτημα ανάκλησης οποιαδήποτε στιγμή μέσα στη διάρκεια ισχύος του αρχικού πιστοποιητικού.

Για όλα τα περιστατικά που περιλαμβάνουν Παραβίαση του Κλειδιού των Πιστοποιητικών που χρησιμοποιήθηκαν για Υπογραφή Κώδικα, ηλεκτρονικές Υπογραφές ή ηλεκτρονικές Σφραγίδες, η HARICA ανακαλεί το Πιστοποιητικό που υπογράφει σύμφωνα και μέσα στα ακόλουθα μέγιστα χρονικά διαστήματα. Τίποτα από αυτά δεν απαγορεύει στην HARICA να ανακαλέσει ένα Πιστοποιητικό Υπογραφής Κώδικα πριν από αυτά τα χρονικά διαστήματα.

1. Η HARICA θα επικοινωνήσει με τον Συνδρομητή μέσα σε μία (1) εργάσιμη μέρα μετά από την γνωστοποίηση του γεγονότος σε αυτήν.
2. Η HARICA θα εκτιμήσει το πλήθος των Βασιζόμενων Μερών που επηρεάζονται (π.χ. σύμφωνα με το αρχείο καταγραφής του OCSP) μέσα σε 72 ώρες από την γνωστοποίηση του γεγονότος σε αυτήν.
3. Η HARICA θα ζητήσει από τον Συνδρομητή να στείλει επιβεβαίωση λήψης του αιτήματος ανάκλησης μέσα σε 72 ώρες.
    a. Αν ο Συνδρομητής αποκριθεί μέσα σε 72 ώρες, η HARICA και ο Συνδρομητής αποφασίζουν μετά από συζητήσεις μία «ρεαλιστική ημερομηνία» ανάκλησης του Πιστοποιητικού
    b. Αν ο Συνδρομητής δεν αποκριθεί μέσα σε 72 ώρες, η HARICA τον ενημερώνει ότι θα ανακαλέσει το Πιστοποιητικό σε 7 μέρες αν δεν υπάρχει άλλη απάντηση.
        i. Αν απαντήσει ο Συνδρομητής μέσα σε 7 μέρες, η HARICA και ο Συνδρομητής θα αποφασίσουν μετά από συζητήσεις μία «ρεαλιστική ημερομηνία» για την ανάκληση του πιστοποιητικού.
        ii. Αν δεν απαντήσει ο Συνδρομητής μέσα σε 7 μέρες, η HARICA ανακαλεί το Πιστοποιητικό, εκτός αν έχει τεκμηριωμένα στοιχεία (π.χ. αρχείο καταγραφής OCSP) ότι αυτή η ενέργεια θα έχει σημαντική αρνητική επίδραση στο ευρύ κοινό.

4.9.4.1 Ημερομηνία ανάκλησης για Πιστοποιητικά τύπου «Υπογραφών»

Όταν ανακαλείται Πιστοποιητικό που χρησιμοποιείται για Υπογραφή Κώδικα, ηλεκτρονικές Υπογραφές ή Σφραγίδες, η HARICA συνεργάζεται με τον Συνδρομητή για να εκτιμήσουν την ημέρα και την ώρα («ρεαλιστική ημερομηνία») που θα έπρεπε να γίνει η ανάκληση ώστε να περιοριστούν οι συνέπειες σε έγκυρα υπογεγραμμένα αντικείμενα (Κώδικας, Έγγραφα, Δεδομένα). Σε περίπτωση παραβίασης κλειδιού, αυτή η ημερομηνία θα πρέπει να είναι προγενέστερη της παραβίασης. Αυτή η «ρεαλιστική ημερομηνία» και ώρα θα πρέπει να χρησιμοποιηθεί ως χρονική στιγμή ανάκλησης για Πιστοποιητικά Υπογραφής Κώδικα προκειμένου να παρεμποδιστεί η εκτέλεση Ύποπτου Κώδικα. Το ίδιο εφαρμόζεται σε Πιστοποιητικά για ηλεκτρονικές Υπογραφές ή Σφραγίδες, για να ακυρωθούν ηλεκτρονικές Υπογραφές και ηλεκτρονικές Σφραγίδες υπογεγραμμένων εγγράφων μετά την υποτιθέμενη παραβίαση. Αυτή η διαδικασία ονομάζεται αναδρομική ανάκληση κι εφαρμόζεται μόνο σε Πιστοποιητικά που χρησιμοποιούνται για την «Υπογραφή» αντικειμένων.

4.9.5 Χρόνος απόκρισης της ΑΠ για ανακλήσεις πιστοποιητικών

Σε περίπτωση που η HARICA λάβει μια Αναφορά Προβλήματος Πιστοποιητικού, οφείλει να ξεκινά τη διερεύνηση δεδομένων και καταστάσεων σχετικά την αναφορά εντός εικοσι-τεσσάρων (24) ωρών, εκτός περιπτώσεων ανωτέρας βίας, και να παρέχει ένα προκαταρκτικό πόρισμα σε σχέση με τα ευρήματα στον Συνδρομητή και τον συντάκτη της Αναφοράς Προβλήματος Πιστοποιητικού.

Μετά την διερεύνηση των δεδομένων και καταστάσεων, η HARICA θα συνεργάζεται με τον Συνδρομητή και τον συντάκτη κάθε Αναφοράς Προβλήματος Πιστοποιητικού για να καθοριστεί εάν το Πιστοποιητικό θα ανακληθεί ή όχι, και σε περίπτωση που θα ανακληθεί, ποια θα είναι η ημερομηνία ανάκλησης. Η περίοδος μεταξύ λήψης της Αναφοράς Προβλήματος ή αιτήματος ανάκλησης έως την δημοσίευση ανάκλησης, δεν πρέπει να ξεπερνά τα χρονικά όρια που αναφέρονται στην ενότητα 4.9.1.1. Η ημερομηνία που θα επιλεγεί από τη HARICA, μπορεί να λάβει υπ' όψιν τα ακόλουθα κριτήρια:

1. Τη φύση του φερόμενου προβλήματος (εύρος, περιεχόμενο, βαρύτητα, μέγεθος, ρίσκο ή βλάβη). The nature of the alleged problem (scope, context, severity, magnitude, risk of harm).
2. Τις συνέπειες της ανάκλησης (άμεσες ή παράπλευρες επιπτώσεις σε Συνδρομητές και Βασιζόμενα Μέρη).
3. Τον αριθμό των Αναφορών Προβλήματος Πιστοποιητικών που έχουν υποβληθεί για ένα συγκεκριμένο Πιστοποιητικό ή Συνδρομητή.
4. Το υποκείμενο που καταθέτει την Αναφορά (για παράδειγμα, μια αναφορά από όργανο επιβολής του νόμου ότι ένας ιστοχώρος εμπλέκεται σε παράνομες δραστηριότητες έχει μεγαλύτερο βάρος από μια αναφορά ενός καταναλωτή που φέρεται να μην έχει λάβει τα προϊόντα που παρήγγειλε).
5. Σχετική νομοθεσία.

Αιτήματα ανάκλησης που παρέχουν επαρκή στοιχεία θα εξετάζονται άμεσα. Η μέγιστη καθυστέρηση ανάμεσα στην πραγματοποίηση της ανάκλησης πιστοποιητικού και στην αλλαγή της πληροφορίας που γίνεται διαθέσιμη σε Βασιζόμενα Μέρη και αφορά στην κατάσταση αυτού του πιστοποιητικού, δεν πρέπει να είναι πάνω από **εξήντα (60)** λεπτά.

4.9.6 Μηχανισμοί με τους οποίους Βασιζόμενα Μέρη ελέγχουν την κατάσταση των πιστοποιητικών

Τα Βασιζόμενα Μέρη πρέπει να ακολουθούν τις διαδικασίες της παραγράφου 1.3.4 πριν εμπιστευθούν οποιοδήποτε πιστοποιητικό. Θα πρέπει να μεταφορτώνουν τις Λίστες Ανάκλησης Πιστοποιητικών (ΛΑΠ) όλων των Πιστοποιητικών των Υφιστάμενων Αρχών Πιστοποίησης που μεσολαβούν μέχρι την εκδότρια αρχή του τελικού πιστοποιητικού. Οι Λίστες Ανάκλησης βρίσκονται πάντα δημοσιευμένες στο Αποθετήριο και είναι διαθέσιμες δημόσια. Οι Λίστες Ανάκλησης Πιστοποιητικών θα περιλαμβάνουν την κατάσταση των ανακλημένων πιστοποιητικών τουλάχιστον μέχρι την ημερομηνία λήξης τους. Εναλλακτικά, οι Βασιζόμενα Μέρη πρέπει να ελέγχουν για όλα τα Πιστοποιητικά (συμπεριλαμβανομένων των Πιστοποιητικών των Υφιστάμενων ΑΠ) αν έχουν ανακληθεί μέσω του OCSP.

4.9.7 Συχνότητα έκδοσης ΛΑΠ

Η ΛΑΠ υπογράφεται από την Εκδούσα ΑΠ ή μία άλλη οντότητα που έχει σχεδιαστεί από την HARICA.

Η ΛΑΠ πρέπει να ενημερώνεται και να δημοσιεύεται:

- για Πιστοποιητικά τελικών χρηστών/συσκευών, το αργότερο κάθε **επτά (7) ημέρες**. Η ΛΑΠ θα ισχύει για μέγιστο χρονικό διάστημα ίσο με **επτά (7) ημέρες.** Σε περίπτωση ανάκλησης ενός τελικού πιστοποιητικού, μια νέα ΛΑΠ θα εκδοθεί και θα δημοσιευθεί μέσα σε **24 ώρες** από τη στιγμή της ανάκλησης.
- για Πιστοποιητικά Υφιστάμενων Αρχών Πιστοποίησης και Πιστοποιητικά τελικών χρηστών/συσκευών που περιέχουν επέκταση EKU η οποία περιλαμβάνει την τιμή id-kp-timeStamping (όπως ορίζεται στο RFC 5280), τουλάχιστον κάθε **δώδεκα (12) μήνες**. Η ΛΑΠ θα ισχύει για μέγιστο χρονικό διάστημα ίσο με **δώδεκα (12) μήνες**

Σε περίπτωση έκθεσης μυστικού κλειδιού ή άλλου σημαντικού συμβάντος όπως για παράδειγμα ανάκληση Πιστοποιητικού Ενδιάμεσης Αρχής Πιστοποίησης ή Πιστοποιητικού Χρονοσήμανσης, θα εκδίδεται ενημερωμένη ΛΑΠ εντός 24 ωρών από τη στιγμή της ανάκλησης.

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

4.9.8 Χρόνος δημοσίευσης ΛΑΠ στο Αποθετήριο

Μετά από την ανάκληση κάποιου πιστοποιητικού δημιουργείται η ΛΑΠ και ενημερώνεται το Αποθετήριο. Η ΛΑΠ δημοσιεύεται στο Αποθετήριο μέσα σε λίγα λεπτά από την έκδοσή της. Στο Αποθετήριο το πιστοποιητικό χαρακτηρίζεται ως ανακληθέν.

Η HARICA λειτουργεί και συντηρεί τις ΛΑΠ και τις δυνατότητες της υπηρεσίας OCSP με ικανά συστήματα που εξασφαλίζουν μέγιστο χρόνο απόκρισης τα δέκα (10) δευτερόλεπτα, υπό φυσιολογικές συνθήκες.

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

Στην ΥΔΚ HARICA λειτουργεί δημόσια διαθέσιμη υπηρεσία ελέγχου Κατάστασης Πιστοποιητικών σε πραγματικό χρόνο (On-line Certificate Status Protocol – OCSP) που συμμορφώνεται με το RFC 6960. Η διεύθυνση της υπηρεσίας είναι ενσωματωμένη στα πιστοποιητικά που εκδίδονται. Η λειτουργία της υπηρεσίας OCSP είναι υποχρεωτική μόνο για Αρχές Πιστοποίησης που εκδίδουν δημόσια αναγνωρισμένα πιστοποιητικά. Οι απαντήσεις της υπηρεσίας OCSP πρέπει:

1. είτε να υπογράφονται από την Εκδούσα ΑΠ της οποίας ελέγχεται για ανάκληση η κατάσταση των πιστοποιητικών
2. είτε να υπογράφονται από έναν OCSP Responder του οποίου το Πιστοποιητικό έχει υπογραφεί από την Εκδούσα ΑΠ της οποίας ελέγχεται για ανάκληση η κατάσταση των πιστοποιητικών

Στην τελευταία περίπτωση, το Πιστοποιητικό του OCSP που υπογράφει πρέπει να περιέχει μια επέκταση του τύπου id-pkix-ocsp-nocheck, σύμφωνα με όσα ορίζονται στο RFC 6960.

4.9.10 Απαιτήσεις ελέγχων για ανάκληση σε πραγματικό χρόνο

Η HARICA υποστηρίζει μεθόδους OCSP χρησιμοποιώντας μεθόδους GET όπως περιγράφεται στο RFC 6960.

Ο χρόνος εγκυρότητας ενός OCSP response είναι η διαφορά του χρόνου μεταξύ των πεδίων `thisUpdate` και `nextUpdate`, συμπεριλαμβανομένων των τιμών αυτών. Για τον υπολογισμό των διαφορών αυτών, η διαφορά των 3.600 δευτερολέπτων ισούται με μία (1) ώρα, και η διαφορά των 86400 δευτερολέπτων ισούται με μία (1) ημέρα, αγνοώντας τα «επιπλέον δευτερόλεπτα» (leap-seconds).

Για την κατάσταση των Πιστοποιητικών Συνδρομητών:

- Οι απαντήσεις OCSP πρέπει να έχουν διάστημα εγκυρότητας μεγαλύτερο ή ίσο με **οκτώ (8) ώρες**.
- Οι απαντήσεις OCSP πρέπει να έχουν διάστημα εγκυρότητας μικρότερο ή ίσο με **δέκα (10) ημέρες**.
- Για απαντήσεις OCSP με διαστήματα εγκυρότητας μικρότερα των **δεκαέξι (16) ωρών**, η HARICA θα πρέπει να ενημερώνει την πληροφορία που παρέχεται από την υπηρεσία OCSP πριν το **μισό της περιόδου** εγκυρότητας πριν την τιμή `nextUpdate`.
- Για απαντήσεις OCSP με διαστήματα εγκυρότητας μεγαλύτερη ή ίση των **δεκαέξι (16) ωρών**, η HARICA θα πρέπει να ενημερώνει την πληροφορία που παρέχεται από την υπηρεσία OCSP το πολύ **οκτώ (8) ώρες** πριν την τιμή `nextUpdate` και όχι πέρα από **τέσσερεις (4) ημέρες** μετά την τιμή `thisUpdate`.

Για την κατάσταση των Πιστοποιητικών Υφιστάμενων ΑΠ:

- Η HARICA θα επικαιροποιεί τις πληροφορίες που παρέχονται μέσω OCSP τουλάχιστον (i) κάθε **δώδεκα (12) μήνες** και (ii) εντός **είκοσι τεσσάρων (24) ωρών** μετά την ανάκληση Πιστοποιητικού Ενδιάμεσης ΑΠ.

Αν η υπηρεσία OCSP λάβει αίτημα για την κατάσταση ενός σειριακού αριθμού πιστοποιητικού το οποίο είναι «unused», τότε η υπηρεσία δεν χρειάζεται να απαντήσει με την κατάσταση “good”.

Αν η υπηρεσία OCSP είναι για ΑΠ που ΔΕΝ ΕΙΝΑΙ Τεχνικά Περιορισμένη σύμφωνα με τα όσα αναφέρονται στην παράγραφο 7.1.5, τότε η υπηρεσία ΔΕΝ ΠΡΕΠΕΙ να απαντήσει με την κατάσταση “good” σε τέτοια αιτήματα.

Η υπηρεσία OCSP μπορεί να παρέχει οριστικές απαντήσεις για “reserved” σειριακούς αριθμούς πιστοποιητικών, σαν να υπήρχαν αντίστοιχα τελικά πιστοποιητικά που ταιριάζουν το Precertificate [RFC 6962]

Ο σειριακός αριθμός ενός αιτήματος OCSP είναι ένας από τους παρακάτω τρεις τύπους:

1. "assigned" αν το Πιστοποιητικό με τον συγκεκριμένο αριθμό έχει εκδοθεί από την Εκδούσα ΑΠ, χρησιμοποιώντας το τρέχον ή το κάποιο προηγούμενο κλειδί που σχετίζεται με την ΑΠ με βάση το subjectDN της, ή
2. "reserved" αν ένα Precertificate [RFC6962] με τον συγκεκριμένο σειριακό αριθμό έχει εκδοθεί είτε (a) από την εκδούσα ΑΠ είτε (b) από ένα Precertificate Signing Certificate [RFC6962] που σχετίζεται με την εκδούσα ΑΠ, ή
3. "unused" αν δεν ικανοποιείται καμία από τις παραπάνω δύο καταστάσεις.

4.9.11 Άλλες μορφές ανακοίνωσης ανάκλησης πιστοποιητικών

Στο Αποθετήριο Πιστοποιητικών όπου λειτουργεί μηχανή αναζήτησης πιστοποιητικών μέσω ιστοσελίδας, τα πιστοποιητικά που ανακαλούνται εμφανίζονται στην περιγραφή τους ως «Ανακληθέντα».

Από 2021-04-01, η HARICA θα δημοσιοποιεί πλήρες CRL URL για κάθε μη-ληγμένο, μη-ανακλημένο Πιστοποιητικό Αρχής Πιστοποίησης που δημοσιεύεται στη CCADB (https://ccadb.org).

4.9.12 Παραλλαγές για την περίπτωση έκθεσης/παραβίασης ιδιωτικού κλειδιού

Ισχύει ότι ορίζεται στη παράγραφο 4.9.1.

Υπάρχει δυνατότητα σε μη-Συνδρομητές να επικοινωνήσουν με τη HARICA και να αναφέρουν ότι έχει εκτεθεί/παραβιαστεί ένα ιδιωτικό κλειδί που σχετίζεται με μη-ληγμένο, μη-ανακλημένο Πιστοποιητικό, σύμφωνα με τις διαδικασίες επικοινωνίας που περιγράφονται στην ενότητα 4.9.3.2, χρησιμοποιώντας μια από τις ακόλουθες μεθόδους απόδειξης κατοχής/ελέγχου του ιδιωτικού κλειδιού που σχετίζεται με ένα Πιστοποιητικό. Η HARICA δύναται να επιτρέψει επιπλέον μεθόδους που δεν αναφέρονται σε αυτή την ενότητα κατά τη διακριτική της ευχέρεια.

4.9.12.1 Δημιουργία και υπογραφή δοκιμαστικού αρχείου

Δημιουργείται ένα απλό αρχείο κειμένου με περιεχόμενο “This key is compromised” ή αντίστοιχη γλώσσα, προκειμένου να σημειώσει ότι ο υπογράφων αυτού του μηνύματος ισχυρίζεται ότι το κλειδί έχει εκτεθεί/παραβιαστεί. Μπορεί να χρησιμοποιηθεί η παρακάτω εντολή από γραμμή εντολών:

- `echo “This key is compromised” > compromised.txt`

Υπογράφεται το sha256 hash του παραγόμενου αρχείου χρησιμοποιώντας το ιδιωτικό κλειδί (σε μορφή PEM) που θέλετε να αναφέρετε ως παραβιασμένο, χρησιμοποιώντας το λογισμικό openssl:

- `openssl dgst -sha256 -sign private-key.pem -out compromised.txt.signed compromised.txt`

Στέλνετε το αρχείο “compromised.txt.signed” στη HARICA σύμφωνα με την ενότητα 4.9.3.2.

4.9.12.2 Δημιουργία CSR που περιλαμβάνει ειδικό κείμενο

Δημιουργείται ένα CSR το οποίο στο πεδίο `subject:commonName` περιλαμβάνει το κείμενο “This key is compromised” ” ή αντίστοιχη γλώσσα, προκειμένου να σημειώσει ότι ο υπογράφων αυτού του μηνύματος ισχυρίζεται ότι το κλειδί έχει εκτεθεί/παραβιαστεί. Μπορεί να χρησιμοποιηθεί η παρακάτω εντολή από γραμμή εντολών χρησιμοποιώντας το λογισμικό openssl:

- `openssl req -new -key private-key.pem -subj "/CN=This key is compromised" -out compromised.csr`

Στέλνετε το αρχείο “compromised.csr” στη HARICA σύμφωνα με την ενότητα 4.9.3.2.

4.9.12.3 Δημοσίευση του Ιδιωτικού Κλειδιού

Η μέθοδος αυτή δεν προτείνεται αλλά θα θεωρηθεί από τη HARICA απόδειξη έκθεσης/παραβίασης ενός Ιδιωτικού Κλειδιού.

Στέλνετε το ίδιο το παραβιασμένο ιδιωτικό κλειδί στη HARICA σύμφωνα με την ενότητα 4.9.3.2.

4.9.13 Περιπτώσεις αναστολής πιστοποιητικών

Αναστολή Πιστοποιητικού επιτρέπεται μόνο για Πιστοποιητικά που χρησιμοποιούνται για «Υπογραφή» (Υπογραφή κώδικα, ηλεκτρονική υπογραφή, ηλεκτρονική σφραγίδα, S/MIME). Όταν λάβει αίτημα ανάκλησης η HARICA σύμφωνα με τις παραγράφους 4.9.3.2 ή 4.9.3.3, και ανάλογα με τα ευρήματα της έρευνας, η επιλογή για αναστολή των Πιστοποιητικών γίνεται κατά την αποκλειστική κρίση της HARICA.

4.9.14 Ποιος μπορεί να αιτηθεί αναστολή πιστοποιητικών

Αναστολή Πιστοποιητικού μπορεί να ζητηθεί μόνο για Πιστοποιητικά που χρησιμοποιούνται για «Υπογραφή» από τα Βασιζόμενα Μέρη ή τους Προμηθευτές Λογισμικού Εφαρμογών όπως περιγράφεται στις 4.9.3.2 ή 4.9.3.3 αντίστοιχα.

4.9.15 Διαδικασία αιτήματος αναστολής πιστοποιητικού

Αναστολή Πιστοποιητικού μπορεί να ζητηθεί μέσω αιτήματος ανάκλησης. Η αναστολή των Πιστοποιητικών που χρησιμοποιούνται για «Υπογραφή» παραμένει στην αποκλειστική κρίση της HARICA. Ο Συνδρομητής που σχετίζεται με το Πιστοποιητικό ενημερώνεται πάντα από την HARICA για κάθε αλλαγή κατάστασης αυτού, συμπεριλαμβανομένης της αναστολής Πιστοποιητικού.

Αν η HARICA αποφασίσει να αναστείλει Πιστοποιητικό που χρησιμοποιείται για «Υπογραφή», η σχετική ΛΑΠ ενημερώνεται με την καταχώρηση εγγραφής που αφορά στο πιστοποιητικό που ανακλήθηκε και στο λόγο ανάκλησης μέσω του πεδίου ”certificateHold”, όπως ορίζεται στο RFC 5280. Εάν αποκατασταθεί αυτό το Πιστοποιητικό, καταργείται η αντίστοιχη καταχώρηση. Αν το Πιστοποιητικό ανακληθεί, ενημερώνεται η συγκεκριμένη καταχώρηση και τροποποιείται ανάλογα ο λόγος ανάκλησης. Άπαξ ένα Πιστοποιητικό ανακληθεί, δεν μπορεί να αποκατασταθεί.

4.9.16 Χρονική περίοδος αναστολής πιστοποιητικού

Η αναστολή των πιστοποιητικών δεν μπορεί να υπερβεί τις δύο (2) εβδομάδες.

4.10 Υπηρεσίες ελέγχου κατάστασης πιστοποιητικών

4.10.1 Λειτουργικά χαρακτηριστικά

Η HARICA ΠΑΡΕΧΕΙ ακριβείς κι ενημερωμένες πληροφορίες για την κατάσταση ανάκλησης Πιστοποιητικών που χρησιμοποιούνται για επαλήθευση ταυτότητας (π.χ. SSL/TLS) μέχρι τη λήξη τους.

Η HARICA ΠΑΡΕΧΕΙ ακριβείς κι ενημερωμένες πληροφορίες για την κατάσταση ανάκλησης Πιστοποιητικών για μία περίοδο τουλάχιστον **επτά (7) ετών** από τη λήξη των Πιστοποιητικών που χρησιμοποιούνται για ηλεκτρονικές Υπογραφές, ηλεκτρονικές Σφραγίδες, Υπογραφή Κώδικα και Χρονοσήμανση. Μετά τη λήξη μιας Εκδούσας ΑΠ που εκδίδει Πιστοποιητικά για ηλεκτρονικές Υπογραφές, ηλεκτρονικές Σφραγίδες, Υπογραφή Κώδικα και Χρονοσήμανση, οι αντίστοιχες ΛΑΠ παραμένουν δημοσιευμένες για τουλάχιστον άλλα **πέντε (5) χρόνια**.

Η HARICA ΠΑΡΕΧΕΙ απαντήσεις OCSP για Πιστοποιητικά που χρησιμοποιούνται για ηλεκτρονικές Υπογραφές, ηλεκτρονικές Σφραγίδες, Υπογραφή Κώδικα και Χρονοσήμανση για τουλάχιστον **επτά (7) έτη** από τη λήξη ενός τέτοιου Πιστοποιητικού. Οι Προμηθευτές Λογισμικού Εφαρμογών μπορούν να ζητούν από την HARICA να υποστηρίξει μεγαλύτερο χρονικό διάστημα σύμφωνα με τις απαιτήσεις των δικών τους αποθετηρίων πιστοποιητικών.

Σημείωση: Αν ένα Πιστοποιητικό Υπογραφής Κώδικα περιέχει το αναγνωριστικό (OID) “Lifetime Signing”, η ψηφιακή υπογραφή χάνει την εγκυρότητά της όταν λήγει αυτό το Πιστοποιητικό, ακόμα και αν η ψηφιακή υπογραφή περιέχει χρονοσήμανση.

Η HARICA συμπεριλαμβάνει διευθύνσεις (URLs) που αφορούν πληροφορίες ανάκλησης μέσα στο Πιστοποιητικό οποιασδήποτε οντότητας και συγκεκριμένα στις επεκτάσεις CRL Distribution Points (όπου είναι δυνατό) και Authority Information Access.

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 Αποθετήριο πιστοποιητικών**

Το on-line αποθετήριο 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. Το Αποθετήριο Πιστοποιητικών πρέπει να εμφανίζει όλα τα πιστοποιητικά που έχουν εκδοθεί/ανακληθεί. Αυτό το Αποθετήριο πιστοποιητικών είναι διαθέσιμο στη διεύθυνση https://repo.harica.gr.

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

Η HARICA προβαίνει σε όλες τις αναγκαίες ενέργειες για όσο το δυνατόν αδιάλειπτη διαθεσιμότητα των υπηρεσιών ελέγχου κατάστασης πιστοποιητικών.

4.10.3 Προαιρετικά χαρακτηριστικά

Δεν ορίζεται.

4.11 Λήξη συνδρομής

Η συνδρομή τερματίζεται όταν ένα Πιστοποιητικό

- φτάσει την ημερομηνία "validTo" και λήξει
- ανακληθεί πριν φτάσει η ημερομηνία "validTo".

Η ανάκληση πιστοποιητικού που έχει λήξει δεν είναι απαραίτητη, παρά μόνο αν συντρέχει κάποιος από τους λόγους που αναφέρονται στην παράγραφο 4.9.1.

4.12 Μεσεγγύηση ιδιωτικού κλειδιού (key escrow) και Επαναφορά κλειδιού

4.12.1 Διαδικασίες και πρακτικές συνοδείας ιδιωτικού κλειδιού και επαναφοράς

Η HARICA δεν παρέχει αυτή τη στιγμή υπηρεσίες μεσεγγύησης.

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

Η HARICA δεν παρέχει αυτή τη στιγμή υπηρεσίες μεσεγγύησης.

5 Διοικητικοί, Τεχνικοί και Λειτουργικοί έλεγχοι

5.1 Φυσική ασφάλεια και έλεγχος πρόσβασης

5.1.1 Τοποθεσία εγκαταστάσεων

Τη HARICA σήμερα διαχειρίζεται το Κέντρο Ηλεκτρονικής Διακυβέρνησης (ΚΗΔ) του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης. Ο εξοπλισμός των ΑΠ/ΑΚ βρίσκεται σε ασφαλές περιβάλλον σε γεωγραφικά διαχωρισμένα datacenter.

Εξοπλισμός που σχετίζεται με τις λειτουργίες της ΑΠ και της ΑΚ όσον αναφορά σε πληροφοριακό υλικό και λογισμικό βρίσκεται υπό συνεχή παρακολούθηση και απαγορεύεται η απομάκρυνση/μετακίνηση εξοπλισμού σε άλλο φυσικό χώρο χωρίς προηγούμενη έγκριση από την ανώτερη διοίκηση της HARICA.

5.1.2 Φυσική πρόσβαση

Η φυσική πρόσβαση στον εξοπλισμό των ΑΠ και ΑΚ επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό με έμπιστους ρόλους.

Ο εξοπλισμός της ΑΠ της HARICA βρίσκεται σε κλειδωμένα ερμάρια που είναι σε επίσης κλειδωμένες αίθουσες εξοπλισμού εξυπηρετητών. Η πρόσβαση στις αίθουσες εξοπλισμού εξυπηρετητών βρίσκεται υπό συνεχή παρακολούθηση κι έλεγχο.

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

5.1.3 Κλιματισμός και ρύθμιση τροφοδοσίας με ρεύμα

Όλος ο εξοπλισμός της ΑΠ της HARICA 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 ΑΠ της HARICA βρίσκεται σε χώρο που δεν κινδυνεύει σε μεγάλο βαθμό από πλημμύρες.

5.1.5 Πρόληψη και προστασία από φωτιά

Ο εξοπλισμός της ΑΠ HARICA υπόκειται στην ελληνική νομοθεσία σχετικά με την πρόληψη και την προστασία πυρκαγιάς στα δημόσια κτίρια.

5.1.6 Αποθηκευτικά μέσα

Τα ιδιωτικά κλειδιά της HARICA που σχετίζονται με τα Πιστοποιητικά των ΑΠ είναι αποθηκευμένα σε ασφαλές εξωτερικό μέσο αποθήκευσης, κρυπτογραφημένα και διανέμονται μόνο σε εξουσιοδοτημένο προσωπικό, με την απαίτηση να υπάρχουν τουλάχιστον δύο έμπιστα πρόσωπα για να υπάρξει πρόσβαση σε αυτά.

Αντίγραφα ασφαλείας του λογισμικού των ΑΠ/ΑΚ της HARICA, του αρχείου της ΑΚ και του αρχείου συναλλαγών συμβάντων βρίσκονται σε αποσπώμενα αποθηκευτικά μέσα σε κρυπτογραφημένη μορφή.

Και τα δύο παραπάνω αποθηκευτικά μέσα βρίσκονται σε φυσικές τοποθεσίες, 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 (π.χ. memory flash disks), τα αρχεία διαγράφονται με ασφάλεια προκειμένου να μην υπάρχει δυνατότητα επαναχρησιμοποίησης, σύμφωνα με τις μεθόδους που περιγράφονται στην παράγραφο 6.2.10.

Σε περίπτωση που το αποθηκευτικό μέσο είναι κρυπτογραφημένο, η καταστροφή του κλειδιού αποκρυπτογράφησης θεωρείται ικανή συνθήκη για να θεωρηθεί ότι το κρυπτογραφημένο μέσο έχει καταστραφεί.

5.1.7 Διάθεση απορριμμάτων

Απορρίμματα που περιέχουν οποιαδήποτε εμπιστευτική πληροφορία όπως εύκαμπτοι μαγνητικοί δίσκοι, σκληροί δίσκοι κ.α. καταστρέφονται πριν απορριφθούν. Ιδιωτικά κλειδιά Μονάδων Χρονοσήμανσης που είναι αποθηκευμένα σε κρυπτογραφική συσκευή τμήμα της ΜΧΣ, σβήνονται με την απόσυρση της συσκευής με τέτοιον τρόπο που είναι πρακτικά αδύνατο να ανακτηθούν.

5.1.8 Τήρηση αντιγράφων ασφαλείας εκτός εγκαταστάσεων

Αντίγραφα ασφαλείας των λογισμικών και των δεδομένων της ΥΔΚ της HARICA τηρούνται εκτός εγκαταστάσεων. Αντίγραφα ασφαλείας του λογισμικού των ΑΠ/ΑΚ της HARICA, του αρχείου της ΑΚ και του αρχείου συναλλαγών-συμβάντων βρίσκονται σε αποσπώμενα αποθηκευτικά μέσα σε κρυπτογραφημένη μορφή και είναι προσβάσιμα από εξουσιοδοτημένο προσωπικό. Επίσης, τα ιδιωτικά κλειδιά της ΑΠ είναι αποθηκευμένα εκτός εγκαταστάσεων με κρυπτογραφημένη μορφή, και είναι προσβάσιμα από εξουσιοδοτημένο προσωπικό, σύμφωνα με τις προϋποθέσεις της παραγράφου 5.2.2.

5.2 Έλεγχος διαδικασιών

5.2.1 Έμπιστοι ρόλοι

Το προσωπικό που ορίζεται για να λειτουργεί την ΥΔΚ της HARICA κατέχει έναν τεκμηριωμένο και με σαφήνεια καθορισμένο ρόλο. Κάθε έμπιστος ρόλος εξουσιοδοτείται για την εκτέλεση συγκεκριμένων διαδικασιών που σχετίζονται με τις λειτουργίες των Αρχών Πιστοποίησης και Καταχώρησης κάτω από σαφώς καθορισμένες διαδικασίες. Οι έμπιστοι ρόλοι και τα καθήκοντα του προσωπικού περιγράφονται με σαφήνεια. Ανάλογα με το ρόλο, καθορίζονται και τα καθήκοντα του προσωπικού ακολουθώντας πάντα την αρχή του περιορισμού κατ' ελάχιστον των προνομίων πρόσβασης (least privilege principle) στη διαχείριση λογαριασμών χρηστών και στις διαδικασίες ελέγχου πρόσβασης.

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

Οι ευαίσθητες λειτουργίες της ΥΔΚ απαιτούν την ενεργό συμμετοχή από τουλάχιστον δύο εξουσιοδοτημένα άτομα για να εκτελεσθεί η ευαίσθητη λειτουργία. Τα ιδιωτικά κλειδιά της ΑΠ αντιγράφονται, αποθηκεύονται και ανακτώνται μόνο από το προσωπικό με έμπιστους ρόλους χρησιμοποιώντας, τουλάχιστον, διπλό έλεγχο σε φυσικά ασφαλές περιβάλλον.

5.2.3 Εξακρίβωση ταυτότητας για κάθε ρόλο

Ένα πρόσωπο που κατέχει έμπιστο ρόλο, πρέπει να αναγνωρίζεται/ταυτοποιείται στο Σύστημα Διαχείρισης Πιστοποιητικών πριν εκτελέσει συγκεκριμένα καθήκοντα, χρησιμοποιώντας μοναδικά στοιχεία πρόσβασης που δημιουργήθηκαν ή ανατέθηκαν σε αυτό το πρόσωπο.

5.2.4 Ρόλοι που απαιτούν διαχωρισμό καθηκόντων

Στο προσωπικό που ανατέθηκε ο ρόλος του «ελεγκτή ασφάλειας ΑΠ» δεν ανατίθεται άλλος ρόλος όταν εκτελεί διαδικασίες που σχετίζονται με τελετή κλειδιού ΑΠ.

Για τα EV Πιστοποιητικά, η HARICA επιβάλλει το διαχωρισμό των καθηκόντων στον έλεγχο εγκυρότητας για να εξασφαλίσει ότι ένα και μόνο άτομο δεν μπορεί να κάνει τον έλεγχο εγκυρότητας και να εγκρίνει την έκδοση EV πιστοποιητικού. Τα βήματα τελικής διασταύρωσης (Final Cross-Correlation) και ελέγχου με την δέουσα επιμέλεια (Due Diligence), όπως περιγράφεται στην Ενότητα 11.13 των Οδηγιών EV, ΜΠΟΡΟΥΝ να πραγματοποιηθούν από το ένα από τα αρμόδια άτομα. Για παράδειγμα, ένας Ειδικός Ελέγχου Εγκυρότητας μπορεί να ελέγξει και να επαληθεύσει όλες τις πληροφορίες του Αιτούντα και ένας δεύτερος Ειδικός Ελέγχου Εγκυρότητας ΜΠΟΡΕΙ να εγκρίνει την έκδοση του EV Πιστοποιητικού.

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.

Η HARICA εξακριβώνει την ταυτότητα και την αξιοπιστία ενός ατόμου, πριν την απασχόλησή του στη διαδικασία διαχείρισης Πιστοποιητικών, είτε ως υπάλληλος, εκπρόσωπος ή ανεξάρτητος εργολάβος.

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 ή ΑΚ και έχει πρόσβαση σε διαδικασίες κρυπτογράφησης, εκπαιδεύεται και καταρτίζεται σε λειτουργίες της ΑΠ/ΑΚ από ειδικούς σε θέματα ΥΔΚ της HARICA. 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 και να κατανοεί όλα τα κείμενα πολιτικής/διαδικασιών και ειδικά την παρούσα Πολιτική Πιστοποίησης /Δήλωση Διαδικασιών Πιστοποίησης. Οι υπεύθυνοι επαλήθευσης εκπαιδεύονται και αξιολογούνται πάνω στα κριτήρια επαλήθευσης EV.

5.3.4 Διαδικασίες και συχνότητα επανεκπαιδεύσεων

Το προσωπικό που κατέχει έμπιστους ρόλους διατηρεί υψηλό επίπεδο δεξιοτήτων. Όποτε υπάρχουν νέες εξελίξεις στον κλάδο της τεχνολογίας ΥΔΚ ή λειτουργικές αλλαγές, διοργανώνεται ένα σεμινάριο κατάρτισης και οι κατάλληλες πληροφορίες διαχέονται στο προσωπικό.

Η HARICA ενημερώνει το προσωπικό που είναι υπεύθυνο για εξακρίβωση/επιβεβαίωση στοιχείων και διαχείριση Πιστοποιητικών, για περιστατικά ασφάλειας άλλων ΠΥΕ που εκδίδουν Δημόσια Έμπιστα Πιστοποιητικά, όπως και για κάθε σχετική συζήτηση, προκλήσεις, βέλτιστες πρακτικές που αναδεικνύονται από οργανισμούς προτύπων όπως το CA/Browser Forum και το ETSI.

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, συμπεριλαμβανομένων πειθαρχικών ποινών σύμφωνα με την Πολιτική Ασφάλειας της HARICA και τις εσωτερικές διαδικασίες.

5.3.7 Έλεγχος σε προσωπικό εξωτερικών εργολάβων που εργάζονται εκτός της GUnet και εμπλέκονται με την ΥΔΚ HARICA

Σε περίπτωση που η HARICA προσλαμβάνει εξωτερικό εργολάβο για επιθεώρηση ή άλλες εργασίες, ο εργολάβος θα πρέπει να υπογράφει Σύμβαση Εμπιστευτικότητας. Το ίδιο ισχύει και στις περιπτώσεις ελέγχων μέσω ομάδας Εξωτερικών Ελεγκτών (External Auditors). Προσωπικό Εξουσιοδοτημένου Τρίτου Εταίρου που εμπλέκεται στην έκδοση ενός Πιστοποιητικού πληροί τις απαιτήσεις εκπαίδευσης και προσόντων που περιγράφονται στην παράγραφο 5.3.3 και τις απαιτήσεις διατήρησης εγγράφων και καταγραφής συμβάντων της παραγράφου 5.4.3 και 5.4.1 αντίστοιχα., συμπεριλαμβανομένων των απαιτήσεων αρχειοθέτησης της παραγράφου 5.5.2.

5.3.8 Τεκμηρίωση που παρέχεται στο προσωπικό κατά τη διάρκεια εκπαίδευσης

Σχετικό υλικό τεκμηρίωσης βρίσκεται διαθέσιμο από τη 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 όλες τις συναλλαγές που σχετίζονται με αιτήσεις έκδοσης πιστοποιητικού, έκδοση ή ανάκληση πιστοποιητικών, έκδοση των ΛΑΠ, έκδοση ή ανάκληση των Πιστοποιητικών των ΑΠ και όλες τις πληροφορίες που ανταλλάχθηκαν με την Αρχή Καταχώρισης. Επίσης, καταγράφονται σε όλους τους εξυπηρετητές της ΥΔΚ HARICA οι διεργασίες των λειτουργικών συστημάτων, οι προσπάθειες ελέγχου εισόδου, οι HTTP συνδέσεις με τους εξυπηρετητές ιστοσελίδων κ.α.

Πιο συγκεκριμένα, η HARICA και κάθε Εξουσιοδοτημένος Τρίτος Εταίρος θα καταγράφει λεπτομέρειες σχετικά με την επεξεργασία αιτήματος για έκδοση Πιστοποιητικού, περιλαμβάνοντας στοιχεία που σχετίζονται με το αίτημα, ώρα, ημερομηνία, καθώς και το προσωπικό που απασχολήθηκε. Η HARICA θα παρέχει τα συγκεκριμένα στοιχεία στον Φορέα Επιθεώρησης ως αποδεικτικά στοιχεία συμμόρφωσης με την ΠΠ/ΔΔΠ.

Η HARICA θα καταγράφει κατ' ελάχιστο τα ακόλουθα γεγονότα που σχετίζονται με:

1. Πιστοποιητικά Αρχών Πιστοποίησης και τον κύκλο ζωής των κλειδιών τους, συμπεριλαμβάνοντας πληροφορίες για:
    1. Δημιουργία κλειδιών, αντίγραφα ασφαλείας, αποθήκευση, ανάκτηση, αρχειοθέτηση και καταστροφή,
    2. Αιτήματα Πιστοποιητικών, ανανεώσεις, αλλαγή κλειδιών και ανάκληση,
    3. Έγκριση και απόρριψη αιτημάτων πιστοποιητικών,
    4. Τον κύκλο ζωής διαχείρισης κρυπτογραφικών συσκευών,
    5. Δημιουργία Λιστών Ανάκλησης Πιστοποιητικών και εγγραφών OCSP,
    6. Εισαγωγή νέων Προφίλ Πιστοποιητικών και την διακοπή χρήσης υφιστάμενων Προφίλ Πιστοποιητικών.
2. Τελικά Πιστοποιητικά Συνδρομητών συμπεριλαμβάνοντας πληροφορίες για:
    1. Αιτήματα Πιστοποιητικών, ανανεώσεις, αλλαγή κλειδιών και ανάκληση,
    2. Τις ενέργειες εξακρίβωσης που περιγράφονται στην παρούσα ΠΠ/ΔΔΠ,
    3. Έγκριση και απόρριψη αιτημάτων πιστοποιητικών,
    4. Έκδοση των Πιστοποιητικών, και
    5. Δημιουργία Λιστών Ανάκλησης Πιστοποιητικών και εγγραφών OCSP.
3. Συμβάντα ασφάλειας, συμπεριλαμβάνοντας πληροφορίες για:
    1. Επιτυχή και αποτυχημένη απόπειρα πρόσβασης σε συστήματα της Υποδομής Δημοσίου Κλειδιού,
    2. Ενέργειες σχετικά με το σύστημα ασφάλειας της ΥΔΚ,
    3. Αλλαγές στο προφίλ ασφάλειας,
    4. Εγκατάσταση, ενημέρωση και αφαίρεση λογισμικού σε συστήματα διαχείρισης Πιστοποιητικών,
    5. Περιπτώσεις που συστήματα δεν ανταποκρίνονται, αστοχίες υλικού ή άλλες ανωμαλίες των συστημάτων,
    6. Ενέργειες που αφορούν διεργασίες δρομολογητών και τειχών προστασίας,
    7. Είσοδο και έξοδο από τους χώρους των ΑΠ.

Τα δεδομένα συναλλαγών θα περιλαμβάνουν τα ακόλουθα στοιχεία:

1. Ημερομηνία και ώρα της συναλλαγής,
2. Αναγνωριστικό του προσώπου που πραγματοποιεί την ενημέρωση του αρχείου συναλλαγών και
3. Περιγραφή της συναλλαγής.

Όλα τα συστήματα που καταγράφουν δεδομένα είναι συγχρονισμένα μέσω πρωτοκόλλου NTP (Network Time Protocol).

5.4.2 Συχνότητα αρχειοθέτησης των επεξεργασμένων συναλλαγών-συμβάντων

Το σύστημα αρχειοθετεί καθημερινά όλες τις συναλλαγές.

5.4.3 Διάστημα τήρησης του αρχείου συναλλαγών-συμβάντων

Η HARICA θα διατηρεί για τουλάχιστον **δύο (2) χρόνια**:

1. Συναλλαγές-συμβάντα που σχετίζονται με Πιστοποιητικά ΑΠ και τον κύκλο ζωής των κλειδιών, όπως περιγράφονται στην ενότητα 5.4.1(1), έπειτα από:
    1. Την καταστροφή του Ιδιωτικού Κλειδιού της Αρχής Πιστοποίησης, ή
    2. Την ανάκληση ή λήξη του Πιστοποιητικού της Αρχής Πιστοποίησης στην ομάδα Πιστοποιητικών τα οποία περιλαμβάνουν την επέκταση X.509v3 `basicConstraints` με το πεδίο `cA` ρυθμισμένο ως true, έχοντας το ίδιο Δημόσιο Κλειδί που αντιστοιχεί στο Ιδιωτικό Κλειδί της ΑΠ,
2. Συναλλαγές-συμβάντα που σχετίζονται με τον κύκλο ζωής τελικών Πιστοποιητικών Συνδρομητών, όπως περιγράφονται στην ενότητα 5.4.1(2), έπειτα από την ανάκληση ή λήξη των τελικών Πιστοποιητικών;
3. Οποιαδήποτε συναλλαγή που σχετίζεται με συμβάντα ασφάλειας όπως περιγράφονται στην ενότητα 5.4.1 (3) μετά το συμβάν.

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. Συμβάντα που σχετίζονται με τον κύκλο ζωής του Πιστοποιητικού, έγγραφα πολιτικής/διαδικασίων, τελετές Κλειδιού είναι αρχειοθετημένα και διατηρούνται για όσο ορίζεται στην παράγραφο 5.5.2.

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. Πολλαπλά αντίγραφα αρχείων συναλλαγών-συμβάντων αποθηκεύονται σε διαφορετικές τοποθεσίες και προστατεύονται με κατάλληλους φυσικούς και λογικούς ελέγχους πρόσβασης.

5.4.5 Διαδικασίες αντιγράφων ασφαλείας αρχείων συναλλαγών-συμβάντων

Τηρείται αντίγραφο ασφαλείας του αρχείου συναλλαγών-συμβάντων σε διαφορετική τοποθεσία σε κατάσταση μόνο για ανάγνωση, που προστατεύεται με ελέγχους φυσικής και λογικής πρόσβασης.

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 πραγματοποιεί ετήσια Αξιολόγηση Κινδύνων που

1. Αναγνωρίζει προβλέψιμες εσωτερικές κι εξωτερικές απειλές που θα είχαν ως αποτέλεσμα μη εξουσιοδοτημένη πρόσβαση, γνωστοποίηση, κατάχρηση, τροποποίηση ή καταστροφή οποιουδήποτε Δεδομένου Πιστοποιητικού ή Διαδικασιών Διαχείρισης Πιστοποιητικών,
2. Αξιολογεί την πιθανότητα καταστροφής που προκαλείται από αυτές τις απειλές λαμβάνοντας υπόψη την ευαισθησία των Δεδομένων των Πιστοποιητικών και των Διαδικασιών Διαχείρισης Πιστοποιητικών, και
3. Αξιολογεί την επάρκεια των πολιτικών, των διαδικασιών, της τεχνολογίας των πληροφοριακών συστημάτων, και άλλων ρυθμίσεων που εφαρμόζει η ΑΠ για να αντιμετωπίσει τέτοιες απειλές.

Διενεργούνται Περιοδικές Δοκιμές Διείσδυσης (Penetration Tests), τουλάχιστον ετησίως, και τριμηνιαίες Σαρώσεις για Ευπάθειες 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

Η HARICA διατηρεί τις εγγραφές που σχετίζονται με τα αιτήματα πιστοποιητικών και την επαλήθευση συνδρομητών, και με όλα τα Πιστοποιητικά και τις ανακλήσεις, για τουλάχιστον:

- **Επτά (7) έτη** για τα «Εγκεκριμένα πιστοποιητικά για ηλεκτρονικές υπογραφές/σφραγίδες»,
- **Επτά (7) έτη** για τα πιστοποιητικά χρήσης SSL/TLS, Υπογραφής Κώδικα και μη εγκεκριμένα Πιστοποιητικά χρηστών
- **Ένα (1) έτος** για τα Πιστοποιητικά Χρονοσήμανσης

μετά την ημερομηνία λήξης του Πιστοποιητικού.

Τα Πιστοποιητικά Χρονοσήμανσης είναι έγκυρα για δέκα (10) χρόνια αλλά απαιτούν επανέκδοση κλειδιού κάθε χρόνο. Οπότε, το αρχείο καταγραφής που αφορά Πιστοποιητικά Χρονοσήμανσης διατηρείται για έντεκα (11) χρόνια.

Τα διαστήματα αυτά δύνανται να τροποποιηθούν ανάλογα με τις εξελίξεις της σχετικής νομοθεσίας για την προστασία προσωπικών δεδομένων.

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

Πριν τη φθορά αποθηκευτικών μέσων μακράς αποθήκευσης που χρησιμοποιούν παρωχημένη τεχνολογία, τα δεδομένα θα πρέπει να μεταφέρονται σε μέσα μακράς αποθήκευσης χρησιμοποιώντας πιο τρέχουσα τεχνολογία, πιθανότατα χρησιμοποιώντας διαφορετικό κρυπτοσύστημα, έτσι ώστε τα δεδομένα να είναι προστατευμένα από εκφυλισμό.

Σε κάθε περίπτωση, τα νέα δεδομένα θα μεταφέρονται και θα αποθηκεύονται σε κρυπτογραφημένη μορφή, και τα παλαιότερα δεδομένα θα πρέπει να καταστρέφονται.

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 αρχείων εγγραφών

Στην παρούσα φάση δεν απαιτείται ψηφιακή χρονοσήμανση (κατά το RFC 3161) των αρχείων εγγραφών. Όλα τα έγγραφα περιέχουν ημερομηνία και ώρα από μια έμπιστη πηγή, όπως περιγράφεται στην παράγραφο 6.8.

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

Η HARICA χρησιμοποιεί εσωτερικό σύστημα συλλογής αρχείων εγγραφών. Κάθε αντίγραφο προστίθεται στο αρχείο είναι κρυπτογραφημένο για διαφύλαξη της εμπιστευτικότητας, και υπογράφεται ψηφιακά για τη διατήρηση ακεραιότητας.

5.5.7 Διαδικασίες για ανάκτηση και επαλήθευση των στοιχείων των αρχείων εγγραφών

Η HARICA ελέγχει περιοδικά την ακεραιότητα του αρχείου εγγραφών εκτελώντας διαδικασία ανάκτησης δεδομένων και έλεγχο υπογραφών των αρχείων καταγραφής.

5.6 Ριζική αλλαγή κλειδιού

Σε περίπτωση αλλαγής κλειδιού κάποιας Αρχής Πιστοποίησης, τα πιστοποιητικά χρηστών/συσκευών που δεν έχουν λήξει πρέπει να ανακληθούν και να ξαναδημιουργηθούν σύμφωνα με τις διαδικασίες της παραγράφου 4.1.

Η HARICA θα εξασφαλίσει ότι όταν τα Πιστοποιητικά Υφιστάμενων ΑΠ φτάσουν στην λήξη της διάρκειας ισχύος τους, θα σταματήσουν την έκδοση νέων πιστοποιητικών και θα αντικατασταθούν με νέα Πιστοποιητικά Υφιστάμενων ΑΠ. Τα ληγμένα Πιστοποιητικά Υφιστάμενων ΑΠ θα παραμείνουν στην ΥΔΚ μέχρι να λήξουν ή να ανακληθούν όλα τα πιστοποιητικά τελικών χρηστών/συσκευών.

Κορυφαία Πιστοποιητικά θα αντικατασταθούν με δημιουργία νέων Πιστοποιητικών και θα διανεμηθούν σε βασιζόμενα μέρη και Προμηθευτές Λογισμικού Εφαρμογών σύμφωνα με την παράγραφο 6.1.4.

5.7 Επαναφορά από παραβίαση ασφάλειας και καταστροφή

5.7.1 Διαδικασίες και χειρισμός περιστατικών παραβίασης

Τα αρχεία καταγραφής ελέγχονται περιοδικά για ανίχνευση προσπαθειών παραβίασης ασφάλειας ή παραβιάσεων του Συστήματος Πιστοποιητικών. Σε περίπτωση που ανιχνευθεί κάποια ανωμαλία ή υπάρχει υποψία παραβίασης, διακόπτεται η παροχή της υπηρεσίας και γίνεται ενδελεχής έλεγχος όλων των συστημάτων. Καταγράφεται εσωτερικά η διαδικασία αντιμετώπισης του περιστατικού. Η διαδικασία αυτή περιλαμβάνει βήματα για την ενημέρωση των περιστατικών ασφάλειας προς Παρόχους Λογισμικού (Application Software Suppliers).

Η HARICA φροντίζει για τη συμμόρφωση με όλες τις απαιτήσεις (νομικές, κανονιστικές ή άλλες) για την προστασία δεδομένων από αλλοίωση, απώλεια ή παραποίηση, σύμφωνα με την εφαρμοστέα νομοθεσία, περιλαμβάνοντας τη νομοθεσία περί προστασίας δεδομένων, Ευρωπαϊκούς Κανονισμούς και σχετικά Ευρωπαϊκά πρότυπα.

Για περιστατικά που σχετίζονται με Εγκεκριμένα Πιστοποιητικά για ηλεκτρονικές υπογραφές/σφραγίδες, εφαρμόζονται όλα τα προβλεπόμενα του άρθρου 19 του Ευρωπαϊκού Κανονισμού No. 910/2014 σχετικά με την ενημέρωση της Εθνικής Εποπτεύουσας Αρχής που είναι η Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ).

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 του Συστήματος Πιστοποιητικών. Σε περίπτωση που επιβεβαιωθεί παραβίαση, ελέγχεται αν υπάρχει παραβίαση σε ιδιωτικά κλειδιά της ΑΠ. Σε

περίπτωση παραβίασης χωρίς απώλεια ιδιωτικών κλειδιών της ΑΠ, 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 λειτουργία. Σε περίπτωση απώλειας κλειδιών της ΑΠ, ακολουθούνται οι διαδικασίες της παραγράφου 5.7.3.

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 κλειδιών που αντιστοιχούν σε πιστοποιητικά τελικών χρηστών/συσκευών, γίνεται ανάκλησή τους από την αρχή πιστοποίησης και έκδοση νέων, χωρίς την διακοπή της υπηρεσίας.
Σε περίπτωση απώλειας ιδιωτικού κλειδιού Ενδιάμεσης Αρχής Πιστοποίησης, ειδοποιούνται όλοι οι Συνδρομητές της αντίστοιχης 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 της, να προχωρήσει στην ανάκληση όλων των πιστοποιητικών, να εκδώσει μια τελευταία ΛΑΠ και τέλος να ειδοποιήσει τις σχετικές αρχές ασφάλειας κι εποπτείας. Στη συνέχεια η Υποδομή Δημοσίου Κλειδιού θα πρέπει να συσταθεί ξανά με δημιουργία νέων Αρχών Πιστοποίησης, ξεκινώντας από νέα Κορυφαία 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 σχέδιο επιχειρησιακής συνέχειας (business continuity plan). Το σχέδιο επιχειρησιακής συνέχειας περιλαμβάνει:

1. Τις συνθήκες ενεργοποίησης του πλάνου,
2. Επείγουσες διαδικασίες,
3. Εναλλακτικές διαδικασίες,
4. Διαδικασίες συνέχισης,
5. Πρόγραμμα συντήρησης για το πλάνο,
6. Απαιτήσεις επίγνωσης κι εκπαίδευσης,
7. Τις αρμοδιότητες των προσώπων,
8. Αντικειμενικός χρόνος επαναφοράς,
9. Τακτικοί έλεγχοι των εναλλακτικών πλάνων,
10. Το σχέδιο της ΑΠ να διατηρεί ή να επαναφέρει τις επιχειρησιακές λειτουργίες της έγκαιρα, μετά από διακοπή ή αποτυχία κρίσιμων διαδικασιών της,
11. Απαίτηση για αποθήκευση κρίσιμου κρυπτογραφικού υλικού (π.χ. ασφαλή διάταξη κρυπτογράφησης και αντικείμενα ενεργοποίησης) σε εναλλακτική τοποθεσία,
12. Ποια θεωρείται ως αποδεκτή απώλεια συστήματος και ποιος είναι ο αποδεκτός χρόνος επαναφοράς,

13. Πόσο συχνά λαμβάνονται αντίγραφα ασφαλείας ευαίσθητων επιχειρησιακών πληροφοριών και λογισμικών,
14. Την απόσταση από τις εγκαταστάσεις επαναφοράς μέχρι την κύρια τοποθεσία της ΑΠ, και
15. Διαδικασίες για τη διασφάλιση της λειτουργίας στο μέτρο του δυνατού κατά την περίοδο μετά από την καταστροφή και πριν από την αποκατάσταση, σε ασφαλές περιβάλλον είτε στην αρχική είτε σε άλλη τοποθεσία.

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

5.8 Τερματισμός Αρχής Πιστοποίησης ή Αρχής Καταχώρησης

Στην περίπτωση της προγραμματισμένης απόφασης τερματισμού της, η HARICA θα ενημερώνει τους Συνδρομητές, να μεταβούν σε κάποιον άλλο Πάροχο Υπηρεσιών Εμπιστοσύνης. Όταν έρθει η στιγμή του τερματισμού, κάθε Διαχειριστής Ενδιάμεσης ΑΠ ανακαλεί όλα τα πιστοποιητικά που έχουν εκδοθεί, ενημερώνει τη σχετική ΛΑΠ και ανακαλεί και το δικό της πιστοποιητικό. Αυτή η διαδικασία ανάκλησης περιλαμβάνει όλα τα Πιστοποιητικά Μονάδων Χρονοσήμανσης και το Πιστοποιητικό της Εκδούσας ΑΠ. Επιπλέον, ενημερώνει τις κατάλληλες αρχές και δημοσιοποιεί τον τερματισμό της λειτουργίας της. Σε κάθε περίπτωση ακολουθείται η εθνική κι Ευρωπαϊκή νομοθεσία νομοθεσία τερματισμού Αρχών Πιστοποίησης.

Στην περίπτωση μεταβίβασης των δραστηριοτήτων της HARICA σε άλλο διαπιστευμένο Πάροχο Υπηρεσιών Εμπιστοσύνης, υπάρχει ήδη ένα λεπτομερές σχέδιο μετάβασης και τερματισμού, το οποίο θα εφαρμοστεί. Όλοι οι συνδρομητές θα λάβουν την ειδοποίηση αυτής της μετάβασης για να αποφασίσουν αν επιθυμούν να αλλάξουν Πάροχο ή όχι. Κατά τη διάρκεια της μεταβίβασης των δραστηριοτήτων, όλες οι κρίσιμες διεργασίες προβλέπεται να λειτουργούν κανονικά.

Σε κάθε περίπτωση, τα αρχεία καταγραφής των ΑΚ /ΑΠ που σχετίζονται με τα αιτήματα πιστοποιητικών και την επαλήθευση αυτών, και όλα τα Πιστοποιητικά και η ανάκληση αυτών, φυλάσσονται για την περίοδο που αναφέρεται στην παράγραφο 5.5.2, με σημείο εκκίνησης τη λήξη εγκυρότητας του Πιστοποιητικού. Το διάστημα αυτό δύναται να τροποποιηθεί ανάλογα με τις εξελίξεις της σχετικής νομοθεσίας.

Όταν ένας άλλος δια-πιστοποιημένος Πάροχος Υπηρεσιών Εμπιστοσύνης σταματά όλες του τις λειτουργίες, συμπεριλαμβανομένης της διαχείρισης των ανακλήσεων, ανακαλούνται όλα τα δια-πιστοποιητικά που εκδόθηκαν σύμφωνα με την παράγραφο 3.2.6.

6 Έλεγχοι τεχνικής ασφάλειας

6.1 Δημιουργία ζεύγους κλειδιών και εγκατάσταση

6.1.1 Δημιουργία ζεύγους κλειδιών

6.1.1.1 Δημιουργία Ζεύγους Κλειδιού για Αρχές Πιστοποίησης και Μονάδες Χρονοσήμανσης

Τα Ζεύγη Κλειδιών των ΑΠ δημιουργούνται σε ασφαλές περιβάλλον και εγκαθίστανται σε ειδικές κρυπτοσυσκευές (Hardware Security Modules – HSMs). Οι ειδικές κρυπτοσυσκευές πρέπει να καλύπτουν τις προδιαγραφές που ορίζονται στην παράγραφο 6.2.1. Τα Ζεύγη Κλειδιών Μονάδων Χρονοσήμανσης, επίσης δημιουργούνται σε ασφαλές περιβάλλον από προσωπικό που κατέχει έμπιστους ρόλους με τουλάχιστον διπλό έλεγχο.

Πρέπει να ελέγχεται κατά το χρόνο δημιουργίας των κλειδιών η ύπαρξη πληροφοριών για σφάλματα του λογισμικού ή του υλικού που χρησιμοποιείται, και σχετίζεται με τη δημιουργία κλειδιών.

Για την έκδοση Ζεύγους Κλειδιών ΑΠ ή Πιστοποιητικό Μονάδας Χρονοσήμανσης, τηρείται προκαθορισμένη διαδικασία (τελετή δημιουργίας κλειδιών) η οποία εκτελείται παρουσία μελών εξουσιοδοτημένης Επιτροπής. Ειδικότερα για την έκδοση του Πιστοποιητικού Κορυφαίας (ROOT) Αρχής Πιστοποίησης ή Ενδιάμεσης ΑΠ Εξωτερικής Διαχείρισης, η διαδικασία είτε γίνεται παρουσία εξωτερικού ελεγκτή (auditor), είτε βιντεοσκοπείται η δημιουργία του Ζεύγους Κλειδιού της Αρχής Πιστοποίησης και στη συνέχεια αποστέλλεται σε εξωτερικό ελεγκτή ο οποίος εκδίδει σχετικό πόρισμα.

6.1.1.2 Δημιουργία Ζεύγους Κλειδιών για Αρχές Καταχώρησης

Δεν ορίζεται.

6.1.1.3 Δημιουργία Ζεύγους Κλειδιών Συνδρομητών

Τα κλειδιά των συνδρομητών δημιουργούνται από υλικό και κατάλληλο λογισμικό στην πλευρά των Αιτούντων ή σε εξ αποστάσεως Διάταξη Δημιουργίας Υπογραφής, και παραμένουν κάτω από τον απόλυτο έλεγχό τους, σε όλη τη διάρκεια ισχύος τους. Σε περίπτωση που κάποια Αρχή Πιστοποίησης επιτρέψει στις διαδικασίες της μαζική δημιουργία κλειδιών για λογαριασμό τρίτων, θα πρέπει να προβλέπεται η καταστροφή όλων των αντιγράφων ιδιωτικών κλειδιών μετά την παράδοσή τους στους χρήστες, ώστε στο τέλος τα ιδιωτικά κλειδιά να βρίσκονται μόνο στην κατοχή των δικαιούχων Συνδρομητών.

Αν ένα τελικό Πιστοποιητικό Συνδρομητή περιλαμβάνει την επέκταση extKeyUsage η οποία περιλαμβάνει είτε την τιμή `id-kp-serverAuth` [RFC5280] είτε `anyExtendedKeyUsage` [RFC5280], η HARICA ΔΕΝ θα δημιουργήσει Ζεύγος Κλειδιών για λογαριασμό του Συνδρομητή, και ΔΕΝ θα δεχθεί ένα αίτημα πιστοποιητικού που θα χρησιμοποιεί Ζεύγος Κλειδιών το οποίο δημιουργήθηκε κάποια στιγμή στο παρελθόν από τη HARICA.

Ειδικά για την περίπτωση που κάποιος Αιτών επιθυμεί να αποκτήσει πιστοποιητικό κλάσης Α, όπως περιγράφεται στην παράγραφο 3.2.3.1, θα πρέπει να

- υποβάλει την αίτηση με παρουσία εξουσιοδοτημένου τεχνικού της Αρχής Καταχώρησης ώστε να πιστοποιηθεί ότι η δημιουργία των κλειδιών θα γίνει σε κρυπτογραφική συσκευή, όπως περιγράφεται στην παράγραφο 6.2.1, ή
- μπορεί να λάβει μία κρυπτογραφική συσκευή όπως περιγράφεται στην παράγραφο 6.2.1, που θα περιέχει ήδη τα Κλειδιά τα οποία έχουν δημιουργηθεί νωρίτερα από εξουσιοδοτημένο προσωπικό της HARICA που κατέχει Έμπιστο Ρόλο και ακολουθούν τις διαδικασίες που περιγράφονται στην παράγραφο 6.1.2, ή
- χρησιμοποιήσει ειδική κρυπτοσυσκευή που επιβεβαιώνει μέσω λειτουργίας “key attestation” τη δημιουργία ασύμμετρου κλειδιού εντός της συσκευής και όχι την εισαγωγή του.

Οι Συνδρομητές μπορούν να χρησιμοποιούν εξ’ αποστάσεως Διατάξεις Δημιουργίας Υπογραφής ή κάποιο τρίτο μέρος που θα διαχειρίζεται ειδικό κρυπτογραφικό υλικό για λογαριασμό του υπογράφοντα. Σε αυτή την περίπτωση:

1. Η ενεργοποίηση του κλειδιού θα πρέπει να βασίζεται σε εξουσιοδότηση τουλάχιστον δύο χαρακτηριστικών (2-factor authentication – 2FA),
2. Δεν επιτρέπεται αντιγραφή του ιδιωτικού κλειδιού, εκτός από κατάλληλα τεκμηριωμένο σκοπό για την αδειάλειπτη παροχή της υπηρεσίας, και το αντίγραφο του κλειδιού πρέπει να προστατεύεται κατ’ ελάχιστο με τα ίδια μέτρα ασφαλείας όπως το πρωτότυπο,
3. Το τρίτο μέρος πρέπει να διαθέσει στην HARICA την τεκμηρίωση (τεχνική μελέτη, διαδικασίες και εφαρμογή) για τη διαχείριση του ειδικού κρυπτογραφικού υλικού,
4. Το τρίτο μέρος πρέπει να αποδέχεται σε ετήσιο έλεγχο συμμόρφωσης της υπηρεσίας με το κείμενο Πολιτικής Πιστοποίησης και/ή το κείμενο Διαδικασιών Πιστοποίησης ή θα πρέπει να Πιστοποιηθεί σύμφωνα με κατάλληλα διεθνή πρότυπα όπως τη σειρά CEN EN 419 241 ή αντίστοιχα από Διαπιστευμένο Φορέα Πιστοποίησης.

Η HARICA θα απορρίψει αιτήματα πιστοποιητικών αν μία ή περισσότερες από τις παρακάτω συνθήκες ικανοποιηθούν:

1. Το Ζεύγος Κλειδιών δεν ικανοποιεί τις απαιτήσεις της ενότητας 6.1.5 ή/και 6.1.6,
2. Υπάρχουν επαρκή στοιχεία που αποδεικνύουν ότι η συγκεκριμένη μέθοδος δημιουργίας Ιδιωτικού Κλειδιού ήταν ελαττωματική,
3. Η HARICA γνωρίζει κάποια επαληθεύσιμη ή αποδεδειγμένη μέθοδο που καθιστά το Ιδιωτικό Κλειδί του Αιτούμενου ευάλωτο,
4. Η HARICA έχει ενημερωθεί ότι το Ιδιωτικό Κλειδί του Αιτούμενου είναι εκτεθειμένο, όπως προβλέπεται στις διαδικασίες της ενότητας 4.9.1.1,
5. Η HARICA γνωρίζει κάποια επαληθεύσιμη μέθοδο με την οποία μπορεί εύκολα να υπολογιστεί το Ιδιωτικό Κλειδί του Αιτούμενου με βάση το Δημόσιο Κλειδί όπως Debian weak key (CVE-2008-01666) και ROCA (CVE-2017-15361).

Η HARICA θα απορρίπτει αιτήματα πιστοποιητικών που θα περιλαμβάνουν Δημόσιο Κλειδί που βρισκόταν σε Πιστοποιητικό που εκδόθηκε από τη HARICA το οποίο ανακλήθηκε λόγω του ότι το αντίστοιχο Ιδιωτικό Κλειδί είχε εκτεθεί.

6.1.2 Παράδοση Ιδιωτικού κλειδιού σε Συνδρομητή

Η HARICA απαγορεύεται να δημιουργήσει ζεύγος κλειδιών για λογαριασμό συνδρομητών όταν τα κλειδιά συνδέονται με Ψηφιακό Πιστοποιητικό για χρήση SSL/TLS αλλά επιτρέπεται για πιστοποιητικά άλλων χρήσεων.

Κατά τη δημιουργία ιδιωτικών κλειδιών εκ μέρους άλλης οντότητας ακολουθείται η παρακάτω διαδικασία ή αυστηρότερη:

- Αν η HARICA ή Ενδιάμεση ΑΠ έχει αρκετές πληροφορίες για να επιβεβαιώσει την ταυτότητα του χρήστη εκ των προτέρων, έχει την δυνατότητα να δημιουργήσει ζεύγος κλειδιών και πιστοποιητικό γι' αυτόν τον χρήστη.
- Η επαλήθευση ταυτότητας γίνεται όταν οι ιδιοκτήτες παραλαμβάνουν τα διαπιστευτήρια (πιστοποιητικό και κλειδιά) τους από την Αρχή Καταχώρησης. Το μοντέλο αυτό ονομάζεται «ομαδικό».
- Η HARICA ή μία Ενδιάμεση ΑΠ πρέπει να ακολουθούν μία διαδικασία διαγραφής του μυστικού κλειδιού που σχετίζεται με το κάθε ψηφιακό πιστοποιητικό μόλις αυτό παραδοθεί στον δικαιούχο Συνδρομητή, έτσι ώστε τελικά το ιδιωτικό κλειδί να βρίσκεται στην κατοχή αποκλειστικά του δικαιούχου Συνδρομητή.
- Σε περίπτωση που η HARICA ή η Ενδιάμεση ΑΠ αντιληφθεί ότι το Ιδιωτικό Κλειδί Συνδρομητή έχει δοθεί σε μη εξουσιοδοτημένο πρόσωπο ή οργανισμό που δεν σχετίζεται με τον Συνδρομητή, τότε η ΑΠ πρέπει να ανακαλέσει όλα τα πιστοποιητικά που περιέχουν το Δημόσιο Κλειδί που αντιστοιχεί σε αυτό το Ιδιωτικό Κλειδί.

Τα Ιδιωτικά Κλειδιά μπορεί να διανέμονται στους Συνδρομητές μέσω κρυπτογραφικής συσκευής. Σε αυτήν την περίπτωση:

1. Η HARICA εξασφαλίζει ότι το Ζεύγος Κλειδιών του Συνδρομητή δημιουργείται στην κρυπτογραφική συσκευή
2. Η HARICA λαμβάνει τα κατάλληλα μέτρα για να προστατέψει την κρυπτογραφική συσκευή από ενεργοποίηση, παραβίαση ή τροποποίηση κατά τη διαδικασία διανομής
3. Ο Συνδρομητής πρέπει να γνωστοποιήσει την παραλαβή της κρυπτογραφικής συσκευής
4. Η HARICA πρέπει να διανέμει την κρυπτογραφική συσκευή με τέτοιο τρόπο που εξασφαλίζει ότι οι σωστές κρυπτογραφικές συσκευές και δεδομένα ενεργοποίησης παραδόθηκαν στον σωστό Συνδρομητή
5. Η HARICA διανέμει τα δεδομένα ενεργοποίησης στον Συνδρομητή χρησιμοποιώντας ξεχωριστό ασφαλές κανάλι επικοινωνίας.

6.1.3 Παράδοση δημόσιου κλειδιού συνδρομητή στην Αρχή Πιστοποίησης

Ο Αιτών υποβάλλει στην Αρχή Καταχώρισης το δημόσιο κλειδί του μέσω δομημένης Αίτησης Υπογραφής Πιστοποιητικού (Certificate Signing Request) (π.χ. τύπου PKCS#10) για έκδοση πιστοποιητικού. Η αίτηση είναι υπογεγραμμένη με το σχετικό ιδιωτικό κλειδί. Περισσότερες πληροφορίες είναι διαθέσιμες στην παράγραφο 3.2.1.

6.1.4 Παράδοση του δημόσιου κλειδιού της Αρχής Πιστοποίησης σε βασιζόμενα μέρη

Τα Κορυφαία Πιστοποιητικά της HARICA διανέμονται κυρίως μέσω των Προμηθευτών Λογισμικού Εφαρμογών, μέσω κατάλληλων προγραμμάτων Κορυφαίων ΑΠ (π.χ. Microsoft , Apple , Mozilla). Τα Πιστοποιητικά Υφιστάμενων ΑΠ της HARICA, είναι διαθέσιμα για ασφαλή λήψη μέσω του αποθετηρίου πιστοποιητικών της HARICA όπως περιγράφεται στην παράγραφο 2.1. Τα Κορυφαία Πιστοποιητικά βρίσκονται επίσης στο Αξιόπιστο Μητρώο Παρόχων Υπηρεσιών Πιστοποίησης της Ευρωπαϊκής Ένωσης μέσω της Εθνικής Εποπτικής Αρχής (Ελληνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων). Τα Πιστοποιητικά Μονάδων Χρονοσήμανσης επίσης βρίσκονται στο Ευρωπαϊκό Αξιόπιστο Μητρώο Παρόχων που διανέμεται μέσω της Εθνικής Εποπτικής Αρχής (ΕΕΤΤ). Άλλες διαδικασίες παράδοσης περιλαμβάνουν παράδοση μέσω παραδοσιακού ταχυδρομείου και μετάδοση των αντίστοιχων αποτυπωμάτων μέσα από ένα εναλλακτικό κανάλι επικοινωνίας.

6.1.5 Μεγέθη κλειδιών

Για ζεύγη κλειδιών RSA η HARICA θα πρέπει να εξασφαλίσει ότι:

- το modulus size, κωδικοποιημένο, θα είναι τουλάχιστον 2048 bits, και
- το modulus size, σε bits, θα διαιρείται ακριβώς με το 8.

Για ζεύγη κλειδιών ECDSA η HARICA θα πρέπει να εξασφαλίσει ότι:

- το κλειδί εκπροσωπεί ένα έγκυρο σημείο στην ελλειπτική καμπύλη NIST P-256, NIST P-384 ή NIST P-521.

Οι ΑΠ που εκδίδουν πιστοποιητικά τύπου “codeSigning”, πρέπει να καταλήγουν μέσω της αλυσίδας πιστοποιητικών σε Αρχή Πιστοποίησης η οποία να έχει μέγεθος κλειδιού τουλάχιστον 4096 bits σε περίπτωση χρήσης αλγόριθμου RSA ή ECC NIST-P384 και πρέπει να υποστηρίζουν αλγόριθμο κατακερματισμού τύπου SHA2. Τα Ζεύγη Κλειδιών δημιουργούνται με χρήση αλγορίθμων και παραμέτρων σύμφωνα με τις τρέχουσες εξελίξεις της τεχνολογίας ακολουθώντας τις απαιτήσεις του προτύπου ETSI TS 119 312.

6.1.6 Παράμετροι δημιουργίας δημοσίων κλειδιών και έλεγχος ποιότητας

Οι παράμετροι δημιουργίας Δημοσίων Κλειδιών μπορεί να επιλέγονται από τους Συνδρομητές, αλλά επαληθεύονται από την ΑΚ και την ΑΠ. Τα Ζεύγη κλειδιών δημιουργούνται με χρήση ασφαλών αλγορίθμων και παραμέτρων σύμφωνα με τις τρέχουσες εξελίξεις της τεχνολογίας ακολουθώντας τις απαιτήσεις του προτύπου ETSI TS 119 312.

Για κλειδιά RSA, η HARICA θα επιβεβαιώνει ότι η τιμή του public exponent είναι μονός αριθμός που ισούται με 3 ή παραπάνω. Επιπλέον το public exponent προτείνεται να είναι στο διάστημα μεταξύ $2^{16}+1$ και $2^{256}-1$. Το modulus προτείνεται να έχει τα ακόλουθα χαρακτηριστικά [Πηγή: Ενότητα 5.3.3, NIST SP 800-89]:

- Μονός αριθμός
- Όχι δύναμη πρώτου αριθμού (prime) και
- να μην είναι ακέραιο πολλαπλάσιο αριθμού μικρότερου του 752.

Για κλειδιά ECDSA, η HARICA θα προσπαθήσει να επιβεβαιώνει την εγκυρότητα όλων των κλειδιών χρησιμοποιώντας είτε τη ρουτίνα ECC Full Public Key Validation ή την ECC Partial Public Key Validation. [Πηγή: Ενότητες 5.6.2.3.2 και 5.6.2.3.3 αντίστοιχα, NIST SP 800-56A: Revision 2].

Η HARICA πραγματοποιεί ελέγχους ποιότητας των κλειδιών που είναι να ενσωματωθούν σε Πιστοποιητικά κατά τη διαδικασία έκδοσης. Δείτε επίσης την ενότητα 6.1.1.3.

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

Τα Ιδιωτικά Κλειδιά που σχετίζονται με Κορυφαία Πιστοποιητικά δεν πρέπει να χρησιμοποιούνται για υπογραφή Πιστοποιητικών, ΕΚΤΟΣ από τις ακόλουθες περιπτώσεις:

1. Αυθυπόγραφα (Self-signed) Πιστοποιητικά που εκπροσωπούν την ίδια την Κορυφαία Αρχή Πιστοποίησης,
2. Πιστοποιητικά για υποκείμενες (Subordinate) Αρχές Πιστοποίησης και Δια-Πιστοποιητικά (Cross Certificates),
3. Πιστοποιητικά για σκοπούς διαχείρισης υποδομής (πιστοποιητικά για διαχειριστικούς ρόλους, πιστοποιητικά για συσκευές εσωτερικής διαχείρισης ΑΠ), και
4. Πιστοποιητικά για επαλήθευση απαντήσεων OCSP

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.

Περισσότερες πληροφορίες για τις επεκτάσεις των πιστοποιητικών βρίσκονται στην παράγραφο 7.1.2.

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

6.2 Προστασία ιδιωτικού κλειδιού και Έλεγχοι Προστασίας Κρυπτογραφικών συσκευών

6.2.1 Προδιαγραφές για κρυπτογραφικές μονάδες

Όλα τα ιδιωτικά κλειδιά ΑΠ και ΜΧΣ πρέπει να φυλάσσονται σε ασφαλείς κρυπτογραφικές διατάξεις (Hardware Security Modules – HSMs), οι οποίες 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 ασφαλών διατάξεων. Τα ιδιωτικά κλειδιά των ΑΠ και ΜΧΣ δεν μπορούν να εξαχθούν σε οποιαδήποτε μορφή και δεν είναι προσβάσιμα εκτός των ασφαλών κρυπτογραφικών διατάξεων.

Τα Ιδιωτικά Κλειδιά Συνδρομητών μπορεί να δημιουργούνται και να φυλάσσονται είτε μέσω λογισμικού είτε μέσω ασφαλών κρυπτογραφικών διατάξεων.

Αναφορικά με τους Συνδρομητές που χρησιμοποιούν Πιστοποιητικά Υπογραφής Κώδικα, η HARICA πρέπει να λάβει μια βεβαίωση από αυτούς ότι θα χρησιμοποιήσουν μία από τις ακόλουθες επιλογές για να δημιουργήσουν και να προστατεύσουν τα ιδιωτικά κλειδιά του Πιστοποιητικού Υπογραφής Κώδικα:

1. Μία μονάδα αξιόπιστης πλατφόρμας (Trusted Platform Module - TPM) που δημιουργεί και προστατεύει ένα ζεύγος κλειδιών και πιστοποιεί την προστασία του ιδιωτικού κλειδιού του Συνδρομητή μέσω ειδικού ελέγχου εγκυρότητας (TPM key attestation).
2. Μία ασφαλή κρυπτογραφική διάταξη που είναι πιστοποιημένη κατά FIPS 140 Level 2, ή Common Criteria EAL 4+, ή ισοδύναμο.
3. Άλλος τύπος συσκευής αποθήκευσης δεδομένων σε μορφή κάρτας Secure Digital (SD) ή USB token (χωρίς απαραίτητα να είναι πιστοποιημένη κατά FIPS 140 Level 2 ή Common Criteria EAL 4+). Ο Συνδρομητής πρέπει να εγγυάται επίσης, ότι θα φυλάσσει την διάταξη σε ξεχωριστό μέρος από την συσκευή που φιλοξενεί τη λειτουργία της υπογραφής κώδικα όσο δεν απαιτείται διαδικασία υπογραφής.

Στις περιπτώσεις Πιστοποιητικών EV υπογραφής κώδικα, η HARICA πρέπει να εξασφαλίσει ότι το ιδιωτικό κλειδί του Συνδρομητή έχει δημιουργηθεί, αποθηκευτεί και χρησιμοποιείται σε ειδική κρυπτοσυσκευή που πληροί ή ξεπερνά τα ακόλουθα κριτήρια:

- FIPS 140-2 level 2, ή
- Common Criteria (ISO 15408 & ISO 18045) - Protection Profiles CEN prEN 14169 (όλα τα μέρη που εφαρμόζονται στον τύπο της συσκευής) ή πρότυπα όπως η σειρά CEN EN 419 241 ή αντίστοιχα, για εξ' αποστάσεως διαχειριζόμενες συσκευές, ή
- ενός Κράτους Μέλους της Ευρωπαϊκής Ένωσης ως Εγκεκριμένη Διάταξη Δημιουργίας Υπογραφής (ΕΔΔΥ) μετά την 1η Ιουλίου 2016, ή ήταν αναγνωρισμένη ως «Ασφαλής Διάταξη Δημιουργίας Υπογραφής (ΑΔΔΥ) από Εποπτική Αρχή Κράτους Μέλους της ΕΕ πριν την 1η Ιουλίου 2016.
- **Από 2021-02-01**, μόνο Εγκεκριμένες Διατάξεις Δημιουργίας Υπογραφής/Σφραγίδας θα επιτρέπεται να χρησιμοποιηθούν για τη δημιουργία Ζεύγους Κλειδιών που θα συσχετίζονται με Πιστοποιητικά για Εγκεκριμένες Ηλεκτρονικές Υπογραφές/Σφραγίδες.

Ειδικοί έλεγχοι πρέπει να είναι τοποθετημένοι για να διασφαλίζουν ότι κάθε κρυπτογραφικό υλικό δεν έχει τροποποιηθεί και λειτουργεί κανονικά. Η ακεραιότητα του υλικού και του λογισμικού που χρησιμοποιείται για τη δημιουργία κλειδιών, καθώς και κάθε διεπαφή που χρησιμοποιείται για να αποκτήσει πρόσβαση στο υλικό και το λογισμικό, πρέπει να ελέγχεται πριν την παραγωγική λειτουργία.

Στις περιπτώσεις Εγκεκριμένων Πιστοποιητικών σε Εγκεκριμένες Διατάξεις Δημιουργίας Υπογραφής/Σφραγίδας (QSCD) (πιστοποιητικά «κλάσης Α»), το ιδιωτικό κλειδί πρέπει να δημιουργείται και να αποθηκεύεται σε εγκεκριμένη διάταξη δημιουργίας υπογραφής/σφραγίδας (ΕΔΔΥ) και δεν μπορεί να εξαχθεί σε καμία

μορφή. Οι ΕΔΔΥ 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.

Η HARICA παρακολουθεί σχετικές πληροφορίες για ΕΔΔΥ πιστοποιήσεις χρησιμοποιώντας μια πληροφοριακού χαρακτήρα λίστα από Πιστοποιημένες ΕΔΔΥ του Ευρωπαϊκού Συμβουλίου σύμφωνα με το Άρθρο 31 του Κανονισμού (ΕΕ) 2014/910:

- https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds.

Για εξ αποστάσεως ΕΔΔΥ που διαχειρίζονται Ιδιωτικά Κλειδιά για λογαριασμό των Συνδρομητών, η HARICA παρακολουθεί τη συμμόρφωση με το σχετικό Security Target που ορίστηκε κατά Common Criteria για την εξ αποστάσεως ΕΔΔΥ. Τα εν λόγω Πιστοποιητικά, περιλαμβάνουν ένα επιπλέον αναγνωριστικό πολιτικής (policy OID) σύμφωνα με την ενότητα 7.1.6

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

Οι διαδικασίες ενεργοποίησης ιδιωτικού κλειδιού της κάθε ΑΠ (συμπεριλαμβανομένων των αντιγράφων ασφαλείας) γίνονται σύμφωνα με όσα περιγράφονται στην παράγραφο 5.2.2.

6.2.3 Μεσεγγύηση ιδιωτικού κλειδιού

Η HARICA δεν παρέχει αυτή τη στιγμή υπηρεσίες μεσεγγύησης.

6.2.4 Αντίγραφα ασφαλείας ιδιωτικού κλειδιού

Το ιδιωτικό κλειδί κάθε Αρχής Πιστοποίησης πρέπει να φυλάσσεται σε αντίγραφο ασφαλείας. Τα ιδιωτικά κλειδιά Μονάδων Χρονοσήμανσης μπορεί να φυλάσσονται σε αντίγραφο ασφαλείας. Το αντίγραφο του ιδιωτικού κλειδιού της ΑΠ και της ΜΧΣ πρέπει να είναι κρυπτογραφημένα και να ακολουθούνται οι διαδικασίες που περιγράφονται στην παράγραφο 5.1.6. Η πρόσβαση στο αντίγραφο ασφαλείας επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό που κατέχει Έμπιστο ρόλο. Η επαναφορά κλειδιών ΑΠ και ΜΧΣ από αντίγραφα ασφαλείας απαιτεί ενέργειες από τουλάχιστον δύο φυσικά πρόσωπα σε Έμπιστους Ρόλους σε χώρο που είναι φυσικά προστατευμένος. Όλα τα αντίγραφα ιδιωτικών κλειδιών των ΑΠ και ΜΧΣ προστατεύονται ώστε να εξασφαλίζεται από την κρυπτογραφική συσκευή η ακεραιότητα και η εμπιστευτικότητά τους πριν αποθηκευτούν εκτός αυτής.

Η τήρηση αντιγράφων ασφαλείας για τα ιδιωτικά κλειδιά πιστοποιητικών Συνδρομητών (εφόσον επιτρέπεται τεχνικά η συγκεκριμένη δυνατότητα), είναι αποκλειστικά στην ευχέρεια και ευθύνη των Συνδρομητών.

6.2.5 Αρχειοθέτηση αντιγράφων ασφαλείας ιδιωτικών κλειδιών

Το αντίγραφο ασφαλείας του ιδιωτικού κλειδιού κάθε Αρχής Πιστοποίησης και Μονάδας Χρονοσήμανσης 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 Πιστοποίησης και Μονάδων Χρονοσήμανσης που έχουν λήξει, αποσύρονται και δεν ξαναχρησιμοποιούνται.

6.2.6 Μεταφορά Ιδιωτικού Κλειδιού από και προς ένα κρυπτογραφικό σύστημα

Οι κάτοχοι των ιδιωτικών κλειδιών, μπορούν να μεταφέρουν κατά την κρίση τους το ιδιωτικό κλειδί τους από αποθετήριο πιστοποιητικών ενός λογισμικού (software certificate store) σε οποιαδήποτε κρυπτογραφική συσκευή (hardware) π.χ. κρυπτογραφικές συσκευές USB, έξυπνες κάρτες. 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 μονάδα αποθήκευσης πιστοποιητικών μορφής υλικού σε μονάδα αποθήκευσης μορφής λογισμικού) δεν επιτρέπεται.
Όλες οι μεταφορές Ιδιωτικών Κλειδιών ΑΠ από και προς μια κρυπτογραφική συσκευή γίνονται σύμφωνα με τις διαδικασίες που ορίζει ο κατασκευαστής αυτής της συσκευής.

6.2.7 Αποθήκευση ιδιωτικού κλειδιού σε κρυπτογραφική συσκευή

Τα ιδιωτικά κλειδιά των ΑΠ και Μονάδων Χρονοσήμανσης πρέπει να βρίσκονται εγκατεστημένα σε ειδική Κρυπτοσυσκευή προκειμένου να εκτελέσουν εργασίες υπογραφής. Τα ιδιωτικά κλειδιά των συνδρομητών μπορούν επίσης να δημιουργηθούν σε κρυπτογραφική συσκευή. Ειδικά για την περίπτωση Εγκεκριμένων Πιστοποιητικών για «Εγκεκριμένες» ηλεκτρονικές σφραγίδες/υπογραφές, το ιδιωτικό κλειδί πρέπει να δημιουργηθεί σε ΑΔΔΥ ή σε ΕΔΔΥ και δεν μπορεί να μπορεί να εξαχθεί από αυτήν με κανένα μηχανισμό.

Οι κρυπτογραφικές συσκευές για ειδικές κατηγορίες πιστοποιητικών, πρέπει 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) ένα ιδιωτικό κλειδί;

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

Τα ιδιωτικά κλειδιά που αντιστοιχούν σε πιστοποιητικά Συνδρομητών πρέπει να τηρούνται επίσης προστατευμένα-κρυπτογραφημένα. Ο κάτοχος κάθε πιστοποιητικού είναι υπεύθυνος για την ενεργοποίηση και προστασία του ιδιωτικού κλειδιού που αντιστοιχεί στο σχετικό πιστοποιητικό.

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 (tokens) ταυτοποίησης/εξουσιοδότησης πρόσβασης. Κάθε εξουσιοδοτημένο μέλος με κλειδί ενεργοποίησης κατέχει διαφορετικό στοιχείο (token) των συστατικών ενεργοποίησης.

Μόνο ένας συνδυασμός από εξουσιοδοτημένα μέλη με κλειδί ενεργοποίησης μπορεί να ενεργοποιήσει ένα ιδιωτικό κλειδί.

Για την περίπτωση ιδιωτικού κλειδιού Συνδρομητή σε κρυπτογραφική συσκευή απαιτείται ειδικός κωδικός PIN. Αν τα ιδιωτικά κλειδιά Συνδρομητή είναι αποθηκευμένα σε αποθετήρια πιστοποιητικών λογισμικών (π.χ. 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 άλλα αντίστοιχα μέτρα 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 ένα Κορυφαίο Πιστοποιητικό, το κλειδί παραμένει «ενεργό» μόνο για το διάστημα που απαιτείται να εκτελεστούν κρυπτογραφικές διαδικασίες π.χ. υπογραφή Ενδιάμεσης ΑΠ, υπογραφή Πιστοποιητικού OCSP ή δημιουργία ΛΑΠ.

6.2.9 Μέθοδοι απενεργοποίησης ιδιωτικών κλειδιών.

Δεν ορίζεται.

6.2.10 Μέθοδοι καταστροφής ιδιωτικών κλειδιών.

Όταν η ΑΠ φτάνει στο τέλος της διάρκειας ζωής της το ιδιωτικό κλειδί καταστρέφεται με ασφάλεια σύμφωνα με τη διαδικασία διαγραφής της ειδικής κρυπτογραφικής συσκευής (HSM) που ορίζει ο κατασκευαστής αυτής, υπό την μέθοδο του διπλού ελέγχου που περιγράφεται στην παράγραφο 5.2.2. Η καταστροφή αυτή, επηρεάζει μόνο την «φυσική» παρουσία του κλειδιού που φυλάσσεται στην κρυπτογραφική συσκευή. Τα άλλα αντίγραφα ασφαλείας διαγράφονται χρησιμοποιώντας ασφαλείς διαδικασίες διαγραφής, χρησιμοποιώντας το σύστημα ασφαλούς διαγραφής 5220.22-M του Υπουργείου Άμυνας των ΗΠΑ ή ισχυρότερο.

Καθώς όλα τα αρχεία αντιγράφων ασφαλείας των Ιδιωτικών Κλειδιών ΑΠ και ΜΧΣ κρυπτογραφούνται μέσω συμμετρικού “Master Backup Key”, μια επιπλέον μέθοδος καταστροφής των συγκεκριμένων αντιγράφων ασφαλείας είναι η καταστροφή του “Master Backup Key” που καθιστά όλα τα κρυπτογραφημένα αντίγραφα ασφαλείας πρακτικά αδύνατο να χρησιμοποιούν (δεν μπορούν να αποκρυπτογραφηθούν).

Τα Ιδιωτικά Κλειδιά ΜΧΣ που φτάνουν στο τέλος της διάρκειας ζωής τους σύμφωνα με την παράγραφο 6.3.2, διαγράφονται με τέτοιον τρόπο που είναι πρακτικά αδύνατο να χρησιμοποιηθούν και να εκδώσουν νέα Χρονοσήμανση.

Οι συνδρομητές μπορούν να καταστρέψουν τα ιδιωτικά τους κλειδιά μόνοι τους.

6.2.11 Βαθμολόγηση-αξιολόγηση κρυπτογραφικών συστημάτων

Περιγράφεται στην παράγραφο 6.2.1.

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 του πιστοποιητικού και του ζεύγους κλειδιού

Η διάρκεια χρήσης ενός ζεύγους κλειδιού ξεκινά όταν το δημόσιο κλειδί περιλαμβάνεται για πρώτη φορά σε ψηφιακό πιστοποιητικό που γνωρίζει η HARICA (μέσω αιτήματος CSR από τον Αιτούμενο). Ανάλογα με το είδος του Πιστοποιητικού, η HARICA έχει διαφορετικές διάρκειες χρήσης του ζεύγους κλειδιών.

Η μέγιστη διάρκεια χρήσης των κλειδιών ορίζεται σε

- **είκοσι (20)** έτη για ένα Πιστοποιητικό Κορυφαίας ΑΠ,
- **δεκαπέντε (15**) έτη για ένα Πιστοποιητικό Ενδιάμεσης ΑΠ,
- **τρία (3) έτη** για πιστοποιητικά τελικών χρηστών Αυθεντικοποίησης Πελάτη (Client Authentication), υπογραφής εγγράφων (Document Signing) και S/MIME,
- **δύο (2)** για Πιστοποιητικά χρήσης SSL/TLS και Υπογραφής Κώδικα και
- **δέκα (10)** έτη για πιστοποιητικά Μονάδων Χρονοσήμανσης. Για την περίπτωση Μονάδων Χρονοσήμανσης, νέο Πιστοποιητικό της ΜΧΣ με νέο ιδιωτικό κλειδί πρέπει να δημιουργείται το αργότερο μέσα σε **δεκαπέντε (15) μήνες**.

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.

Η μέγιστη διάρκεια εγκυρότητας Πιστοποιητικών ορίζεται σε:

- **Είκοσι-πέντε (25)** έτη για Πιστοποιητικό Κορυφαίας ΑΠ,
- **Δεκαπέντε (15)** έτη για ένα Πιστοποιητικό Ενδιάμεσης ΑΠ,
- **τρία (3) έτη** για πιστοποιητικά τελικών χρηστών Αυθεντικοποίησης Πελάτη (Client Authentication), υπογραφής εγγράφων (Document Signing) και S/MIME,
- **δύο (2)** για Πιστοποιητικά Υπογραφής Κώδικα
- **Τριακόσιες ενενήντα επτά (397)** ημέρες για Πιστοποιητικά χρήσης SSL/TLS,
- **δέκα (10)** έτη για πιστοποιητικά Μονάδων Χρονοσήμανσης και Χρονοσήμανσης EV.

6.4 Δεδομένα ενεργοποίησης

6.4.1 Δημιουργία και εγκατάσταση δεδομένων ενεργοποίησης και εγκατάσταση

Δεν ορίζεται.

6.4.2 Προστασία δεδομένων ενεργοποίησης

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)** χαρακτήρες. 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.

6.4.3 Άλλα θέματα δεδομένων ενεργοποίησης

Δεν ορίζεται.

6.5 Έλεγχοι ασφάλειας υπολογιστών

6.5.1 Συγκεκριμένες τεχνικές απαιτήσεις ασφάλειας

- Τα Λειτουργικά Συστήματα των υπολογιστών της ΥΔΚ HARICA φυλάσσονται με υψηλό επίπεδο ασφάλειας εφαρμόζοντας όλα τα διεθνή πρότυπα και τις οδηγίες ασφάλειας.
- Συστήματα καταγραφής ενεργειών και συναγερμού που υπάρχουν στους υπολογιστές της ΥΔΚ HARICA ελέγχονται τακτικά ενώ τα αρχεία καταγραφής μελετώνται προσεκτικά για διαπίστωση τυχόν ανωμαλιών και προσπαθειών παραβίασης, προκειμένου να ενεργοποιηθούν διαδικασίες επέμβασης. Οι διαδικασίες επέμβασης σε τέτοια περιστατικά προβλέπουν το προσωπικό να παρέμβει το συντομότερο δυνατό προκειμένου να περιορίσει το μέγεθος της παραβίασης ασφάλειας.
- Τα προγράμματα που συνοδεύουν το Λειτουργικό Σύστημα είναι τα απολύτως απαραίτητα για την εύρυθμη λειτουργία των ΑΚ/ΑΠ και οι υπολογιστές 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.
- Η ΥΔΚ της HARICA υποχρεώνει πολύ-παραγοντικό έλεγχο ταυτότητας για όλους τους λογαριασμούς διαχειριστών που σχετίζονται με την έκδοση πιστοποιητικού.

6.5.2 Βαθμολόγηση ασφάλειας υπολογιστών

Δεν ορίζεται.

6.6 Κύκλος ζωής τεχνικών ελέγχων

6.6.1 Έλεγχοι ανάπτυξης συστημάτων

Στο λογισμικό της ΥΔΚ της HARICA εφαρμόζονται ασφαλείς διαδικασίες όσον αφορά την ανάπτυξη του πριν χρησιμοποιηθεί στο περιβάλλον παραγωγής .

6.6.2 Έλεγχοι διαχείρισης ασφάλειας

Η ΥΔΚ της HARICA αναφορικά με την ασφάλεια του δικτύου, ακολουθεί τις κατευθυντήριες γραμμές της παραγράφου 7.8 του ETSI EN 319 401. Επιπλέον, η HARICA ακολουθεί τις προδιαγραφές ασφάλειας που περιγράφονται στο "Network and Certificate System Security Requirements" του CA/Browser Forum.

6.6.3 Κύκλος ζωής ελέγχων ασφάλειας

Η ΥΔΚ της HARICA εφαρμόζει εσωτερικές διαδικασίες προκειμένου να εξασφαλίσει ότι οι Φυσικοί Εξυπηρετητές, οι κρυπτογραφικές συσκευές και μονάδες κρυπτογράφησης που χρησιμοποιούνται σε κρίσιμες λειτουργίες της ΥΔΚ παραμένουν απαραβίαστες κατά τη διάρκεια μεταφοράς ή αποθήκευσης. Όλες οι κρίσιμες συσκευές για τη λειτουργία της ΥΔΚ βρίσκονται σε φυσικά ασφαλισμένο χώρο.

6.7 Έλεγχοι ασφάλειας δικτύου

Οι εξυπηρετητές των ΑΠ/ΑΚ λειτουργούν πίσω από τείχος προστασίας που επιτρέπει την πρόσβαση μόνο σε εξουσιοδοτημένους άλλους εξυπηρετητές και μόνο σε θύρες που χρησιμοποιούνται για τη διαχείριση της ΑΠ και την έκδοση Πιστοποιητικών ή Χρονοσφραγίδων. Η δικτυακή μετάδοση ευαίσθητων πληροφοριών προστατεύεται με κρυπτογράφηση για να εξασφαλιστεί η ακεραιότητα και η εμπιστευτικότητα τους.

6.8 Χρονοσήμανση

Στην ΥΔΚ της HARICA λειτουργεί Εγκεκριμένη Αρχή Χρονοσήμανσης.

6.8.1 Έκδοση Χρονοσφραγίδων

Οι Χρονοσφραγίδες συμμορφώνονται με το πρότυπο ETSI EN 319 422, εκδίδονται με ασφάλεια και αναπαριστούν τον σωστό χρόνο σύμφωνα με την ΣΠΩ (UTC).

Αν διαπιστωθεί ότι το ρολόι της ΜΧΣ έχει χάσει την καθορισμένη ακρίβεια του τότε δεν εκδίδονται Χρονοσφραγίδες μέχρι να συγχρονιστεί.

Οι Χρονοσφραγίδες υπογράφονται με κλειδί που δημιουργείται αποκλειστικά γι'αυτόν τον σκοπό και σχετίζεται με Πιστοποιητικό ΜΧΣ.

Χρονοσφραγίδες δεν παράγονται στο τέλος της διάρκειας ισχύος του Ιδιωτικού Κλειδιού της ΜΧΣ.

6.8.2 Μονάδα Χρονοσήμανσης

Οι ΜΧΣ που λειτουργούν στην ΥΔΚ της HARICA πρέπει να έχουν μοναδικό κλειδί υπογραφής χρονοσήμανσης κάθε φορά. Η ισχύς του ιδιωτικού κλειδιού που χρησιμοποιείται για να υπογράφει στοιχεία χρονοσήμανσης ορίζεται στην παράγραφο 6.3.2.

Τα κλειδιά που επαληθεύουν την υπογραφή ΜΧΣ είναι διαθέσιμα σε βασιζόμενα μέρη σε δημόσιο πιστοποιητικό που χρησιμοποιεί timestamping EKU (παράγραφος 7.1.2 και ΠΑΡΑΡΤΗΜΑ Β (Περιγράμματα Κοινών Πιστοποιητικών HARICA).

Στις ΜΧΣ αντιστοιχεί ένα Ζεύγος Κλειδιών που παράγεται αποκλειστικά για υπηρεσίες Χρονοσήμανσης.

Οι ΜΧΣ χρησιμοποιούν αλγόριθμο κατακερματισμού SHA2 στα δεδομένα που παίρνουν χρονοσήμανση.

Η ΥΔΚ της HARICA χρησιμοποιεί ξεχωριστά σημεία πρόσβασης της υπηρεσίας και διαφορετικές ΜΧΣ ως προς το όνομα του υποκειμένου (subject) του δημοσίου κλειδιού του πιστοποιητικού τους, για να διακρίνουν υπογεγραμμένες Εγκεκριμένες Χρονοσφραγίδες από μη Εγκεκριμένες.

6.8.3 Τεκμήρια Χρονοσήμανσης

Τεκμήρια Χρονοσήμανσης (TSTs) που υπογράφονται από ΜΧΣ της ΥΔΚ της HARICA εκδίδονται με ασφάλεια και περιλαμβάνουν ακριβή αναπαράσταση του χρόνου σύμφωνα με την Παγκόσμια Ώρα. Ο χρόνος που χρησιμοποιεί μια ΜΧΣ σε μια χρονοσήμανση, έχει διαδρομή ελέγχου σε τουλάχιστον μία πραγματική τιμή που διανέμει ένα αναγνωρισμένο εργαστήριο UTC(k).

Κάθε τεκμήριο χρονοσήμανσης συμμορφώνεται με τις απαιτήσεις του προτύπου ETSI EN 319 422 και περιλαμβάνει:

- το αναγνωριστικό `policy` για την πολιτική που ακολουθεί η χρονοσήμανση όπως ορίζεται στην παράγραφο 7.1.8,
- ένα πεδίο `genTime` που έχει τιμή που αναπαριστά τον χρόνο με την λεπτομέρεια που είναι απαραίτητη για να υποστηρίξει την καθορισμένη ακρίβεια,
- το πεδίο `accuracy` με ελάχιστη ακρίβεια ενός (1) δευτερολέπτου σε σύγκριση με την ΣΠΩ (UTC), ανιχνεύσιμο σε πάροχο ΣΠΩ,
- ένα μοναδικό σειριακό αριθμό για κάθε TST,
- μία ηλεκτρονική υπογραφή που δημιουργείται με κλειδί που χρησιμοποιείται αποκλειστικά για χρονοσήμανση και
- μια παράμετρο `signerInfo` για την αναγνώριση της ΜΧΣ.

6.8.4 Συγχρονισμός ρολογιού με την ΣΠΩ

Για τον συγχρονισμό του ρολογιού ισχύουν οι ακόλουθες απαιτήσεις:

- Η προσαρμογή του ρολογιού της ΜΧΣ πρέπει να διατηρείται έτσι ώστε τα ρολόγια να μην αποκλίνουν από την καθορισμένη ακρίβεια.
- Αν διαπιστωθεί ότι ο χρόνος που εμφανίζεται σε χρονοσφραγίδα αποκλίνει ή είναι εκτός συγχρονισμού με την ΣΠΩ, η ΜΧΣ σταματά την έκδοση χρονοσφραγίδων.
- Ο συγχρονισμός του ρολογιού διατηρείται όταν γίνεται αντιληπτή απόκλιση ενός δευτερολέπτου από κατάλληλο όργανο.

Η ΥΔΚ της HARICA συγχρονίζει και προσαρμόζει συνεχώς το ρολόι (τουλάχιστον κάθε ώρα) με πηγές ΣΠΩ. Στο απίθανο γεγονός που το ρολόι της ΜΧΣ αποκλίνει από την καθορισμένη ελάχιστη ακρίβεια και αποτύχει ο επανασυντονισμός, η ΜΧΣ σταματά την έκδοση χρονοσφραγίδων μέχρι να συντονιστεί κατάλληλα το ρολόι.

Η ΥΔΚ της HARICA διατηρεί αρχείο συναλλαγών συμβάντων για όλες τις προσαρμογές του ρολογιού με την ΣΠΩ.

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".

Διευκρινίζεται ότι, όπως περιγράφεται στο RFC 6962 – Certificate Transparency, ένα Pre-certificate δεν θεωρείται «Πιστοποιητικό» που υπόκειται στις απαιτήσεις του RFC 5280.

Τεχνικά περιορισμένα Πιστοποιητικά Ενδιάμεσων ΑΠ χρησιμοποιούν την επέκταση «Περιορισμοί Ονόματος» (Name Constraints), που περιγράφεται στην παράγραφο 7.1.5 και αναφέρεται ως «μη-κρίσιμη». Αυτό αποτελεί εξαίρεση στο RFC 5280 (4.2.1.10) που επιτρέπεται σύμφωνα με τα πρότυπα του CA/Browser Forum, μέχρι η επέκταση «Περιορισμοί Ονόματος» (Name Constraints) να υποστηρίζεται από Προμηθευτές Λογισμικού Εφαρμογών των οποίων το λογισμικό χρησιμοποιείται από μία σημαντική μερίδα των Βασιζόμενων Μερών παγκοσμίως.

7.1.1 Έκδοση

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

7.1.2 Επεκτάσεις Πιστοποιητικού

Κάθε πιστοποιητικό που εκδίδεται περιλαμβάνει επεκτάσεις που ορίζονται στο πρότυπο Πιστοποιητικών X.509v3. Ακολουθεί μία λίστα επεκτάσεων που χρησιμοποιούνται από την ΥΔΚ της HARICA. Η λίστα δεν είναι περιοριστική.

- `basicConstraints` (κρίσιμη): 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 σε πιστοποιητικά τελικών χρηστών/συσκευών.
- `keyUsage` (κρίσιμη): Ορίζει τον σκοπό χρήσης του κλειδιού που περιέχεται στο Πιστοποιητικό. Για τις ΑΠ, παίρνει τις τιμές *digitalSignature, keyCertSign* και *cRLSign*. Για πιστοποιητικά τελικών χρηστών/συσκευών, οι πιθανές τιμές περιλαμβάνουν *digitalSignature* (επαλήθευση ταυτότητας), *nonrepudiation* (ψηφιακή υπογραφή και μη αποποίηση ευθύνης αλλά χρησιμοποιείται μόνο σε συνδυασμό με το *digitalSignature*), *keyEncipherment* (κρυπτογράφηση).
- `certificatePolicies`: περιγράφεται στην παράγραφο 7.1.6
- `cRLDistributionPoints` (όχι κρίσιμη): Περιλαμβάνει ένα URL για την ΛΑΠ του πιστοποιητικού της Εκδούσας ΑΠ
- `authorityInformationAccess`: Δείχνει το URL του OCSP Responder και μπορεί επίσης να περιλαμβάνει το URL για το πιστοποιητικό της εκδούσας ΑΠ
- Authority Key Identifier: Παρέχει πληροφορίες αναγνώρισης του Δημοσίου Κλειδιού που αντιστοιχεί στο Ιδιωτικό Κλειδί που χρησιμοποιήθηκε για να

υπογράψει ένα πιστοποιητικό. Αυτό το πεδίο περιέχει το αναγνωριστικό "Subject Key Identifier" του Πιστοποιητικού της εκδούσας ΑΠ
    - Για Πιστοποιητικά ΑΠ, ενδέχεται να περιλαμβάνει το HTTP URL του OCSP Responder της εκδούσας ΑΠ (accessMethod = 1.3.6.1.5.5.7.48.1).
    - Για τελικά Πιστοποιητικά, ΠΡΕΠΕΙ να περιλαμβάνει το HTTP URL του OCSP Responder της εκδούσας ΑΠ (accessMethod = 1.3.6.1.5.5.7.48.1).
- Subject Key Identifier: Αναγνωρίζει μοναδικά ένα Δημόσιο Κλειδί. Περιέχει το ID του κλειδιού του Κατόχου του Πιστοποιητικού
- Subject Information: Όπως ορίζεται στην παράγραφο 7.1.4.7
- Subject Alternative Name (απαιτείται για Πιστοποιητικά χρήσης SSL/TLS και S/MIME): Παρέχει διάφορες τιμές που αφορούν σε διεύθυνση email, Microsoft UPN, όνομα χώρου (DNS) ή ένα URI
- Extended Key Usage (EKU): Δείχνει έναν ή περισσότερους σκοπούς χρήσης πιστοποιητικού. Μπορεί να περιέχει τις ακόλουθες τιμές :
    - serverAuth (OID: 1.3.6.1.5.5.7.3.1)
    - clientAuth (OID: 1.3.6.1.5.5.7.3.2)
    - codeSigning (OID: 1.3.6.1.5.5.7.3.3)
    - emailProtection (OID: 1.3.6.1.5.5.7.3.4)
    - IP Sec EndSystem (OID: 1.3.6.1.5.5.7.3.5)
    - IP Sec Tunnel (OID: 1.3.6.1.5.5.7.3.6)
    - IP Sec User (OID: 1.3.6.1.5.5.7.3.7)
    - TimeStamping (OID: 1.3.6.1.5.5.7.3.8)
    - OCSP Signing (OID: 1.3.6.1.5.5.7.3.9)
    - smartcardlogon (OID: 1.3.6.1.4.1.311.20.2.2)
    - Encrypting File System (OID: 1.3.6.1.4.1.311.10.3.4)
    - Document Signing (OID: 1.3.6.1.4.1.311.10.3.12)
    - Lifetime Signing (OID: 1.3.6.1.4.1.311.10.3.13)

Δεν πρέπει να χρησιμοποιείται μία μοναδική Εκδούσα ΑΠ για να εκδίδει πιστοποιητικά που συνδυάζουν τις επεκτάσεις χρήσης κλειδιών `id-kp-serverAuth` [RFC5280], `id-kp-emailProtection` [RFC5280], `id-kp-codeSigning` [RFC5280] και `id-kp-timestamping` [RFC5280]. Νέες Εκδούσες ΑΠ πρέπει να διαχωρίζουν τις Επεκτάσεις Χρήσης Κλειδιών για Επαλήθευση Ταυτότητας Εξυπηρετητή, S/MIME, Υπογραφή Κώδικα και Χρονοσήμανση. Από την **1η Ιουνίου 2020**, η τιμή `id-kp-ocspSigning` [RFC5280] ΔΕΝ ΠΡΕΠΕΙ να χρησιμοποιείται στην επέκταση EKU Πιστοποιητικών ΑΠ.

- Qualified Certificate Statements (qcStatements): Αν το Πιστοποιητικό χρησιμοποιείται όπως ορίζεται στον Κανονισμό (EU) No. 910/2014, η συγκεκριμένη επέκταση περιέχει χαρακτηριστικά/τιμές για να μεταβιβάσει πληροφορίες στα Βασιζόμενα Μέρη. Η τιμή "`id-etsi-qcs-QcCompliance`" ορίζει ότι πρόκειται για Πιστοποιητικό ηλεκτρονικών υπογραφών/σφραγίδων σε συμμόρφωση με τον Ευρωπαϊκό Κανονισμό 910/2014 και ΠΡΕΠΕΙ να υπάρχει πάντοτε σε Πιστοποιητικά που αφορούν Προηγμένες/Εγκεκριμένες ηλεκτρονικές υπογραφές/σφραγίδες. Επιπρόσθετα, τα Πιστοποιητικά για Εγκεκριμένες ηλεκτρονικές υπογραφές/σφραγίδες ΠΡΕΠΕΙ να περιέχουν την τιμή "`id-etsi-qcs-`

`QcSSCD`", η οποία διαβεβαιώνει ότι το ιδιωτικό κλειδί δημιουργήθηκε σε ΑΔΔΥ/ΕΔΔΥ. Επιτρέπονται πρόσθετες τιμές οι οποίες πρέπει να ακολουθούν τις απαιτήσεις που περιγράφονται στο πρότυπο ETSI EN 319 412-1.

- PSD2 Qualified Certificate Statements: Εάν το Πιστοποιητικό χρησιμοποιείται σύμφωνα με τον κανονισμό (ΕΕ) No. 2018/389 και την οδηγία (ΕΕ) 2015/2366, αυτή η επέκταση περιέχει ειδικά χαρακτηριστικά / τιμές για τη μετάδοση πληροφοριών σε Βασιζόμενη Μέρη σχετικά με τους Παρόχους Υπηρεσιών Πληρωμών.
    - Ο ρόλος του παρόχου υπηρεσιών πληρωμών, ο οποίος πρέπει να είναι ένας ή περισσότερους από τους παρακάτω:
        - παροχή λογαριασμού (PSP_AS),
        - ένταξη πληρωμής (PSP_PI),
        - πληροφορίες λογαριασμού (PSP_AI),
        - έκδοση μέσων πληρωμών με κάρτα (PSP_IC).
    - Το όνομα της αρμόδιας αρχής στην οποία είναι εγγεγραμμένος ο πάροχος υπηρεσιών πληρωμών.
- CA/Browser Form Organization Identifier: Αν το πεδίο `subject:organizationIdentifier` βρίσκεται στο πιστοποιητικό, το πεδίο αυτό ΠΡΕΠΕΙ να βρίσκεται υποχρεωτικά σε ειδική επέκταση του CA/Browser Forum. Η συγκεκριμένη επέκταση πιστοποιητικού πρέπει να ακολουθεί τις απαιτήσεις των ενοτήτων 9.2.8 και 9.8.2 των EV Guidelines.

Στο ΠΑΡΑΡΤΗΜΑ Β (Περιγράμματα Κοινών Πιστοποιητικών HARICA) καταγράφεται λίστα με τα πιο συνήθη περιγράμματα πιστοποιητικών.

7.1.3 Αναγνωριστικά αλγορίθμων

Οι αλγόριθμοι υπογραφών πρέπει να ακολουθούν τις απαιτήσεις των παραγράφων 6.1.5 και 6.1.6. Όλοι οι αλγόριθμοι που χρησιμοποιούνται για Πιστοποιητικά ΑΠ, Συνδρομητή και ΜΧΣ, πρέπει να ακολουθούν τις τελευταίες εξελίξεις της τεχνολογίας προκειμένου να παρέχουν την απαιτούμενη ασφάλεια για τους σκοπούς που χρησιμοποιούνται.

7.1.3.1 SubjectPublicKeyInfo

Για Πιστοποιητικά ή Precertificates τύπου SSL/TLS, ισχύουν οι παρακάτω απαιτήσεις κωδικοποίησης σε σχέση με το πεδίο subjectPublicKeyInfo. Δεν επιτρέπονται άλλες κωδικοποιήσεις εκτός από αυτές που ρητά ορίζονται.

7.1.3.1.1 RSA

Η HARICA ΠΡΕΠΕΙ να σηματοδοτεί ένα κλειδί RSA χρησιμοποιώντας το rsaEncryption (OID: 1.2.840.113549.1.1.1) αναγνωριστικό αλγορίθμου. Το πεδίο parameters ΠΡΕΠΕΙ να υπάρχει και ΠΡΕΠΕΙ να είναι NULL. Η HARICA ΔΕΝ ΠΡΕΠΕΙ να χρησιμοποιήσει διαφορετικό αλγόριθμο, όπως το αναγνωριστικό αλγορίθμου id-RSASSA-PSS (OID: 1.2.840.113549.1.1.10) για να σηματοδοτήσει ένα κλειδί RSA.

Σε κωδικοποιημένη μορφή, το πεδίο `AlgorithmIdentifier` για κλειδιά RSA ΠΡΕΠΕΙ να είναι byte-for-byte πανομοιότυπο με τα ακόλουθα (κωδικοποιημένα σε δεκαεξαδικό) bytes: `300d06092a864886f70d0101010500`.

7.1.3.1.2 ECDSA

Η HARICA ΠΡΕΠΕΙ να σηματοδοτεί ένα κλειδί ECDSA χρησιμοποιώντας το id-ecPublicKey (OID: 1.2.840.10045.2.1) αναγνωριστικό αλγορίθμου. Το πεδίο parameters ΠΡΕΠΕΙ να χρησιμοποιεί την κωδικοποίηση `namedCurve`.

- Για κλειδιά P-256, η τιμή `namedCurve` ΠΡΕΠΕΙ να είναι `secp256r1` (OID: 1.2.840.10045.3.1.7).
- Για κλειδιά P-384, η τιμή `namedCurve` ΠΡΕΠΕΙ να είναι `secp384r1` (OID: 1.3.132.0.34).
- Για κλειδιά P-521, η τιμή `namedCurve` ΠΡΕΠΕΙ να είναι `secp521r1` (OID: 1.3.132.0.35).

Σε κωδικοποιημένη μορφή, το πεδίο AlgorithmIdentifier για κλειδιά ECDSA ΠΡΕΠΕΙ να είναι byte-for-byte πανομοιότυπο με τα ακόλουθα (κωδικοποιημένα σε δεκαεξαδικό) bytes:

- Για κλειδιά P-256, `301306072a8648ce3d020106082a8648ce3d030107`.
- Για κλειδιά P-384, `301006072a8648ce3d020106052b81040022`.
- Για κλειδιά P-521, `301006072a8648ce3d020106052b81040023`.

7.1.3.2 Signature AlgorithmIdentifier

Για Πιστοποιητικά τύπου SSL/TLS, όλα τα αντικείμενα που υπογράφονται από το Ιδιωτικό Κλειδί της ΑΠ ΠΡΕΠΕΙ να συμμορφώνονται στη χρήση του τύπου `AlgorithmIdentifier` ή `AlgorithmIdentifier`-παράγωγο για τις υπογραφές. Ειδικότερα, εφαρμόζονται στα παρακάτω αντικείμενα και πεδία:

- Το πεδίο signatureAlgorithm ενός Πιστοποιητικού ή Precertificate.
- Το πεδίο signature ενός TBSCertificate (για παράδειγμα, όπως χρησιμοποιείται σε Πιστοποιητικό ή Precertificate).
- Το πεδίο signatureAlgorithm ενός CertificateList
- Το πεδίο signature ενός TBSCertList
- Το πεδίο signatureAlgorithm ενός BasicOCSPResponse.

Δεν επιτρέπονται άλλες κωδικοποιήσεις εκτός από αυτές που ρητά ορίζονται.

7.1.3.2.1 RSA

Η HARICA ΠΡΕΠΕΙ να χρησιμοποιεί έναν από τους παρακάτω αλγορίθμους υπογραφών και κωδικοποιήσεις. Σε κωδικοποιημένη μορφή, το πεδίο `AlgorithmIdentifier` ΠΡΕΠΕΙ να είναι byte-for-byte πανομοιότυπο με τα ακόλουθα (κωδικοποιημένα σε δεκαεξαδικό) bytes.

- RSASSA-PKCS1-v1_5 με SHA-256:
  Κωδικοποίηση: `300d06092a864886f70d01010b0500`.
- RSASSA-PKCS1-v1_5 με SHA-384:
  Κωδικοποίηση: `300d06092a864886f70d01010c0500`.
- RSASSA-PKCS1-v1_5 με SHA-512:
  Κωδικοποίηση: 300d06092a864886f70d01010d0500.
- RSASSA-PSS με SHA-256, MGF-1 με SHA-256, και salt μήκους 32 bytes:
  Κωδικοποίηση:
  `304106092a864886f70d01010a3034a00f300d06096086480165030402010`
  0500a11c301a06092a864886f70d010108300d060960864801650304020 1
  0500a203020120

- RSASSA-PSS με SHA-384, MGF-1 με SHA-384, και salt μήκους 48 bytes:
  Κωδικοποίηση:
  304106092a864886f70d01010a3034a00f300d060960864801650304020 2
  `0500a11c301a06092a864886f70d010108300d060960864801650304020 2`
  0500a203020130
- RSASSA-PSS με SHA-512, MGF-1 με SHA-512, και salt μήκους 64 bytes:
  Κωδικοποίηση:
  304106092a864886f70d01010a3034a00f300d060960864801650304020 3
  `0500a11c301a06092a864886f70d010108300d060960864801650304020 3`
  0500a203020140

Επιπλέον, η HARICA ΔΥΝΑΤΑΙ να χρησιμοποιήσει τους παρακάτω αλγορίθμους υπογραφής και κωδικοποιήσεις,

- RSASSA-PKCS1-v1_5 with SHA-1:
- Encoding: `300d06092a864886f70d0101050500`

αν όλες οι παρακάτω προϋποθέσεις ισχύουν:

- Αν χρησιμοποιείται εντός Πιστοποιητικού, όπως το πεδίο `signatureAlgorithm` ενός Πιστοποιητικού ή το πεδίο `signature` ενός TBSCertificate:
  - Το νέο Πιστοποιητικό είναι ένα Κορυφαίο ή Ενδιάμεσο Πιστοποιητικό ΑΠ το οποίο είναι ένα Δια-Πιστοποιητικό, και,
  - Υπάρχει ένα υφιστάμενο Πιστοποιητικό, το οποίο έχει εκδωθεί από την ίδια Εκδούσα ΑΠ, χρησιμοποιώντας την ακόλουθη κωδικοποίηση για τον αλγόριθμο υπογραφής, και
  - Το υφιστάμενο Πιστοποιητικό έχει ένα `serialNumber` το οποίο έχει μήκος τουλάχιστον 64 bits, και
  - Οι μόνες διαφορές μεταξύ του νέου και του υφιστάμενου Πιστοποιητικού είναι από τις ακόλουθες:
    - Ένα νέο `subjectPublicKey` εντός του `subjectPublicKeyInfo`, χρησιμοποιώντας τον ίδιο αλγόριθμο και μήκος κλειδιού, ή/και,
    - Ένα νέο `serialNumber`, με το ίδιο μήκος (σε κωδικοποιημένη μορφή) όπως το υφιστάμενο Πιστοποιητικό, ή/και
    - Η επέκταση `extKeyUsage` του νέου Πιστοποιητικού είναι παρούσα, έχει τουλάχιστον ένα ορισμένο key usage, και κανένα από τα key usages δεν είναι id-kp-serverAuth (OID: 1.3.6.1.5.5.7.3.1) ή anyExtendedKeyUsage (OID: 2.5.2937.0), ή/και
    - Η επέκταση `basicConstraints` του νέου Πιστοποιητικού έχει pathLenConstraint το οποίο έχει τιμή μηδέν.
- Αν χρησιμοποιείται εντός OCSP response, όπως το πεδίο `signatureAlgorithm` ενός BasicOCSPResponse:
  - Όλα τα μη-ληγμένα, μη-ανακλημένα Πιστοποιητικά που περιλαμβάνουν το Δημόσιο Κλειδί του Ζεύγους Κλειδιών της ΑΠ και έχουν το ίδιο Subject Name, ΠΡΕΠΕΙ επίσης να περιλαμβάνουν την επέκταση extKeyUsage extension με μοναδική τιμή id-kp-ocspSigning (OID: 1.3.6.1.5.5.7.3.9) keyPurposeId.

- Αν χρησιμοποιείται εντός ΛΑΠ, όπως το πεδίο `signatureAlgorithm` ενός CertificateList ή στο πεδίο `signature` ενός TBSCertList:
    - Η ΛΑΠ είναι παραπομπή από ένα ή περισσότερα Πιστοποιητικά Κορυφαίας ή Ενδιάμεσης ΑΠ, και,
    - Το Πιστοποιητικό Κορυφαίας ή Ενδιάμεσης ΑΠ έχει εκδώσει ένα ή περισσότερα Πιστοποιητικά χρησιμοποιώντας τη συγκεκριμένη κωδικοποίηση για τον αλγόριθμο υπογραφής.

7.1.3.2.2 ECDSA

Η HARICA ΠΡΕΠΕΙ να χρησιμοποιεί έναν από τους παρακάτω αλγορίθμους υπογραφών και κωδικοποιήσεις βάσει του κλειδιού που χρησιμοποιεί για την υπογραφή.

- Αν το κλειδί που υπογράφει είναι `P-256`, η υπογραφή ΠΡΕΠΕΙ να είναι ECDSA με SHA-256. Σε κωδικοποιημένη μορφή, το πεδίο `AlgorithmIdentifier` ΠΡΕΠΕΙ να είναι byte-for-byte πανομοιότυπο με τα ακόλουθα (κωδικοποιημένα σε δεκαεξαδικό) bytes: `300a06082a8648ce3d040302`.
- Αν το κλειδί που υπογράφει είναι `P-384`, η υπογραφή ΠΡΕΠΕΙ να είναι ECDSA με SHA-384. Σε κωδικοποιημένη μορφή, το πεδίο `AlgorithmIdentifier` ΠΡΕΠΕΙ να είναι byte-for-byte πανομοιότυπο με τα ακόλουθα (κωδικοποιημένα σε δεκαεξαδικό) bytes: `300a06082a8648ce3d040303`.
- Αν το κλειδί που υπογράφει είναι `P-521`, η υπογραφή ΠΡΕΠΕΙ να είναι ECDSA με SHA-512. Σε κωδικοποιημένη μορφή, το πεδίο `AlgorithmIdentifier` ΠΡΕΠΕΙ να είναι byte-for-byte πανομοιότυπο με τα ακόλουθα (κωδικοποιημένα σε δεκαεξαδικό) bytes: `300a06082a8648ce3d040304`.

7.1.4 Μορφή πεδίων πιστοποιητικού

7.1.4.1 **Σειριακός Αριθμός**

Κάθε πιστοποιητικό έχει ενσωματωμένο σειριακό αριθμό που δημιουργείται αυτόματα από το σύστημα. Οι Εκδούσες ΑΠ παράγουν σειριακούς αριθμούς πιστοποιητικών που δεν είναι διαδοχικοί, είναι μεγαλύτεροι από το μηδέν (0) και περιέχουν τουλάχιστον εξήντα τέσσερα (64) δυαδικά ψηφία εντροπίας ενός CSPRNG.

7.1.4.2 **Αλγόριθμος Υπογραφής**

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

7.1.4.3 **Υπογραφή**

Η υπογραφή της ΑΠ που εκδίδει το πιστοποιητικό. Ο αλγόριθμος που χρησιμοποιείται για τη δημιουργία υπογραφής αναφέρεται εντός των εκδοθέντων πιστοποιητικών όπως περιγράφεται στην παράγραφο 7.1.3.

7.1.4.4 **Αρχή Έκδοσης**

Οι πληροφορίες που περιέχει το πεδίο «Αρχή Έκδοσης» περιλαμβάνουν τα ακόλουθα πεδία:

- commonName (OID: 2.5.4.3) (Απαραίτητο): Το «κοινό όνομα» της Αρχής Έκδοσης. Τα περιεχόμενα λειτουργούν ως αναγνωριστικό του Πιστοποιητικού της ΑΠ, έτσι ώστε το όνομα του Πιστοποιητικού της ΑΠ να είναι μοναδικό σε όλα τα πιστοποιητικά που θα εκδώσει η Εκδότρια ΑΠ.

- organizationalUnitName (OID: 2.5.4.11) (προαιρετικό αν υπάρχει CN): Η οργανωτική ομάδα ή υπο-ομάδα ή ειδική πληροφορία της Αρχής που υπογράφει ανάλογα με τους προβλεπόμενους σκοπούς, ή πληροφορίες του πιστοποιητικού. Η HARICA αποτρέπει το πεδίο αυτό να έχει τιμές από ονόματα, DBA, κατοχυρωμένα ονόματα, σήματα, διεύθυνση, περιοχή ή άλλο κείμενο που αναφέρεται σε συγκεκριμένο φυσικό ή νομικό πρόσωπο, εκτός αν η HARICA έχει επαληθεύσει τις πληροφορίες αυτές σύμφωνα με την ενότητα 3.2, και το πιστοποιητικό περιέχει ήδη τα πεδία subject:organizationName και subject:countryName, τα οποία έχουν επίσης επαληθευθεί σύμφωνα με την ενότητα 3.2.2.1.
- organizationIdentifier (OID: 2.5.4.97) (Απαραίτητο για ΑΠ που εκδίδουν Εγκεκριμένα Πιστοποιητικά): Σύμφωνα με τις πολιτικές QCP-l και QCP-l-qscd, περιλαμβάνει ένα μοναδικό αναγνωριστικό του Οργανισμού σύμφωνα με το ETSI EN 319 412-3. Ανάλογα με την επιλογή του Νομικού Προσώπου, θα πρέπει να χρησιμοποιηθεί μια από τις παρακάτω μορφές:
  - Ο αριθμός αναγνώρισης του Νομικού Προσώπου από ένα Εθνικό Μητρώο Επιχειρήσεων, με την ακόλουθη γραμμογράφηση: “**NTR**GR-123456789”. Στο παράδειγμα αυτό, το GR είναι η χώρα του υποκειμένου.
  - Ο Αριθμός Φορολογικού Μητρώου του Νομικού Προσώπου με την ακόλουθη γραμμογράφηση: “**VAT**GR-123456789”.
- organizationName (OID: 2.5.4.10) (Απαραίτητο): Περιέχει το όνομα του Νομικού Προσώπου ή το DBA της Υποκείμενης ΑΠ όπως έχει επαληθευθεί σύμφωνα με την ενότητα 3.2.2.2. Η HARICA μπορεί να περιλάβει πληροφορία στο πεδίο αυτό που να διαφέρει ελάχιστα από το όνομα που έχει επαληθευθεί, όπως είναι παραλλαγές ή συντμήσεις που η HARICA έχει καταγράψει τις διαφορές και είναι αποδεκτές οι συντμήσεις σε τοπικό επίπεδο. Π.χ. αν το επίσημο μητρώο αναφέρει “Company Name Incorporated”, η HARICA μπορεί να χρησιμοποιήσει το όνομα “Company Name Inc.” ή “Company Name”.
- localityName (OID: 2.5.4.7 (Προαιρετικά): Η πόλη, χωριό ή τοπική περιοχή, στην οποία ανήκει το Νομικό Πρόσωπο, όπως έχει επαληθευθεί σύμφωνα με την ενότητα 3.2.2.1.
- stateOrProvinceName (OID: 2.5.4.8) (Προαιρετικά): Η πολιτεία, νομός, περιφερειακή ενότητα, στην οποία ανήκει το Νομικό Πρόσωπο, όπως έχει επαληθευθεί σύμφωνα με την ενότητα 3.2.2.1.
- countryName (OID: 2.5.4.6) (Απαραίτητο): Η Χώρα στην οποία ανήκει το Νομικό Πρόσωπο, όπως έχει επαληθευθεί σύμφωνα με την ενότητα 3.2.2.1.

Τα περιεχόμενα του issuerDN της Εκδούσας ΑΠ ΠΡΕΠΕΙ να ταιριάζει με το subjectDN της ΑΠ Έκδοσης προκειμένου να υποστηρίζεται το “Name chaining” όπως περιγράφεται στο RFC 5280, στην ενότητα 4.1.2.4.

Για κάθε έγκυρη διαδρομή πιστοποίησης (όπως ορίζεται στην ενότητα 6 του RFC 5280):

- Για κάθε Πιστοποιητικό στη διαδρομή πιστοποίησης, το κωδικοποιημένο περιεχόμενο του πεδίου Issuer Distinguished Name του Πιστοποιητικού ΠΡΕΠΕΙ να είναι byte-for-byte πανομοιότυπο με την κωδικοποιημένη μορφή του πεδίου Subject Distinguished Name του Πιστοποιητικού της Εκδούσας ΑΠ.

- Για κάθε Πιστοποιητικό ΑΠ στη διαδρομή πιστοποίησης, το κωδικοποιημένο περιεχόμενο του πεδίου Subject Distinguished Name του Πιστοποιητικού ΠΡΕΠΕΙ να είναι byte-for-byte πανομοιότυπο με όλα τα Πιστοποιητικά, περιλαμβάνοντας ληγμένα και ανακλημένα, των οποίων τα Subject Distinguished Names μπορούν να συγκριθούν ως ίδια σύμφωνα με την ενότητα 7.1 του RFC 5280.

7.1.4.5 Έγκυρο Από

Η χρονική στιγμή (ημερομηνία/ώρα) που ξεκινά η περίοδος ισχύος του Πιστοποιητικού (μορφή: DD/MM/YYYY HH:MM A.M/P.M GMT)

7.1.4.6 Έγκυρο Έως

Η χρονική στιγμή (ημερομηνία/ώρα) που λήγει η περίοδος ισχύος του Πιστοποιητικού (μορφή: DD/MM/YYYY HH:MM A.M/P.M GMT)

7.1.4.7 Πληροφορίες στο πεδίο «Υποκείμενο» του Πιστοποιητικού

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». Περιλαμβάνει τα εξής:

- Email (E) (Δεν επιτρέπεται για πιστοποιητικά χρήσης SSL/TLS): Το email του υποκειμένου που επιβεβαιώνεται με τις διαδικασίες που περιγράφονται στην παράγραφο 3.2.3.
- commonName (OID: 2.5.4.3) (Προαιρετικό για πιστοποιητικά χρήσης SSL, Απαιτούμενο για Πιστοποιητικά Υπογραφής Κώδικα και Πιστοποιητικών χρηστών). Είναι το «κοινό όνομα» του Υποκειμένου. Αν υπάρχει το συγκεκριμένο πεδίο σε πιστοποιητικά που προορίζονται για χρήση SSL/TLS, πρέπει υποχρεωτικά να περιλαμβάνει ένα FQDN ή μία Διεύθυνση IP που είναι μία από τις τιμές που βρίσκονται στην επέκταση subjectAltName του Πιστοποιητικού. Για τα Πιστοποιητικά χρηστών, S/MIME ή Υπογραφής Κώδικα, αυτό το πεδίο πρέπει να περιέχει πληροφορίες που εκπροσωπούν το όνομα του Υποκειμένου που επιβεβαιώνεται με τις διαδικασίες που ορίζει η παράγραφος 3.2.2.1. Απαγορεύονται επίσης commonName τιμές οι οποίες ανήκουν στην περιοχή ονομάτων DNS για πιστοποιητικά που δεν είναι χρήσης SSL/TLS.
- givenName (OID: 2.5.4.42) και surname (OID: 2.5.4.4): Σύμφωνα με τις πολιτικές QCP-n και QCP-n-qscd, αντιπροσωπεύουν το όνομα και το επώνυμο του Υποκειμένου που επιβεβαιώνεται με τις διαδικασίες που ορίζει η παράγραφος 3.2.2.1. Εφαρμόζονται επιπλέον προδιαγραφές του προτύπου ETSI EN 319 412-2.
- streetAddress (OID: 2.5.4.9): Η φυσική διεύθυνση του Υποκειμένου που επιβεβαιώνεται με τις διαδικασίες που ορίζει η παράγραφος 3.2.2.1.
- postalCode (OID: 2.5.4.17): Η ταχυδρομική διεύθυνση του Υποκειμένου που επιβεβαιώνεται με τις διαδικασίες που ορίζει η παράγραφος 3.2.2.1.
- organizationalUnitName (OID: 2.5.4.11) (προαιρετικό): Η Μονάδα του Οργανισμού του Υποκειμένου ή αλλιώς υπο-μονάδα, ή ειδικό χαρακτηριστικό του υπογράφοντα ανάλογα με τους σκοπούς χρήσης ή τα χαρακτηριστικά του πιστοποιητικού. Η HARICA δεν επιτρέπει στο πεδίο OU να περιέχει στοιχεία όπως όνομα, Διακριτικό Τίτλο (DBA), εμπορικό όνομα, εμπορικό σήμα, διεύθυνση, τοποθεσία, ή άλλο κείμενο που

σχετίζεται με συγκεκριμένο Φυσικό ή Νομικό Πρόσωπο, εκτός αν η HARICA έχει επιβεβαιώσει την εγκυρότητα της πληροφορίας, όπως ορίζεται στην ενότητα 3.2 και το Πιστοποιητικό περιλαμβάνει επίσης τα πεδία subject:organizationName, subject:givenName, subject:surname, subject:localityName, και subject:countryName, τα οποία επίσης έχουν επιβεβαιωθεί σύμφωνα με τις διαδικασίες που περιγράφονται στην ενότητα 3.2.2.1.

- organizationName (OID: 2.5.4.10): Περιέχει το όνομα της οντότητας στο subject του πιστοποιητικού όπως έχει επαληθευτεί σύμφωνα με την ενότητα 3.2.2.1 ή το DBA της Υποκείμενης ΑΠ όπως έχει επαληθευθεί σύμφωνα με την ενότητα 3.2.2.2. Η HARICA μπορεί να περιλάβει πληροφορία στο πεδίο αυτό που να διαφέρει ελάχιστα από το όνομα που έχει επαληθευθεί, όπως είναι παραλλαγές ή συντμήσεις που η HARICA έχει καταγράψει τις διαφορές και είναι αποδεκτές οι συντμήσεις σε τοπικό επίπεδο. Π.χ. αν το επίσημο μητρώο αναφέρει “Company Name Incorporated”, η HARICA μπορεί να χρησιμοποιήσει το όνομα “Company Name Inc.” ή “Company Name”. Στα TLS OV/EV Πιστοποιητικά, είναι απαραίτητο στοιχείο ενώ για τα TLS IV Πιστοποιητικά είναι προαιρετικό αν τα στοιχεία του Φυσικού Προσώπου βρίσκονται στα πεδία surname και givenName, ενώ τα στοιχεία επιβεβαιώνονται με τις διαδικασίες που ορίζει η παράγραφος 3.2.3. Για τα Πιστοποιητικά EV, αυτό το χαρακτηριστικό πρέπει να επαληθεύεται σύμφωνα με την ενότητα 9.2.1 των Οδηγιών EV.
- localityName (OID: 2.5.4.7) Η πόλη, χωριό ή τοπική περιοχή, στην οποία βρίσκεται η οντότητα στο subject του πιστοποιητικού, όπως έχει επαληθευθεί σύμφωνα με την ενότητα 3.2.2.1. Είναι υποχρεωτικό πεδίο για TLS OV/EV Πιστοποιητικά αν το stateOrProvinceName λείπει, αλλιώς είναι προαιρετικό.
- stateOrProvinceName (OID: 2.5.4.8) (Προαιρετικά): Η πολιτεία, νομός, περιφερειακή ενότητα, στην οποία βρίσκεται η οντότητα στο subject του πιστοποιητικού, όπως έχει επαληθευθεί σύμφωνα με την ενότητα 3.2.2.1. Είναι υποχρεωτικό πεδίο για TLS OV/EV Πιστοποιητικά αν το localityName λείπει, αλλιώς είναι προαιρετικό.
- countryName (OID: 2.5.4.6): Η Χώρα του Υποκειμένου που επιβεβαιώνεται με τις διαδικασίες που ορίζει η παράγραφος 3.2.2.3.
- Subject Public Key Information: Περιέχει το Δημόσιο κλειδί και αναγνωρίζει τον αλγόριθμο δημιουργίας του και το μέγεθός του. Πιστοποιητικά που χρησιμοποιούνται για Υπογραφή Κώδικα πρέπει να συνδέονται σε αλυσίδα πιστοποιητικών με Αρχή Πιστοποίησης μεγέθους κλειδιού 4096-bit RSA ή αντίστοιχου ECC (P384).
- serialNumber (OID: 2.5.4.5) (Απαιτείται για Πιστοποιητικά EV, QCP-w) (Προαιρετικό για Πιστοποιητικά LCP, NCP, NCP+, QCP-n, QCP-n-qscd):
    - Για EV και QCP-w περιέχει τον Αριθμό Μητρώου του Νομικού Εκπροσώπου του Υποκειμένου.
        - Για Ιδιωτικές Επιχειρήσεις, αυτό το πεδίο ΠΡΕΠΕΙ να περιέχει τον Αριθμό Μητρώου (ή παρόμοιο) που έχει ανατεθεί στο Υποκείμενο από τον Φορέα Σύστασης ή Εγγραφής στην περιοχή Δικαιοδοσίας της Σύστασης ή Εγγραφής, ανάλογα με την περίπτωση. Εάν κατά τη διαδικασία της Σύστασης ή της Εγγραφής δεν αποδίδεται Αριθμός Μητρώου, τότε θα εισάγεται σε αυτό το πεδίο η

ημερομηνία της Σύστασης ή Εγγραφής σε οποιαδήποτε συνήθη μορφοποίηση ημερομηνίας.
- Για Κρατικούς Φορείς που δεν έχουν Αριθμό Μητρώου ή άμεσα επαληθεύσιμη ημερομηνία ίδρυσης, η HARICA εισάγει την τιμή «Κρατικός Φορέας».
- Για Επιχειρήσεις, εισάγεται σε αυτό το πεδίο ο Αριθμός Μητρώου που έλαβε η Επιχείρηση κατά τη διαδικασία εγγραφής που ορίζει το κράτος. Για τις Επιχειρήσεις που κατά τη διαδικασία της Σύστασης ή της Εγγραφής από τον αρμόδιο Φορέα δεν αποδίδεται Αριθμός Μητρώου σύμφωνα με τη διαδικασία εγγραφής που ορίζει το κράτος, τότε θα εισάγεται σε αυτό το πεδίο η ημερομηνία της εγγραφής σε οποιαδήποτε συνήθη μορφοποίηση ημερομηνίας.

  - Για QCP-n και QCP-n-qscd, περιέχει μοναδικό αναγνωριστικό που διακρίνει το Όνομα Υποκειμένου (Subject Name) στο πλαίσιο μίας Εκδούσας ΑΠ που συμμορφώνεται με το πρότυπο ETSI EN 319 412-2. Ανάλογα με την απόφαση του αιτούντα, χρησιμοποιείται κάποιο από τα παρακάτω αναγνωριστικά:
    - Αριθμός Μητρώου Κοινωνικής Ασφάλισης (ΑΜΚΑ) με την ακόλουθη κωδικοποίηση: “**PNO**GR-12345678”. Σε αυτό το παράδειγμα όπου GR είναι η κωδικοποίησης της Χώρας του Υποκειμένου.
    - Αριθμός ταυτότητας με την ακόλουθη κωδικοποίηση: “**IDC**GR-AK1234567”. Σε αυτό το παράδειγμα όπου GR είναι η κωδικοποίησης της Χώρας του Υποκειμένου.
    - Αριθμός Φορολογικού Μητρώου (ΑΦΜ) με την ακόλουθη κωδικοποίηση: “**TIN**GR-123456789”.
    - Αριθμός διαβατηρίου με την ακόλουθη κωδικοποίηση: “**PAS**GR-1231232”. Σε αυτό το παράδειγμα όπου GR είναι η κωδικοποίησης της Χώρας του Υποκειμένου.
    - Μοναδικό 10ψήφιο αναγνωριστικό που αποδίδεται από την HARICA
- businessCategory (OID: 2.5.4.15): Για τα Πιστοποιητικά EV, αυτό το χαρακτηριστικό πρέπει να περιέχει μία από τις ακόλουθες τιμές: "Private Organization", "Government Entity", "Business Entity" ή "Non-Commercial Entity" ανάλογα με το αν το Υποκείμενο πληροί τις προϋποθέσεις της ενότητας 8.5.2 , 8.5.3, 8.5.4 ή 8.5.5 των Οδηγιών EV, αντίστοιχα.
- *jurisdictionCountryName* (OID: 1.3.6.1.4.1.311.60.2.1.3), *jurisdictionStateOrProvinceName* (OID: 1.3.6.1.4.1.311.60.2.1.2), *jurisdictionLocalityName* (OID: 1.3.6.1.4.1.311.60.2.1.1): Για τα Πιστοποιητικά EV, αυτό είναι το πεδίο της Περιοχής Δικαιοδοσίας Σύστασης ή Εγγραφής του Υποκειμένου σύμφωνα με την ενότητα 9.2.5 των Οδηγιών EV
- OrganizationIdentifier (OID: 2.5.4.97): Σύμφωνα με τα πρότυπα QCP-l και QCP-l-qscd, περιέχει μοναδικό αναγνωριστικό που αφορά στον Οργανισμό σε συμμόρφωση με το ETSI EN 319 412-3. Ανάλογα με την απόφαση του

Νομικού Εκπροσώπου πρέπει να χρησιμοποιηθεί ένα από τα παρακάτω αναγνωριστικά:

- Αριθμός Μητρώου Νομικής Οντότητας που προκύπτει από εθνικό μητρώο εμπορικών επιχειρήσεων με την ακόλουθη κωδικοποίηση: "**NTR**GR-123456789". Σε αυτό το παράδειγμα όπου GR είναι η κωδικοποίησης της Χώρας του Υποκειμένου.
- Αριθμός Μητρώου Νομικής Οντότητας με την ακόλουθη κωδικοποίηση:"**VAT**GR-123456789".

Για τα Πιστοποιητικά PSD2, η έννοια ορίζεται στην παράγραφο 5.1.4 του προτύπου ETSI TS 119 412-1, η οποία χρησιμοποιεί το σχήμα "**PSD**" για ταυτοποίηση βάσει του εθνικού αριθμού αδείας ενός παρόχου υπηρεσιών πληρωμών σύμφωνα με την Οδηγία για Υπηρεσία Πληρωμών (ΕΕ) 2015/2366. Αυτό χρησιμοποιεί την εκτεταμένη δομή όπως ορίζεται στο πρότυπο ETSI TS 119 495, στην παράγραφο 5.2.1.

- Με εξαίρεση τα EV Πιστοποιητικά, άλλα πεδία μπορεί να βρίσκονται εντός του subjectDN. Αν βρίσκονται άλλα πεδία που δεν περιγράφονται παραπάνω, θα ΠΡΕΠΕΙ να περιλαμβάνουν πληροφορίες που έχουν επαληθευθεί/επιβεβαιωθεί από την HARICA.

Έκδοση Πιστοποιητικού χρήσης SSL/TLS σημαίνει ότι η ΥΔΚ της HARICA ακολούθησε όλες τις διαδικασίες που υπαγορεύονται σε αυτό το κείμενο ΠΠ/ΔΔΠ για να επαληθεύσει ότι, κατά την ημερομηνία έκδοσης του Πιστοποιητικού, όλες οι πληροφορίες του Υποκειμένου ήταν ακριβείς. Η HARICA δεν εντάσσει Όνομα Χώρου ή Διεύθυνση IP στο πεδίο Subject εκτός από ό,τι ορίζεται στην παράγραφο 3.2.2.4 ή στην παράγραφο 3.2.2.5. Για Πιστοποιητικά SSL/TLS, τα πεδία του subjectDN ΔΕΝ ΠΡΕΠΕΙ να περιέχουν δεδομένα όπως '.', '-', και ' ' (δηλαδή το απλό κενό) καθώς και οποιαδήποτε άλλη σήμανση ότι η τιμή είναι απούσα, ελλιπής ή μη εφαρμόσιμη.

Έκδοση Πιστοποιητικού Χρήστη/Υπογραφής Κώδικα σημαίνει ότι η ΥΔΚ της HARICA ακολούθησε όλες τις διαδικασίες που υπαγορεύονται σε αυτό το κείμενο ΠΠ/ΔΔΠ για να επαληθεύσει ότι, κατά την ημερομηνία έκδοσης του Πιστοποιητικού, όλες οι πληροφορίες του Υποκειμένου ήταν ακριβείς. Η HARICA δεν εντάσσει τα commonName, emailAddress στο πεδίο Subject εκτός από ό,τι ορίζεται στην παράγραφο 3.2.3. Επειδή τα χαρακτηριστικά του ονόματος του Υποκειμένου όσον αφορά τα φυσικά πρόσωπα (π.χ. givenName (OID:2.5.4.42) και surname (OID: 2.5.4.4)) δεν υποστηρίζονται ευρέως από λογισμικά εφαρμογών, η HARICA μπορεί να χρησιμοποιεί το πεδίο subject:organizationName για να εκφράσει το όνομα του φυσικού προσώπου του πιστοποιητικού ή Διακριτικό Τίτλο (DBA).

Με την έκδοση Εγκεκριμένου Πιστοποιητικού για Προηγμένες ηλεκτρονικές υπογραφές σύμφωνα με την πολιτική QCP-n ή Εγκεκριμένου Πιστοποιητικού για Εγκεκριμένες ηλεκτρονικές υπογραφές σύμφωνα με την πολιτική QCP-n-qscd, η ΥΔΚ της HARICA εμπεριέχει τουλάχιστον τα χαρακτηριστικά "commonName", "Country", "givenName" and "surname" στο πεδίο SubjectDN. Αν αυτά τα χαρακτηριστικά δεν είναι επαρκή για να εξασφαλίσουν τη μοναδικότητα του ονόματος του Υποκειμένου (Subject) στο πλαίσιο που ακολουθεί η Εκδούσα ΑΠ, τότε θα υπάρχει το serialNumber του πιστοποιητικού.

Με την έκδοση Εγκεκριμένου Πιστοποιητικού για Προηγμένες ηλεκτρονικές σφραγίδες σύμφωνα με την πολιτική QCP-l-qscd ή Εγκεκριμένου Πιστοποιητικού για

Εγκεκριμένες ηλεκτρονικές σφραγίδες σύμφωνα με την πολιτική QCP-l-qscd, η ΥΔΚ της HARICA εμπεριέχει τουλάχιστον τα χαρακτηριστικά "commonName", "Country", "organizationName" and "OrganizationIdentifier" στο πεδίο SubjectDN.

7.1.4.8 Επέκταση Subject Alternative Name

Η συγκεκριμένη επέκταση απαιτείται σε Πιστοποιητικά SSL και S/MIME ενώ είναι προαιρετική για Πιστοποιητικά Υπογραφής Κώδικα.

Περιεχόμενα στα Πιστοποιητικά SSL/TLS: Η επέκταση πρέπει να περιέχει τουλάχιστον μία καταχώρηση. Κάθε καταχώρηση πρέπει να είναι του τύπου dNSName που περιέχει τον Πλήρη Πιστοποιημένο Χώρο Ονομάτων (Fully-Qualified Domain). Η HARICA πρέπει να επιβεβαιώνει ότι ο Αιτών έχει τον πλήρη έλεγχο του FQDN ή έχει την εξουσιοδότηση από τον Καταχωρίζοντα του Ονόματος Χώρου να το χρησιμοποιεί σύμφωνα με όσα ορίζονται στην παράγραφο 3.2.2.4. Για μια Διεύθυνση IP, η HARICA πρέπει να επιβεβαιώσει ότι ο Αιτών έχει τον πλήρη έλεγχο αυτής της Διεύθυνσης IP ή έχει την εξουσιοδότηση να την χρησιμοποιήσει σύμφωνα με όσα ορίζονται στην ενότητα 3.2.2.5. Τα Ονόματα Χώρου Μπαλαντέρ επιτρέπονται. Πιστοποιητικά που περιέχουν χαρακτήρες underscore ("_") στα πεδία ονομάτων στις καταχωρήσεις dNSName ΠΡΕΠΕΙ ΝΑ ΜΗΝ είναι παρόντα. Πιστοποιητικά Μπαλαντέρ δεν επιτρέπονται Πιστοποιητικά EV SSL / TLS εκτός από τις περιπτώσεις που ορίζονται στο Παράρτημα Στ΄ των Οδηγιών EV. Ονόματα Χώρου Μπαλαντέρ επιτρέπονται για Πιστοποιητικά SSL / TLS DV και OV, λαμβάνοντας υπόψη τις διατάξεις της ενότητας 3.2.2.6

Περιεχόμενα σε Πιστοποιητικά Υπογραφής Κώδικα: Αν υπάρχει αυτό το πεδίο, περιέχει το dNSName, το iPAddress ή άλλες καταχωρήσεις που δείχνουν σε ένα Όνομα Χώρου ή σε μια Διεύθυνση IP.

Περιεχόμενα σε Πιστοποιητικά S/MIME: Αυτή η επέκταση πρέπει να περιέχει τουλάχιστον μία καταχώρηση. Κάθε καταχώρηση πρέπει να είναι ένα rfc822Name που περιλαμβάνει μία διεύθυνση email του Συνδρομητή. Δεν πρέπει να περιέχει Όνομα Χώρου ή Διεύθυνση IP. Η HARICA επιβεβαιώνει ότι ο Αιτών έχει τον πλήρη έλεγχο της διεύθυνσης email όπως ορίζεται στην παράγραφο 3.2.3.1.

7.1.5 Επέκταση name constraints

Η HARICA χρησιμοποιεί την επέκταση name constraints προκειμένου να περιορίσει το εύρος Ενδιάμεσων ΑΠ σύμφωνα με το RFC 5280. Η συγκεκριμένη επέκταση χαρακτηρίζεται ως « μη κρίσιμη».

Κάθε Πιστοποιητικό Ενδιάμεσης ΑΠ Ιδρύματος, πρέπει να περιορίζεται σε μία ή περισσότερες περιοχές ονομάτων χώρου (Domain Namespace) που ανήκουν στο Ίδρυμα. Για παράδειγμα, το Πιστοποιητικό της Ενδιάμεσης ΑΠ το Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης περιορίζεται στην περιοχή χώρου ονομάτων "auth.gr", με τη χρήση της επέκτασης name constraints.

Αν το πιστοποιητικό Ενδιάμεσης ΑΠ περιέχει την επέκταση χρήσης κλειδιού id-kp-serverAuth και η αντίστοιχη Ενδιάμεση ΑΠ θεωρείται τεχνικά περιορισμένη και ότι ελέγχεται όπως περιγράφεται στην παράγραφο 8.7, τότε το Πιστοποιητικό της Ενδιάμεσης ΑΠ πρέπει να περιέχει την επέκταση Name Constraints X.509v3 με τους περιορισμούς που ακολουθούν στις τιμές dNSName, iPAddress και DirectoryName:

a) Για κάθε dNSName στο permittedSubtrees, η HARICA πρέπει να επιβεβαιώνει ότι ο Αιτών είναι αυτός που έχει καταχωρήσει το dNSName σε κάποιον καταχωρητή ή ότι ο Αιτών έχει εξουσιοδοτηθεί από τον καταχωρίζοντα να

ενεργεί εκ μέρους του σύμφωνα με τις πρακτικές επαλήθευσης της παραγράφου 3.2.2.4.

b) Για κάθε εύρος iPAddress στο permittedSubtrees, η HARICA πρέπει να επιβεβαιώνει ότι έχει ανατεθεί στον Αιτούντα αυτό το εύρος iPAddress ή ότι ο Αιτών έχει εξουσιοδοτηθεί από αυτόν στον οποίο ανατέθηκε το εύρος iPAddress να ενεργεί εκ μέρους του.
c) Για κάθε DirectoryName στο permittedSubtrees, η HARICA πρέπει να επιβεβαιώνει τους Αιτούντες και/η το όνομα και την τοποθεσία της Θυγατρικής Εταιρείας έτσι ώστε τα πιστοποιητικά τελικών χρηστών/συσκευών που εκδόθηκαν από την Ενδιάμεση ΑΠ να είναι σε συμμόρφωση με την παράγραφο 7.1.2.

Αν το πιστοποιητικό της Ενδιάμεσης ΑΠ περιέχει την επέκταση χρήσης id-kp-serverAuth και η αντίστοιχη Ενδιάμεση ΑΠ θεωρείται τεχνικά περιορισμένη και ότι ελέγχεται όπως περιγράφεται στην παράγραφο 8.7, και δεν επιτρέπεται να εκδίδει πιστοποιητικά με τιμή iPAddress τότε το Πιστοποιητικό της Ενδιάμεσης ΑΠ πρέπει να ορίσει όλο το εύρος των διευθύνσεων IPv4 και IPv6 μέσα στο excludedSubtrees. Το Πιστοποιητικό της Ενδιάμεσης ΑΠ πρέπει να περιέχει μέσα στο πεδίο excludedSubtrees μία τιμή iPAddress GeneralName με 8 μηδενικές οκτάδες (καλύπτοντας όλο το εύρος 0.0.0.0/0 των διευθύνσεων IPv4). Το Πιστοποιητικό της Ενδιάμεσης ΑΠ πρέπει να περιλαμβάνει επίσης, μέσα στο πεδίο excludedSubtrees μία τιμή iPAddress GeneralName με 32 μηδενικές octets (καλύπτοντας όλο το εύρος ::0/0 των διευθύνσεων IPv6). Διαφορετικά, το Πιστοποιητικό της Ενδιάμεσης ΑΠ πρέπει να περιλαμβάνει τουλάχιστον μία τιμή iPAddress μέσα στο permittedSubtrees.

Αν το Πιστοποιητικό της Ενδιάμεσης ΑΠ περιλαμβάνει άλλη επέκταση χρήσης από την “id-kp-serverAuth” θεωρείται τεχνικά περιορισμένο και ότι ελέγχεται όπως περιγράφεται στην παράγραφο 8.7.

Επιπλέον, η Κεντρική Αρχή Πιστοποίησης της HARICA 2011 περιορίζεται στα domains: .gr, .eu, .edu, .org.

7.1.6 Αναγνωριστικό πολιτικής πιστοποίησης

Το αναγνωριστικό (OID) της παρούσας πολιτικής πιστοποίησης αναφέρεται στην ενότητα 1.2. Ανάλογα με το είδος κάθε πιστοποιητικού, τα παρακάτω αναγνωρισμένα OIDs μπορούν να προστεθούν στην επέκταση *certificatePolicies*:

- **BTSP** (Best practice policy for time-stamp)
  - **0.4.0.2023.1.1** όπως περιγράφεται στο ETSI EN 319 421
  - 1.3.6.1.4.1.26513.1.1.6.1
- **QTST** (Qualified time-stamping Certificate)
  - **0.4.0.2023.1.1** όπως περιγράφεται στο ETSI EN 319 421
  - 1.3.6.1.4.1.26513.1.1.6.2
- **QCP-n** (Advanced Electronic Signature)
  - **0.4.0.194112.1.0** όπως περιγράφεται στο ETSI EN 319 411-2
  - 1.3.6.1.4.1.26513.1.1.4.1
- **QCP-l** (Advanced Electronic Seal)
  - **0.4.0.194112.1.1** όπως περιγράφεται στο ETSI EN 319 411-2
  - 1.3.6.1.4.1.26513.1.1.4.3
- **QCP-l-psd2** (Advanced Electronic Seal for PSD2)
  - **0.4.0.194112.1.1** as described in ETSI EN 319 411-2

    - 1.3.6.1.4.1.26513.1.1.4.5
- **QCP-l-psd2-qscd** (Qualified Electronic Seal for PSD2)
    - **0.4.0.194112.1.3** as described in ETSI EN 319 411-2
    - 1.3.6.1.4.1.26513.1.1.4.6
- **QCP-n-qscd** (Qualified Electronic Signature)
    - **0.4.0.194112.1.2** όπως περιγράφεται στο ETSI EN 319 411-2
    - 1.3.6.1.4.1.26513.1.1.4.2
- **QCP-l-qscd** (Qualified Electronic Seal)
    - **0.4.0.194112.1.3** όπως περιγράφεται στο ETSI EN 319 411-2
    - 1.3.6.1.4.1.26513.1.1.4.4
- **QCP-w** (Qualified Website Authentication Certificate)
    - **0.4.0.194112.1.4** όπως περιγράφεται στο ETSI EN 319 411-2
    - 1.3.6.1.4.1.26513.1.1.1.5
- **QCP-w-psd2** (Qualified Website Authentication Certificate for PSD2)
    - **0.4.0.19495.3.1** όπως περιγράφεται στο ETSI TS 119 495
    - 1.3.6.1.4.1.26513.1.1.1.6
- **NCP** (Normalized Certificate Policy)
    - **0.4.0.2042.1.1** όπως περιγράφεται στο ETSI EN 319 411-1
    - 1.3.6.1.4.1.26513.1.1.2.2.1
    - 1.3.6.1.4.1.26513.1.1.2.3.1
    - 1.3.6.1.4.1.26513.1.1.3.1.1
    - 1.3.6.1.4.1.26513.1.1.3.2.1
    - 1.3.6.1.4.1.26513.1.1.5.1.1
    - 1.3.6.1.4.1.26513.1.1.5.2.1
- **NCP+** (Extended Normalized Certificate Policy)
    - **0.4.0.2042.1.2** όπως περιγράφεται στο ETSI EN 319 411-1
    - 1.3.6.1.4.1.26513.1.1.2.2.2
    - 1.3.6.1.4.1.26513.1.1.2.3.2
    - 1.3.6.1.4.1.26513.1.1.3.1.2
    - 1.3.6.1.4.1.26513.1.1.3.2.2
    - 1.3.6.1.4.1.26513.1.1.5.1.2
    - 1.3.6.1.4.1.26513.1.1.5.2.2
- **LCP** (Lightweight Certificate Policy)
    - **0.4.0.2042.1.3** όπως περιγράφεται στο ETSI EN 319 411-1
    - 1.3.6.1.4.1.26513.1.1.2.1
    - 1.3.6.1.4.1.26513.1.1.2.2.3
    - 1.3.6.1.4.1.26513.1.1.2.3.3
    - 1.3.6.1.4.1.26513.1.1.5.1.3
    - 1.3.6.1.4.1.26513.1.1.5.2.3
- **DVCP** (Domain Validated Certificate Policy)
    - **0.4.0.2042.1.6** όπως περιγράφεται στο ETSI EN 319 411-1
    - **2.23.140.1.2.1** όπως περιγράφεται στο CA/B Forum Baseline Requirements
    - 1.3.6.1.4.1.26513.1.1.1.1
- **OVCP** (Organizational Validation Certificate Policy)
    - **0.4.0.2042.1.7** όπως περιγράφεται στο ETSI EN 319 411-1
    - **2.23.140.1.2.2** όπως περιγράφεται στο CA/B Forum Baseline Requirements
    - 1.3.6.1.4.1.26513.1.1.1.2
- **IVCP** (Individual Validation Certificate Policy)
    - **0.4.0.2042.1.8** όπως περιγράφεται στο ETSI EN 319 411-1

    - **2.23.140.1.2.3** όπως περιγράφεται στο CA/B Forum Baseline Requirements
    - 1.3.6.1.4.1.26513.1.1.1.3
- **EVCP** (Extended Validation Certificate Policy)
    - **0.4.0.2042.1.4** όπως περιγράφεται στο ETSI EN 319 411-1
    - **2.23.140.1.1** όπως περιγράφεται στο CA/B Forum EV Guidelines
    - 1.3.6.1.4.1.26513.1.1.1.4
- **Όχι-EV Code Signing**
    - **2.23.140.1.4.1** όπως περιγράφεται στο CA/B Forum Baseline Requirements for Code Signing για Όχι-EV Code Signing Πιστοποιητικά
    - 1.3.6.1.4.1.26513.1.1.3.1.1
    - 1.3.6.1.4.1.26513.1.1.3.1.2
    - 1.3.6.1.4.1.26513.1.1.3.2.1
    - 1.3.6.1.4.1.26513.1.1.3.2.2
- **EV** (Extended Validation) **for Code Signing**
    - **2.23.140.1.3** όπως περιγράφεται στο CA/B Forum EV Guidelines for Code Signing.
    - 1.3.6.1.4.1.26513.1.1.3.3
- **OCSP Certificate**
    - 1.3.6.1.4.1.26513.1.1.7
- **Εξ αποστάσεως ΕΔΔΥ (Remote QSCD)**
    - 1.3.6.1.4.1.26513.1.1.8

Η πλήρης λίστα με τα αναγνωριστικά (OIDs) Πολιτικών είναι διαθέσιμη στο ΠΑΡΑΡΤΗΜΑ ΣΤ ΑΝΑΓΝΩΡΙΣΤΙΚΑ ΠΟΛΙΤΙΚΩΝ HARICA.

Οι Ενδιάμεσες ΑΠ Εσωτερικής Διαχείρισης μπορούν να χρησιμοποιούν το δεσμευμένο αναγνωριστικό “AnyPolicy” με OID: **2.5.29.32.0.** Στην περίπτωση Υφιστάμενων ΑΠ Εξωτερικής Διαχείρισης, πρέπει να χρησιμοποιείται το αντίστοιχο OID της ΠΠ/ΔΔΠ μέσα στην επέκταση Certificate Policy του Πιστοποιητικού Ενδιάμεσης ΑΠ.

Εάν η Ενδιάμεση ΑΠ είναι ενεργοποιημένη για να εκδίδει Εγκεκριμένα Πιστοποιητικά και δεν περιλαμβάνει το πεδίο `subject:organizationIdentifier`, τότε η επέκταση certificatePolicies θα πρέπει να περιλαμβάνει ένα userNotice με τιμή: “*This Qualified Certificate has been Issued by the QTSP "Greek Universities Network (GUnet)" with VAT number EL099028220*”.

Τα τελικά Πιστοποιητικά Συνδρομητών χρήσης SSL/TLS ΠΡΕΠΕΙ να περιλαμβάνουν ένα από τα ειδικά OID πολιτικής του CA/Browser Forum στην επέκταση `certificatePolicies`.

7.1.7 Χρήση της επέκτασης Περιορισμοί πολιτικής (Policy Constraints)

Δεν ορίζεται.

7.1.8 Σύνταξη και σημασιολογία του χαρακτηριστικού πολιτικής

Σε περίπτωση που χρησιμοποιείται το policy qualifier `cPSuri` [RFC 5280], θα περιέχει ένα URI προς τη δημοσιευμένη ΠΠ/ΔΔΠ της HARICA.

Σε περίπτωση που χρησιμοποιείται το policy qualifier `userNotice` [RFC 5280], θα περιέχει κείμενο που θα περιγράφει ειδικές πληροφορίες πολιτικής ή πληροφορία που σχετίζεται με τον Πάροχο Υπηρεσιών Εμπιστοσύνης.

Για Εγκεκριμένα Πιστοποιητικά, το παρακάτω κείμενο δύναται να χρησιμοποιηθεί για να δώσει την πληροφορία ότι η HARICA λειτουργεί ως Πάροχος Υπηρεσιών Εμπιστοσύνης που εκδίδει Εγκεκριμένα Πιστοποιητικά:
“This Qualified Certificate has been Issued by the QTSP "Greek Universities Network (GUnet)" with VAT number EL099028220”.

7.1.9 Επεξεργασία σημασιολογίας για την κρίσιμη επέκταση Πολιτικές Πιστοποίησης (Certificate Policies)

Δεν ορίζεται.

7.2 Περίγραμμα ΛΑΠ

7.2.1 Αριθμός έκδοσης

Ο αριθμός έκδοσης της είναι 2 (η ακέραια τιμή είναι 1), που αντιστοιχεί σε ΛΑΠ X.509v2, σύμφωνα με το RFC 5280.

7.2.2 ΛΑΠ και επεκτάσεις εγγραφών ΛΑΠ

7.2.2.1 Υπογραφή

Οι αλγόριθμοι υπογραφής πρέπει να ακολουθούν τις απαιτήσεις που περιγράφονται στις ενότητες 6.1.5 και 6.1.6.

7.2.2.2 Αλγόριθμος Κατακερματισμού

Επιτρέπονται μόνο αλγόριθμοι κατακερματισμού της οικογένειας SHA2 ή ισχυρότεροι.

7.2.2.3 Όνομα Εκδότη

Το Διακεκριμένο Όνομα της Αρχής Πιστοποίησης που έχει υπογράψει και έχει εκδώσει τη ΛΑΠ.

7.2.2.4 Ημερομηνία Ενημέρωσης

Η ημερομηνία έκδοσης της ΛΑΠ σε UTCTime.

7.2.2.5 Επόμενη Ενημέρωση

Η μέγιστη χρονικά ημερομηνία έκδοσης της επόμενης ΛΑΠ σε UTCTime. Εφαρμόζονται οι απαιτήσεις της ενότητας 4.9.7.

Αν μια Ενδιάμεση ΑΠ:

1. έχει εκδώσει Πιστοποιητικά τα οποία είτε έληξαν είτε ανακλήθηκαν και
2. αυτή η Ενδιάμεση ΑΠ σταματά να εκδίδει νέα Πιστοποιητικά

τότε η ίδια Ενδιάμεση ΑΠ μπορεί να εκδώσει μια τελευταία ΛΑΠ και μπορεί να ρυθμίσει το πεδίο nextUpdate στην ΛΑΠ σε "99991231235959Z" όπως ορίζεται στο RFC 5280. Η τιμή αυτή, που ορίζεται στο RFC 5280 για πιστοποιητικά που δεν έχουν καλά ορισμένη την ημερομηνία λήξης, χρησιμοποιείται εδώ για την περίπτωση της

τελευταίας ΛΑΠ. Η Εκδούσα ΑΠ που δημιουργεί την τελευταία ΛΑΠ ΔΕΝ πρέπει να εκδίδει κανένα νέο Πιστοποιητικό στο εξής.

7.2.2.6 Πιστοποιητικά που ανακλήθηκαν

Λίστα με όλα τα πιστοποιητικά που έχουν ανακληθεί όπου συμπεριλαμβάνονται οι σειριακοί αριθμοί και η ημερομηνία και η ώρα της ανάκλησης κάθε πιστοποιητικού σε UTCTime.

7.2.2.7 Αριθμός ΛΑΠ (OID 2.5.29.20)

Η επέκταση αυτή ΠΡΕΠΕΙ να περιλαμβάνεται και ΔΕΝ ΠΡΕΠΕΙ να χαρακτηρίζεται κρίσιμη. Περιλαμβάνει ένα αυξανόμενο μοναδικό αριθμό που καθορίζει κάθε ΛΑΠ σύμφωνα με την ενότητα 5.2.3 του RFC 5280.

7.2.2.8 Authority Key Identifier

Η επέκταση αυτή ΠΡΕΠΕΙ να περιλαμβάνεται και ΔΕΝ ΠΡΕΠΕΙ να χαρακτηρίζεται κρίσιμη. Περιλαμβάνει το authority key identifier της Εκδούσας ΑΠ σύμφωνα με την ενότητα 5.2.1 του RFC 5280.

7.2.2.9 Ληγμένα Πιστοποιητικά στη ΛΑΠ (OID: 2.5.29.60)

Η επέκταση αυτή ΔΥΝΑΤΑΙ να περιλαμβάνεται και ΔΕΝ ΠΡΕΠΕΙ να χαρακτηρίζεται κρίσιμη. Παρέχει ένδειξη ότι η ΛΑΠ περιλαμβάνει σημειώσεις ανάκλησης ληγμένων πιστοποιητικών σύμφωνα με την ενότητα 9.5.2.8 του ITU-T X.509.

7.2.2.10 **Κωδικός Αιτιολογίας (OID 2.5.29.21)**

Αν περιλαμβάνεται, αυτή η επέκταση εγγραφής ΛΑΠ ΔΕΝ ΠΡΕΠΕΙ να χαρακτηρίζεται κρίσιμη.

Από 2020-09-30 και μόνο για ΑΠ με τεχνική δυνατότητα έκδοσης Πιστοποιητικών SSL/TLS, αν η εγγραφή ΛΑΠ αφορά Πιστοποιητικό Κορυφαίας ή Ενδιάμεσης ΑΠ, συμπεριλαμβανομένων Δια-Πιστοποιητικών, η συγκεκριμένη επέκταση εγγραφής ΛΑΠ ΠΡΕΠΕΙ να περιλαμβάνεται.

Από 2020-09-30, αν η εγγραφή ΛΑΠ αφορά Πιστοποιητικό που δεν έχει τεχνικά δυνατότητα για έκδοση, η συγκεκριμένη επέκταση εγγραφής ΛΑΠ ΜΠΟΡΕΙ να περιλαμβάνεται, αλλά ΔΥΝΑΤΑΙ να παραληφθεί, εφόσον ισχύουν οι ακόλουθες προϋποθέσεις:

- Η ένδειξη `CRLReason` ΔΕΝ ΠΡΕΠΕΙ να είναι unspecified (0). Αν ο ένδειξη ανάκληση είναι unspecified, η εκδούσα ΑΠ ΠΡΕΠΕΙ να παραλείψει την επέκταση εγγραφής `reasonCode`, αν και επιτρέπεται από τις προηγούμενες απαιτήσεις. Αν μια εγγραφή ΛΑΠ αφορά Πιστοποιητικό SSL/TLS, το `CRLReason` ΔΕΝ ΠΡΕΠΕΙ να είναι certificateHold (6). Περισσότερες πληροφορίες βρίσκονται στην ενότητα 4.9.15.
- Αν η επέκταση εγγραφής ΛΑΠ `reasonCode` είναι παρούσα, το `CRLReason` ΠΡΕΠΕΙ να αντιστοιχεί στον πιο κατάλληλο λόγο ανάκλησης του πιστοποιητικού σύμφωνα με την ενότητα 9.5.3.1 του ITU-T X.509 recommendation και του RFC 5280.

7.2.3 ΛΑΠ και επεκτάσεις των εγγραφών της ΛΑΠ

Δεν ορίζεται.

7.3 Περίγραμμα OCSP

Το Online Πρωτόκολλο Κατάστασης Πιστοποιητικών (OCSP) χρησιμοποιείται για την επαλήθευση της κατάστασης ανάκλησης όλων των πιστοποιητικών που έχουν εκδοθεί από την Κορυφαία Κεντρική Αρχή Πιστοποίησης. Η χρήση του OCSP είναι υποχρεωτική για τις υφιστάμενες Αρχές Πιστοποίησης.

Οι εξυπηρετητές OCSP πρέπει να συμμορφώνονται με το RFC 6960.

Από 2020-09-30, αν ένα OCSP response είναι για Πιστοποιητικό Κορυφαίας ή Ενδιάμεσης ΑΠ, συμπεριλαμβανομένων των Δια-Πιστοποιητικών, και το Πιστοποιητικό αυτό έχει ανακληθεί, τότε το πεδίο `revocationReason` εντός του `RevokedInfo` του `CertStatus` ΠΡΕΠΕΙ να περιλαμβάνεται.

Από 2020-09-30, το `CRLReason` που αναφέρεται ΠΡΕΠΕΙ να περιλαμβάνει μια τιμή που επιτρέπεται για ΛΑΠ, σύμφωνα με την ενότητα 7.2.2.

7.3.1 Αριθμός έκδοσης

Υποστηρίζεται η έκδοση 1 των προδιαγραφών OCSP όπως αυτή ορίζεται στο RFC 6960.

7.3.2 OCSP και επεκτάσεις των εγγραφών

Η υπηρεσία OCSP χρησιμοποιεί ασφαλή χρονοσφραγίδα και μέγιστη περίοδο εγκυρότητας όπως ορίζεται στην παράγραφο 4.9.10 για να επιβεβαιώσει την εγκυρότητα της υπογεγραμμένης απάντησης. Οι επόμενες ενημερώσεις θα είναι διαθέσιμες τουλάχιστον μία μέρα πριν η τρέχουσα περίοδος λήξει. Ο αλγόριθμος υπογραφής που χρησιμοποιείται για την απάντηση του OCSP είναι ο SHA2.

Το `singleExtensions` ενός OCSP response ΔΕΝ ΠΡΕΠΕΙ να περιλαμβάνει το `reasonCode` (OID 2.5.29.21) CRL entry extension αλλά ΔΥΝΑΤΑΙ να περιλαμβάνει το `ArchiveCutOff` (OID 1.3.6.1.5.5.7.48.1.6) σύμφωνα με την ενότητα 4.4.4 του RFC 6960.

8 Έλεγχος συμμόρφωσης και Άλλες Αξιολογήσεις

Η ΥΔΚ της HARICA κάθε φορά εκδίδει πιστοποιητικά και λειτουργεί σύμφωνα με την ισχύουσα νομοθεσία και τις απαιτήσεις της παρούσας ΠΠ / ΔΔΠ .

8.1 Συχνότητα ή συνθήκες της αξιολόγησης

Τα Πιστοποιητικά των ΑΠ που χρησιμοποιούνται για την έκδοση νέων πιστοποιητικών πρέπει είτε να έχουν τους Τεχνικούς Περιορισμούς της παραγράφου 7.1.5 και να ελέγχονται σύμφωνα μόνο με την παράγραφο 8.7, ή να μην έχουν Τεχνικούς Περιορισμούς και να ελέγχονται πλήρως σύμφωνα με όλες τις υπόλοιπες απαιτήσεις αυτής της παραγράφου.

Εξωτερικός έλεγχος συμμόρφωσης με την ΠΠ/ΔΔΠ απαιτείται σε ετήσια βάση.

8.2 Ταυτότητα/προσόντα του αξιολογητή

Ο εξωτερικός έλεγχος της HARICA γίνεται από εξειδικευμένο και διαπιστευμένο ελεγκτή, σύμφωνα με τις προδιαγραφές των κριτηρίων ελέγχου.

8.3 Σχέση του αξιολογητή με την αξιολογούμενη οντότητα

Οι εξωτερικοί ελεγκτές πρέπει να είναι ανεξάρτητοι από οποιαδήποτε σχέση που ενδέχεται να συνιστά σύγκρουση συμφερόντων, ή που θα μπορούσε σε οποιαδήποτε περίπτωση να επηρεάσει την αντικειμενική αξιολόγηση των εξωτερικών ελεγκτών.

8.4 Τα θέματα που καλύπτονται από την αξιολόγηση

Η ΥΔΚ HARICA καλύπτει τις προδιαγραφές των:

- ETSI EN 319 411-1 "*Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trusted Service Providers issuing certificates; Part 1: General Requirements*",
- ETSI EN 319 411-2 "*Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trusted Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*",
- ETSI EN 319 421 "*Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trusted Service Providers issuing Time-Stamps*", and
- Κανονισμός (EU) No 910/2014 (e-IDAS) του Ευρωπαϊκού Κοινοβουλίου και Συμβουλίου για την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης σε ηλεκτρονικές συναλλαγές στην ενδο-κοινοτική αγορά.

Επίσης, η HARICA έχει ενσωματώσει οδηγίες και διαδικασίες από τα κείμενα:

- "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates",
- "Guidelines for the Issuance and Management of Extended Validation Certificates",
- "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates Code Signing Certificates" and
- "Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates",

που δημοσιεύονται στη διεύθυνση https://www.cabforum.org.

Εκτός από τα παραπάνω πρότυπα, η HARICA συμμορφώνεται με το πρότυπο ETSI TS 119 495 που υποστηρίζει Περιγράμματα Εγκεκριμένων Πιστοποιητικών και Απαιτήσεις Πολιτικής του Παρόχου Υπηρεσιών Εμπιστοσύνης (TSP) βάσει της Οδηγίας (ΕΕ) 2015/2366 για τις υπηρεσίες πληρωμής και του Κανονισμού (ΕΕ) 2018/389 ως προς τις Κανονιστικές Τεχνικές Προδιαγραφές περί ισχυρής ταυτοποίησης πελατών και κοινά και ασφαλή ανοικτά πρότυπα επικοινωνίας.

8.5 Δράσεις που λαμβάνονται ως αποτέλεσμα της ανεπάρκειας

Σε περίπτωση που Ενδιάμεση ΑΠ διαπιστωθεί ότι δεν συμμορφώνεται με τις εγγυήσεις που αναφέρονται στην παράγραφο 9.6.1.1 και αποτύχει να συμμορφωθεί σε ικανοποιητικό βαθμό με τους στόχους που θέτουν, θα πρέπει να σταματήσει την έκδοση πιστοποιητικών που φέρουν το αντίστοιχο αναγνωριστικό πολιτικής (policy identifier), μέχρι να αξιολογηθεί ως συμμορφωμένη.

8.6 Ανακοίνωση των αποτελεσμάτων

Η Έκθεση Ελέγχου αναφέρει ρητά το πεδίο εφαρμογής των κριτηρίων ελέγχου. Η πιο πρόσφατη έκθεση ελέγχου θα είναι διαθέσιμη στο κοινό στην κεντρική ιστοσελίδα της HARICA (https://www.harica.gr). Οι εκθέσεις αυτές θα πρέπει επίσης, να υποβληθούν στους Προμηθευτές Λογισμικού Εφαρμογών για τα διάφορα προγράμματα Κορυφαίας ΑΠ και στην Εθνική Εποπτική Αρχή. Η HARICA δεν είναι υποχρεωμένη να δημοσιοποιεί τα γενικά πορίσματα του ελέγχου που δεν επηρεάζουν τη συνολική ελεγκτική γνώμη. Ορισμένοι Προμηθευτές Λογισμικού Εφαρμογών απαιτούν να συμπληρωθούν και να υπογραφούν από τους ελεγκτές ειδικές πρότυπες φόρμες. Αυτές οι φόρμες δεν απαιτείται να είναι διαθέσιμες στο κοινό, αλλά υποβάλλονται απευθείας στον αντίστοιχο Προμηθευτή Λογισμικού Εφαρμογών.

8.7 Εσωτερικός Έλεγχος

Η HARICA ανά πάσα στιγμή παρακολουθεί την τήρηση αυτής της ΠΠ/ΔΔΠ και ελέγχει την ποιότητα των υπηρεσιών της, εκτελώντας εσωτερικούς ελέγχους τουλάχιστον σε τριμηνιαία βάση σε ένα τυχαία επιλεγμένο δείγμα μεγαλύτερο του ενός πιστοποιητικού ή τουλάχιστον τρία τοις εκατό (3%) των Δημόσια Αξιόπιστων Πιστοποιητικών που εκδίδονται για SSL/TLS ή Υπογραφή Κώδικα, συμπεριλαμβανομένων των Πιστοποιητικών EV. Για όλα τα EV Πιστοποιητικά που οι απαιτήσεις περί της τελικής διασταύρωσης (Final Cross-Correlation) και ελέγχου με την δέουσα επιμέλεια (Due Diligence) της Ενότητας 11.13 των Οδηγιών EV εκπληρώνονται από μία εξωτερική ΑΚ, η HARICA ΠΡΕΠΕΙ να ελέγχει αυστηρά την ποιότητα των υπηρεσιών της ΑΚ πραγματοποιώντας τακτικούς εσωτερικούς ελέγχους

σε τυχαία επιλεγμένο δείγμα που αντιστοιχεί σε τουλάχιστον 6% των EV Πιστοποιητικών που εξέδωσε κατά την περίοδο που ξεκινά μετά την περίοδο του προηγούμενου δείγματος.

Στη χρονική διάρκεια κατά την οποία εκδίδει πιστοποιητικά για χρήση SSL/TLS μια Τεχνικά Περιορισμένη Ενδιάμεση ΑΠ, η HARICA επιβάλλεται να παρακολουθεί την τήρηση αυτής της ΠΠ/ΔΔΠ.

Εάν η HARICA αξιοποιεί κάποιον τρίτο στη διαδικασία ελέγχου εγκυρότητας για την έκδοση Πιστοποιητικών EV, η HARICA υποχρεώνει μέσω σύμβασης κάθε τρίτο Συνεργάτη, ΑΚ, υπεργολάβο και Εταιρική RA να συμμορφωθεί με τις ισχύουσες απαιτήσεις που περιγράφονται στο κείμενο των Οδηγιών EV και να τις εκτελεί όπως προβλέπει η ίδια η HARICA. Η HARICA επιβάλλει αυτές τις υποχρεώσεις και ελέγχει εσωτερικά σε ετήσια βάση τη συμμόρφωση με τις Οδηγίες EV των Συνεργατών, της ΑΚ, των υπεργολάβων και των Εταιρικών ΑΚ.

9 Εμπορικά και Νομικά θέματα

9.1 Κόστη εγγραφής

Δεν καταβάλλονται τέλη για τις παρεχόμενες υπηρεσίες στα Ελληνικά Ακαδημαϊκά κι Ερευνητικά Ιδρύματα. Η HARICA διατηρεί το δικαίωμα να επιβάλλει χρεώσεις στους Συνδρομητές εκτός των βασικών συνεργαζόμενων φορέων. Απαγορεύεται ρητά κάθε είδους μεταπώληση ή άλλου τύπου εκμετάλλευση των παρεχόμενων υπηρεσιών από συνδεδεμένους με την HARICA οργανισμούς.

9.1.1 Κόστος έκδοσης και ανανέωσης πιστοποιητικών

Η HARICA διατηρεί το δικαίωμα να επιβάλλει χρεώσεις στους Συνδρομητές εκτός των βασικών συνεργαζόμενων φορέων-μέλη της GUnet.

9.1.2 Κόστος πρόσβασης σε πιστοποιητικά

Δεν επιβάλλονται χρεώσεις σε πρόσωπα για την πρόσβαση σε πιστοποιητικά.

9.1.3 Κόστος ανάκλησης ή ερώτηση κατάστασης πιστοποιητικών

Δεν επιβάλλονται χρεώσεις για την ανάκληση ή τις πληροφορίες κατάστασης του πιστοποιητικού.

9.1.4 Κόστος άλλων υπηρεσιών

Η HARICA διατηρεί το δικαίωμα να επιβάλλει χρεώσεις για υπηρεσίες εκτός των τυπικών διαδικασιών του κύκλου ζωής του πιστοποιητικού.

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 κείμενο ΠΠ/ΔΔΠ.

9.3 Εμπιστευτικότητα πληροφοριών εμπορικού χαρακτήρα

9.3.1 Πεδίο εμπιστευτικών πληροφοριών

Τα ιδιωτικά κλειδιά των Αρχών Πιστοποίησης, ο πηγαίος κώδικας και τα ιδιωτικά κλειδιά για τις διαδικασίες αποθήκευσης/λειτουργίας θεωρούνται διαβαθμισμένες και εμπιστευτικές πληροφορίες. Πληροφορίες σχετικά με τη φυσική πρόσβαση και την ασφάλεια των χώρων όπου έχουν εγκατασταθεί και λειτουργούν οι ΑΠ και οι ΑΚ, θεωρούνται επίσης διαβαθμισμένες.

Τα σχέδια επιχειρησιακής ανάκαμψης σε περιπτώσεις καταστροφής, επίσης είναι εμπιστευτικά.

9.3.2 Πληροφορίες που δεν εμπίπτουν στο πεδίο των εμπιστευτικών πληροφοριών

Οι πληροφορίες που περιλαμβάνονται στα ψηφιακά πιστοποιητικά που εκδίδονται δεν θεωρούνται εμπιστευτικές.

9.3.3 Ευθύνες για την προστασία των εμπιστευτικών πληροφοριών

Το προσωπικό της HARICA και οι συνεργάτες είναι υπεύθυνοι για την προστασία των εμπιστευτικών πληροφοριών, να μην χρησιμοποιούν τις πληροφορίες αυτές γι' άλλον πλην τον σκοπό για τον οποίο αυτές προορίζονται και δεσμεύοντια ρητώς και συμβατικώς προς τούτο. Το προσωπικό της HARICA και οι χειριστές είναι εκπαιδευμένοι πώς να χρησιμοποιούν και να χειρίζονται εμπιστευτικές πληροφορίες σύμφωνα με την παράγραφο 5.3. Η HARICA λαμβάνει όλα τα κατάλληλα τεχνικά και οργανωτικά μέτρα για την εφαρμογή αυτής της πολιτικής.

9.4 Εμπιστευτικότητα πληροφοριών προσωπικού χαρακτήρα

9.4.1 Σχέδιο εμπιστευτικότητας

Η HARICA έχει εφαρμόσει Πολιτική Προστασίας Δεδομένων και έχει εκδώσει Δήλωση Προστασίας Δεδομένων, διαθέσιμη στη διεύθυνση https://repo.harica.gr/documents/Data-Privacy-Statement-EL.pdf, σε συμμόρφωση με την κείμενη νομοθεσία σχετικά με την προστασία δεδομένων και κάθε αντίστοιχη νομοθεσία και Ευρωπαϊκούς Κανονισμούς.

9.4.2 Πληροφορίες που χαρακτηρίζονται εμπιστευτικές

Οι Αρχές Καταχώρισης επεξεργάζονται προσωπικά δεδομένα κατά τη διαδικασία αναγνώρισης ταυτότητας κι επαλήθευσης του Αιτούντα τα οποία χαρακτηρίζονται εμπιστευτικά. Τα προσωπικά δεδομένα δεν αποκαλύπτονται εκτός αν το απαιτεί ο νόμος ή συμπεριλαμβάνονται στις δημόσιες πληροφορίες του πιστοποιητικού (για παράδειγμα στο πεδίο *subject* του πιστοποιητικού) με τη συναίνεση του Αιτούντα. Αν συμφωνεί ο Αιτών να συμπεριλάβει στο Πιστοποιητικό του προσωπικές πληροφορίες που σχετίζονται με την προσωπική του ταυτότητα που περιγράφονται στην παράγραφο 7.1.4.7 (Αριθμός Μητρώου Κοινωνικής Ασφάλισης, Αριθμός Ταυτότητας, Αριθμός Φορολογικού Μητρώου, Αριθμός Διαβατηρίου), τότε αυτές οι πληροφορίες δεν θεωρούνται εμπιστευτικές.

9.4.3 Πληροφορίες που δεν θεωρούνται εμπιστευτικές

Δεν θεωρούνται εμπιστευτικές οι πληροφορίες που περιέχονται στα ψηφιακά πιστοποιητικά που εκδίδονται. Αν ο Αιτών ζήτησε να προστεθούν προσωπικές πληροφορίες σε ένα Πιστοποιητικό, κατά τη διαδικασία της αίτησης, ενσωματώνοντας αυτές στο Πιστοποιητικό που εκδίδεται, ο Συνδρομητής συναινεί στην δημοσίευση αυτών των πληροφοριών από την HARICA.

9.4.4 Ευθύνη για την προστασία 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. Υπάρχουν συγκεκριμένα τεχνικά και οργανωτικά μέτρα για την αποτροπή μη εξουσιοδοτημένης ή παράνομης επεξεργασίας ή εξ' αμελείας απώλεια εμπιστευτικών και προσωπικών πληροφοριών.

9.4.5 Ενημέρωση και συγκατάθεση χρήσης εμπιστευτικών δεδομένων

Εκτός αν αναφέρεται άλλως στην παρούσα ΠΠ/ΔΔΠ, την Δήλωση Προστασίας Δεδομένων (διαθέσιμη στη διεύθυνση https://repo.harica.gr/documents/Data-Privacy-Statement-EL.pdf) ή δυνάμει συμφωνίας, όλες οι εμπιστευτικές και προσωπικές πληροφορίες που διαχειρίζεται και επεξεργάζεται η HARICA δεν χρησιμοποιούνται χωρίς προηγούμενη ενημέρωση ή συγκατάθεση όπου αυτό εφαρμόζεται, για το υποκείμενο στο οποίο αφορούν, σύμφωνα με την ισχύουσα νομοθεσία σχετικά με την προστασία δεδομένων και κάθε ισοδύναμη νομοθεσία και Ευρωπαϊκούς Κανονισμούς.

9.4.6 Γνωστοποίηση πληροφοριών σε δικαστικές ή δημόσιες αρχές

Οι μη εμπιστευτικές πληροφορίες που τηρεί κάθε Αρχή Πιστοποίησης και Καταχώισης είναι διαθέσιμες στις αρχές επιβολής του νόμου, μετά από επίσημη έγγραφη αίτησή τους.

Εμπιστευτικές και προσωπικές πληροφορίες μπορούν να γνωστοποιηθούν σε δικαστική αρχή εφόσον έχει εκδοθεί προς τούτο έγκυρο και εκτελεστό έγγραφο, όπως επίσημη διαταγή δικαστηρίου, απόφαση ή διοικητική πράξη, σύμφωνα με τις γενικές αρχές δικαίου και την ισχύουσα νομοθεσία. Η διαδικασία εκτελείται μέσω της ΕΔΠΠ (βλ. εντότητα 1.5). Ιδιωτικά κλειδιά που χρησιμοποιούνται για την υπογραφή πιστοποιητικών, δεν δημοσιοποιούνται σε τρίτους σε καμία περίπτωση, εκτός αν η HARICA είναι υποχρεωμένη προς τούτο δυνάμει ισχύουσας και εκτελεστής νομοθεσίας.

9.4.7 Άλλες περιπτώσεις διάθεσης πληροφοριών

Οι μη εμπιστευτικές και μη ιδιωτικές πληροφορίες που τηρεί κάθε ΑΠ και ΑΚ δύναται να γνωστοποιηθούν επί τη βάσει αιτημάτων οντοτήτων, για λόγους έννομου συμφέροντος.

Οι πληροφορίες που τηρεί κάθε ΑΠ και ΑΚ είναι διαθέσιμες στο νόμιμο ιδιοκτήτη τους (π.χ. φυσικό πρόσωπο που αιτήθηκε πιστοποιητικό), μετά από νόμιμο αίτημά του.

Αυτή η ενότητα διέπεται από την ισχύουσα νομοθεσία σχετικά με την προστασία δεδομένων και κάθε αντίστοιχη νομοθεσία και Ευρωπαϊκούς Κανονισμούς.

9.5 Δικαιώματα πνευματικής ιδιοκτησίας

Η ΥΔΚ HARICA έχει την κυριότητα όλων των δικαιωμάτων πνευματικής ιδιοκτησίας των υπηρεσιών ΥΔΚ που προσφέρει. Δεν έχει δικαιώματα πνευματικής ιδιοκτησίας στα κλειδιά των εκδιδόμενων πιστοποιητικών Συνδρομητών.

Οποιοσδήποτε μπορεί να αντιγράφει μέρη της ΠΠ/ΔΔΠ με την προϋπόθεση αναφοράς στο αυθεντικό κείμενο.

Σε αυτή την ΠΠ/ΔΔΠ χρησιμοποιούνται αποσπάσματα από τα CA/B Forum Baseline Requirements, Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates καθώς και απαιτήσεις των Mozilla και Microsoft Root Programs.

9.6 Δηλώσεις και Διαβεβαιώσεις

9.6.1 Δηλώσεις και Διαβεβαιώσεις ΑΠ

Με την έκδοση πιστοποιητικού, η HARICA παρέχει τις εξής διαβεβαιώσεις στους εξής δικαιούχους του Πιστοποιητικού και έλκοντες συμφέρον εξ αυτού (Δικαιούχους):

1. Στο Συνδρομητή που είναι συμβαλλόμενο μέρος της Σύμβασης Συνδρομητή ή Όρων Χρήσης του Πιστοποιητικού
2. Σε όλους τους Προμηθευτές Λογισμικού Εφαρμογών, με τους οποίους η Κορυφαία ΑΠ έχει συνάψει σύμβαση για την ένταξη του Κορυφαίου Πιστοποιητικού της στο λογισμικό που διανέμεται από τους εν λόγω Προμηθευτές
3. Σε όλα τα Βασιζόμενα Μέρη τα οποία ευλόγως βασίζονται σε ένα Έγκυρο Πιστοποιητικό.

Η HARICA δηλώνει και διαβεβαιώνει στους Δικαιούχους του πιστοποιητικού ότι, κατά τη περίοδο που το πιστοποιητικό είναι έγκυρο, έχει συμμορφωθεί με αυτό το κείμενο ΠΠ / ΔΔΠ όσον αφορά στην έκδοση και στη διαχείριση του Πιστοποιητικού.

Οι Διαβεβαιώσεις Πιστοποιητικού ειδικότερα περιλαμβάνουν, χωρίς να περιορίζονται, τα ακόλουθα:

- ✓ Παρέχουν και συντηρούν την υποδομή που απαιτείται για τη διατήρηση της ιεραρχίας ενός Παρόχου Υπηρεσιών Εμπιστοσύνης, σύμφωνα με τις διαδικασίες πιστοποίησης που περιγράφονται στο παρόν έγγραφο.
- ✓ Εφαρμόζουν και διατηρούν τις απαιτήσεις ασφάλειας, σύμφωνα με σχετικές παραγράφους του παρόντος εγγράφου.
- ✓ Αποδέχονται ή απορρίπτουν αιτήσεις για έκδοση πιστοποιητικών σύμφωνα με τις σχετικές παραγράφους του παρόντος εγγράφου.
- ✓ Διατηρούν δημόσια προσβάσιμο κατάλογο πιστοποιητικών και ΛΑΠ. Οι πληροφορίες αυτές πρέπει να είναι διαθέσιμες στο κοινό μέσω ευρέως χρησιμοποιούμενων πρωτοκόλλων όπως HTTP, FTP και LDAP.
- ✓ Ανακαλούν πιστοποιητικά όταν συντρέχουν ειδικοί λόγοι ή μετά από ένα αίτημα του υποκειμένου του πιστοποιητικού.
- ✓ Διατηρούν ενημερωμένη τη ΛΑΠ.
- ✓ Διαχειρίζονται όλες τις προσωπικές και εμπιστευτικές πληροφορίες των Συνδρομητών με εμπιστευτικότητα.

- ✓ Ενημερώνουν άμεσα το τεχνικό προσωπικό των Υφιστάμενων ΑΠ, για οποιαδήποτε απώλεια, τροποποίηση ή μη εξουσιοδοτημένη χρήση του ιδιωτικού κλειδιού της ΑΠ.
- ✓ Επιβεβαιώνουν ότι όλες οι υπηρεσίες που παρέχονται στο σύνολο της υποδομής συμμορφώνονται με τους όρους και τις προϋποθέσεις της παρούσας ΠΠ / ΔΔΠ.
- ✓ Η HARICA διατηρεί ένα 24x7 δημοσίως προσβάσιμο Αποθετήριο με τις τρέχουσες πληροφορίες σχετικά με την κατάσταση (αν είναι έγκυρα ή αν έχουν ανακληθεί) όλων των Πιστοποιητικών που δεν έχουν λήξει.
- ✓ Η HARICA θα ανακαλέσει το Πιστοποιητικό για οποιονδήποτε από τους λόγους που αναφέρονται στην παράγραφο 4.9.1.1 της παρούσας ΠΠ / ΔΔΠ.

Για τα Πιστοποιητικά EV (Εκτεταμένου Ελέγχου Εγκυρότητας), οι Εγγυήσεις Πιστοποιητικού EV συμπεριλαμβάνουν ειδικά, αλλά δεν περιορίζονται σε αυτά, τα ακόλουθα:

1. **Νομική Υπόσταση**: Η HARICA έχει επιβεβαιώσει με την Υπηρεσία Σύστασης στην Δικαιοδοσία Σύστασης του Υποκειμένου ότι, από την ημερομηνία έκδοσης του EV Πιστοποιητικού κι έπειτα, το Υποκείμενο που κατονομάζεται στο EV πιστοποιητικό υφίσταται νόμιμα ως έγκυρος οργανισμός ή φορέας στην αντίστοιχη Δικαιοδοσία Σύστασης.
2. **Ταυτότητα**: Η HARICA έχει επιβεβαιώσει ότι, κατά την ημερομηνία έκδοσης του Πιστοποιητικού EV, η επωνυμία του Υποκειμένου που κατονομάζεται στο EV πιστοποιητικό αντιστοιχεί στην επωνυμία που είναι καταχωρισμένη στα επίσημα κρατικά αρχεία της Υπηρεσίας Σύστασης στην Δικαιοδοσία Σύστασης ή Εγγραφής του Υποκειμένου, και εάν περιλαμβάνεται επίσης ένα υποθετικό όνομα, ότι το υποθετικό όνομα έχει καταχωρισθεί σωστά από το Υποκείμενο στην δικαιοδοσία του Τόπου άσκησης της Επιχείρησης.
3. **Δικαίωμα Χρήσης Ονόματος Χώρου**: Η HARICA έχει λάβει όλα τα μέτρα που είναι ευλόγως απαραίτητα για να επαληθεύσει ότι, από την ημερομηνία έκδοσης του Πιστοποιητικού EV κι έπειτα, το Υποκείμενο που κατονομάζεται στο EV πιστοποιητικό έχει το δικαίωμα να χρησιμοποιεί όλα τα Ονόματα Χώρου που περιλαμβάνονται στο EV πιστοποιητικό,
4. **Εξουσιοδότηση για EV πιστοποιητικό**: Η HARICA έχει λάβει όλα τα μέτρα που είναι ευλόγως απαραίτητα για να επαληθεύσει ότι το Υποκείμενο που κατονομάζεται στο EV πιστοποιητικό έχει εξουσιοδοτήσει την έκδοση του Πιστοποιητικού EV,
5. **Ακρίβεια των Πληροφοριών**: Η HARICA έχει λάβει όλα τα μέτρα που είναι ευλόγως απαραίτητα για να επαληθεύσει ότι όλες οι άλλες πληροφορίες στο EV πιστοποιητικό είναι ακριβείς, από την ημερομηνία έκδοσης του Πιστοποιητικού EV κι έπειτα.
6. **Σύμβαση Συνδρομητή**: Το Υποκείμενο που κατονομάζεται στο EV πιστοποιητικό έχει συνάψει με νόμιμο τρόπο έγκυρη και εκτελεστέα Σύμβαση Συνδρομητή με την HARICA σύμφωνα με τις απαιτήσεις αυτής της ΠΠ/ΔΔΠ ή, εφόσον συνεργάζονται, ο Αντιπρόσωπος Αιτούντα έχει αναγνωρίσει και αποδεχτεί τους Όρους Χρήσης,
7. **Κατάσταση**: Η HARICA θα ακολουθήσει τις διαδικασίες αυτής της ΠΠ/ΔΔΠ και θα συντηρεί διαθέσιμο 24 x 7 ένα Αποθετήριο διαδικτυακά (online) που θα περιέχει πληροφορίες για την τρέχουσα κατάσταση του Πιστοποιητικού EV αν είναι Έγκυρο ή ανακληθέν, και

8. **Ανάκληση**: Η HARICA θα ακολουθήσει τις διαδικασίες της παρούσας ΠΠ/ΔΔΠ και θα ανακαλέσει το EV πιστοποιητικό για οποιονδήποτε από τους λόγους ανάκλησης που καθορίζονται στην παρούσα ΠΠ/ΔΔΠ.

Η HARICA είναι υπεύθυνη για την εκπλήρωση και τις διαβεβαιώσεις των Υφιστάμενων ΑΠ, για τη συμμόρφωση των Υφιστάμενων ΑΠ με την παρούσα ΠΠ/ΔΔΠ και για όλες τις υποχρεώσεις και τις αποζημιώσεις των Υφιστάμενων ΑΠ στο πλαίσιο της παρούσας ΠΠ/ΔΔΠ, σαν να ήταν η HARICA η υφιστάμενη ΑΠ που εξέδωσε τα Πιστοποιητικά.

Η HARICA διαβεβαιώνει τα ακόλουθα όσον αφορά τους Συνδρομητές Αρχών Χρονοσήμανσης και τα παραγόμενα τεκμήρια χρονοσήμανσης:

- ✓ Παρέχει και συντηρεί την υποδομή χρονοσήμανσης που απαιτείται για τη συγκρότηση της ιεραρχίας ενός Παρόχου Υπηρεσιών Εμπιστοσύνης, σύμφωνα με τις διαδικασίες πιστοποίησης που περιγράφονται στο παρόν έγγραφο
- ✓ Η ΜΧΣ διατηρεί την ελάχιστη ακρίβεια ± 1 δευτερολέπτου σε UTC
- ✓ Εφαρμόζει και διατηρεί τις απαιτήσεις ασφάλειας σύμφωνα με τις σχετικές παραγράφους του παρόντος κειμένου.

9.6.1.1 Αρμοδιότητες από Αρχών Πιστοποίησης Εξωτερικής Λειτουργίας

Κάθε Αρχή Πιστοποίησης Εξωτερικής Λειτουργίας που έχει εγκριθεί από την ΥΔΚ της HARICA δεσμεύεται για τα παρακάτω:

- ✓ Να ακολουθεί όλους τους κανόνες και τις διαδικασίες που ισχύουν για την παρούσα ΠΠ / ΔΔΠ σχετικά με τις Αρχές Πιστοποίησης.
- ✓ Να κατέχει πιστοποιητικά με περίοδο ισχύος εντός των ορίων της ενεργού σχέσης απασχόλησης (ή άλλης) μεταξύ του αιτούντος και του φορέα ή οργανισμού, σύμφωνα με την ιδιότητα του αιτούντος (π.χ. φοιτητή, εργαζομένου, διδάσκοντα).
- ✓ Να ενημερώνουν την ανώτερη Αρχή Πιστοποίησης αμέσως σε περίπτωση παραβίασης του ιδιωτικού κλειδιού.
- ✓ Να προστατέψει τα ιδιωτικά κλειδιά, που χρησιμοποιούνται για την υπογραφή του πιστοποιητικού, τουλάχιστον στο επίπεδο ασφαλείας που περιγράφεται στο παρόν έγγραφο.
- ✓ Να αναπτύξει (προαιρετικά) τις πολιτικές και τις διαδικασίες πιστοποίησης της, οι οποίες πρέπει να είναι τουλάχιστον τόσο αυστηρές και δεσμευτικές όσο αυτές που περιγράφονται στο παρόν έγγραφο.
- ✓ Σε περίπτωση που ένας οργανισμός θέλει να τρέξει μία υφιστάμενη ΑΠ Εξωτερικής Διαχείρισης, σύμφωνα με το πεδίο εφαρμογής της πιστοποίησης της, πρέπει να παρέχει ένα επίσημο πιστοποιητικό αξιολόγησης, σύμφωνα με τις απαιτήσεις των τελευταίων εκδόσεων του ETSI EN 319 411-1, ETSI EN 319 411-2 (ή ισοδύναμο), και της νεότερης έκδοσης του εγγράφου "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates", που παράγεται από το CA/Browser Forum (www.cabforum.org).

9.6.2 Δηλώσεις και Διαβεβαιώσεις των ΑΚ

- ✓ Κάθε ΑΚ είναι υπεύθυνη να λαμβάνει αιτήσεις πιστοποιητικών από τους Αιτούντες. Επικυρώνει την ταυτότητα του Αιτούντα, επιβεβαιώνει ότι το δημόσιο κλειδί που υπεβλήθη ανήκει στον Αιτούντα και μεταφέρει με ασφάλεια την εφαρμογή στην ΑΠ

- ✓ Ανάλογα με τον τύπο του πιστοποιητικού, οι αιτήσεις μπορούν να υποβληθούν με δια ζώσης συνάντησης με το ενδιαφερόμενο μέρος, μέσω email, μέσω ασφαλούς ιστοσελίδας ή μέσω οποιουδήποτε μηχανισμού που αναγνωρίζει την ταυτότητα του Αιτούντα με ασφάλεια. Η αίτηση περιλαμβάνει όλες τις πληροφορίες που αναγνωρίζουν την ταυτότητα του Συνδρομητή, και το αντίστοιχο δημόσιο κλειδί.
- ✓ Μαζική υποβολή αιτήσεων από ειδικό τμήμα ή Οργανισμό είναι πιθανή εκ μέρους των προσώπων που ανήκουν στο τμήμα ή στον οργανισμό
- ✓ Κάθε ΑΚ πρέπει να επαληθεύει αν οποιοδήποτε πρόσωπο που αιτείται πιστοποιητικό είναι ο νόμιμος δικαιούχος της πιστοποιημένης διεύθυνσης email.
- ✓ Κάθε ΑΚ πρέπει να επαληθεύει ότι το πρόσωπο που αιτείται πιστοποιητικό συσκευής είναι ο νόμιμος κάτοχος και διαχειριστής του FQDN της συσκευής (εξυπηρετητή).
- ✓ Στην περίπτωση που ένας οργανισμός θέλει να λειτουργήσει τη δική του ΑΚ, σύμφωνα με το πεδίο εφαρμογής της πιστοποίησης του, πρέπει να παρέχει επίσημο πιστοποιητικό αξιολόγησης, σύμφωνα με τις απαιτήσεις των τελευταίων εκδόσεων του ETSI EN 319 411-1, ETSI EN 319 411-2 (ή ισοδύναμο), και της νεότερης έκδοσης του εγγράφου “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates”, που παράγεται από το CA/Browser Forum (http://www.cabforum.org).

Οι ΑΚ έχουν επίσης δεσμευτεί να εξασφαλίσουν τα εξής:

- ✓ **Δικαίωμα χρήσης του Ονόματος Χώρου:** Δηλαδή, κατά το χρόνο της έκδοσης, η HARICA εφάρμοσε και ακολούθησε μια διαδικασία για την εξακρίβωση ότι ο Αιτών είτε είχε το δικαίωμα να χρησιμοποιήσει, ή είχε υπό τον έλεγχό του, το Όνομα Χώρου που αναφέρεται στο πεδίο subject του Πιστοποιητικού και στην επέκταση subjectAltName (ή, μόνο στην περίπτωση Ονομάτων Χώρου, του ανατέθηκε το εν λόγω δικαίωμα ή ο έλεγχος από κάποιον που είχε τέτοιο δικαίωμα χρήσης ή ελέγχου).
- ✓ **Εξουσιοδότηση για Πιστοποιητικό:** Δηλαδή, κατά το χρόνο της έκδοσης, η HARICA εφάρμοσε και ακολούθησε διαδικασία για την επαλήθευση ότι το Υποκείμενο εξουσιοδότησε την έκδοση του Πιστοποιητικού και ότι ο Εκπρόσωπος του Αιτούντα εξουσιοδοτείται να αιτηθεί το Πιστοποιητικό για λογαριασμό του Υποκειμένου.
- ✓ **Ακρίβεια των Πληροφοριών:** Δηλαδή, κατά το χρόνο της έκδοσης, η HARICA εφάρμοσε και ακολούθησε διαδικασία για την επαλήθευση της ακρίβειας όλων των πληροφοριών που περιέχονται στο Πιστοποιητικό (με εξαίρεση το χαρακτηριστικό subject:organizationalUnitName).
- ✓ **Μη Παραπλανητικές πληροφορίες**: Κατά τον χρόνο της έκδοσης, η HARICA εφάρμοσε και ακολούθησε διαδικασία για τη μείωση της πιθανότητας οι πληροφορίες που περιέχονται στο χαρακτηριστικό subject:organizationalUnitName του Πιστοποιητικού να είναι παραπλανητικές.
- ✓ **Ταυτότητα του αιτούντος:** Δηλαδή, εάν το πιστοποιητικό περιέχει πληροφορίες ταυτότητας του υποκειμένου, η HARICA εφάρμοσε και ακολούθησε διαδικασία για την εξακρίβωση της ταυτότητας του Αιτούντος, σύμφωνα με την παράγραφο 3.2.
- ✓ **Σύμβαση Συνδρομητή:** Δηλαδή, αν η HARICA και ο Συνδρομητής δεν είναι συνεργάτες, ο Συνδρομητής και η ΑΠ είναι συμβαλλόμενα μέρη σε μια νομικά

έγκυρη και εκτελεστή Σύμβαση Συνδρομητή που ικανοποιεί αυτό το κείμενο ΠΠ / ΔΔΠ ή, αν η HARICA και ο Συνδρομητής είναι Συνδεδεμένες Οντότητες, ότι ο Εκπρόσωπος του Αιτούντα αναγνώρισε και αποδέχθηκε τους Όρους Χρήσης.

9.6.3 Δηλώσεις και Διαβεβαιώσεις Συνδρομητή

Η HARICA απαιτεί, ως μέρος της Σύμβασης Συνδρομητή, ο αιτών να υλοποιεί τις δεσμεύσεις και διαβεβαιώσεις αυτής της ενότητας προς όφελος της HARICA και των Δικαιούχων του Πιστοποιητικού.

Πριν από την έκδοση του Πιστοποιητικού, η HARICA θα λαμβάνει προς σαφές όφελος της ίδιας και των Δικαιούχων του Πιστοποιητικού, τη συμφωνία του Αιτούντος με τη Σύμβαση Συνδρομητή και με τους Όρους Χρήσης.

Η Σύμβαση Συνδρομητή ή οι Όροι Χρήσης περιέχουν τις ακόλουθες υποχρεώσεις και διαβεβαιώσεις:

- ✓ Οι Συνδρομητές της ΥΔΚ της HARICA είναι υποχρεωμένοι να διαβάσουν, να αποδεχθούν και να συμμορφωθούν με την παρούσα Πολιτική Πιστοποίησης / Δήλωση Διαδικασιών Πιστοποίησης. Οι Συνδρομητές είναι υποχρεωμένοι να χρησιμοποιούν τα πιστοποιητικά αποκλειστικά για τους σκοπούς που περιγράφονται στην παρούσα ΠΠ / ΔΠΠ και το ισχύον δίκαιο. Τα Πιστοποιητικά της HARICA δεν μπορούν να χρησιμοποιηθούν για υπηρεσίες ή συστήματα όπου, σε περίπτωση διακοπής λειτουργίας ή βλάβης, προκύπτει αξιοσημείωτη εμφανής ή μη εμφανής καταστροφή ή κίνδυνος για τη ζωή.
- ✓ Η αίτηση του Συνδρομητή για πιστοποιητικό και η έκδοσή του δεν βαρύνεται με δικαιώματα πνευματικής ή διανοητικής ιδιοκτησίας τρίτων, δεν περιέχει δεδομένα τα οποία με οιοδήποτε τρόπο παρεμβαίνουν ή παραβιάζουν δικαιώματα οποιουδήποτε τρίτου, σε οποιαδήποτε δικαιοδοσία, σε σχέση με διπλώματα ευρεσιτεχνίας, εμπορικά σήματα, σήματα υπηρεσιών, επωνυμίες, ονόματα εταιρειών, διακριτικούς τίτλους και άλλα εμπορικά δικαιώματα, και δεν εμφανίζει τα δεδομένα για οποιαδήποτε αιτία που δεν είναι απολύτως νόμιμη.
- ✓ Οι Συνδρομητές πρέπει να δημιουργήσουν ένα ζεύγος κλειδιών (ιδιωτικό και δημόσιο) χρησιμοποιώντας ένα αξιόπιστο και ασφαλές σύστημα και να λάβουν όλες τις απαραίτητες προφυλάξεις για την προστασία του ιδιωτικού κλειδιού τους από καταστροφή, απώλεια ή κλοπή.
- ✓ Αφού λάβουν το πιστοποιητικό τους, οι συνδρομητές συμφωνούν και επιβεβαιώνουν ότι οι πληροφορίες που περιέχονται στο πιστοποιητικό είναι ακριβείς.
- ✓ Οι Συνδρομητές θα πρέπει να ζητήσουν την ανάκληση του πιστοποιητικού όταν δεν χρησιμοποιείται πια, όταν τα δεδομένα που περιέχονται έχουν αλλάξει ή όταν υπάρχει υποψία ότι το ιδιωτικό κλειδί έχει παραβιασθεί ή χαθεί. Η ΜΗ αίτηση ανάκλησης Πιστοποιητικού, ακυρώνει οποιαδήποτε υποχρέωση διεκδικήσεων αν το ιδιωτικό κλειδί ή το Πιστοποιητικό χρησιμοποιηθεί εσφαλμένα ενώ θα έπρεπε να έχει ανακληθεί.
- ✓ Ειδικά στην περίπτωση της υπογραφής κώδικα, οι Συνδρομητές δεσμεύονται από την ΑΚ να παρέχουν πλήρεις, ακριβείς και αληθείς πληροφορίες (π.χ. όνομα εφαρμογής, URL, περιγραφή εφαρμογής, κ.α.) στον υπογεγραμμένο κώδικα. Οι Συνδρομητές επίσης, δεσμεύονται να μην υπογράψουν σκόπιμα

Ύποπτο Κώδικα και αναγνωρίζουν ότι τέτοια ενέργεια θα επιτρέψει στην HARICA να ανακαλέσει αυτόματα το υπογράφων Πιστοποιητικό.

- ✓ **Ακρίβεια των Πληροφοριών:** Η υποχρέωση και εγγύηση να παρέχουν ακριβείς και πλήρεις πληροφορίες, ανά πάσα στιγμή στην HARICA, τόσο κατά την αίτηση για πιστοποιητικό αλλά και όπως αλλιώς ζητηθεί από την HARICA όσον αφορά στην έκδοση του πιστοποιητικού (-ων) που πρέπει να παρέχονται από την HARICA.
- ✓ **Τερματισμός της χρήσης του πιστοποιητικού:** Η υποχρέωση και εγγύηση να παύσει αμέσως κάθε χρήση του Ιδιωτικού Κλειδιού που αντιστοιχεί στο Δημόσιο Κλειδί που περιλαμβάνεται στο Πιστοποιητικό κατά την ανάκληση του εν λόγω πιστοποιητικού, για λόγους παραβίασης του Κλειδιού.
- ✓ **Ανταπόκριση:** Η υποχρέωση να ανταποκριθεί στις οδηγίες της HARICA σχετικά με την παραβίαση του Κλειδιού ή την κατάχρηση πιστοποιητικού εντός συγκεκριμένης χρονικής περιόδου.
- ✓ **Αναγνώριση και Αποδοχή:** Η αναγνώριση και η αποδοχή ότι η HARICA έχει το δικαίωμα να ανακαλέσει το πιστοποιητικό αμέσως αν ο Αιτών παραβιάζει τη Σύμβαση Συνδρομητή ή τους Όρους Χρήσης ή αν η HARICA ανακαλύψει ότι το πιστοποιητικό χρησιμοποιείται για να επιτρέψει εγκληματικές δραστηριότητες, όπως οι επιθέσεις phishing, η απάτη ή διανομή κακόβουλου προγράμματος.

Στην περίπτωση Συνδρομητών Αρχών Χρονοσήμανσης της HARICA,

- ✓ Πρέπει να επαληθεύουν ότι το αιτούμενο τεκμήριο χρονοσήμανσης έχει υπογραφεί από ιδιωτικό κλειδί ΜΧΣ που αντιστοιχεί σε έγκυρο Πιστοποιητικό ΜΧΣ της HARICA και να ελέγχουν για πιθανές ανακλήσεις.
- ✓ Πρέπει να χρησιμοποιούν Χρονοσφραγίδες από ΜΧΣ της HARICA σε συνδυασμό με έγκυρο Πιστοποιητικό (που δεν έχει ανακληθεί).

9.6.4 Δηλώσεις και Διαβεβαιώσεις Βασιζόμενων Μερών

- ✓ Τα Πιστοποιητικά της HARICA δεν μπορούν να χρησιμοποιηθούν για υπηρεσίες ή συστήματα όπου, σε περίπτωση διακοπής λειτουργίας ή βλάβης, προκύπτει αξιοσημείωτη εμφανής ή μη εμφανής καταστροφή ή κίνδυνος για τη ζωή.
- ✓ Οι οντότητες που εμπιστεύονται τα πιστοποιητικά που εκδίδονται είναι υποχρεωμένες να διαβάσουν και αποδεχτούν την Πολιτική Πιστοποίησης/Δήλωση Διαδικασιών Πιστοποίησης και να χρησιμοποιούν τα πιστοποιητικά μόνο με τρόπους που είναι σύμφωνες με την ΠΠ / ΔΔΠ και την ισχύουσα νομοθεσία.
- ✓ Οι οντότητες που εμπιστεύονται τα πιστοποιητικά πρέπει να ελέγχουν την εγκυρότητα της ψηφιακής υπογραφής του πιστοποιητικού και να εμπιστεύονται τις ανώτερες Αρχές Πιστοποίησης. Τέλος, θα πρέπει να ελέγχεται περιοδικά για πιθανές ανακλήσεις η εγκυρότητα του πιστοποιητικού στην αντίστοιχη ΛΑΠ, με χρήση του Online Πρωτοκόλλου Κατάστασης Πιστοποιητικών (OCSP).
- ✓ Οι οντότητες που εμπιστεύονται τα πιστοποιητικά πρέπει να ελέγχουν την επέκταση χρήσης κλειδιού X.509 στο τελικό Πιστοποιητικό και στο Πιστοποιητικό της Εκδούσας ΑΠ για την κατάλληλη χρήση των πιστοποιητικών.
- ✓ Συλλέγουν αρκετές πληροφορίες για να προσδιοριστεί ο βαθμός στον οποίο μπορούν να βασίζονται σε ένα ψηφιακό πιστοποιητικό

- ✓ Φέρουν την πλήρη και αποκλειστική ευθύνη για οποιαδήποτε απόφαση να βασίζονται σε ένα ψηφιακό πιστοποιητικό
- ✓ Αναλαμβάνουν πλήρως τις συνέπειες, συμπεριλαμβανομένων των νομικών ευθυνών, για οποιαδήποτε μη τήρηση των υποχρεώσεων και των ευθυνών τους, όπως περιγράφεται σε αυτό το ΠΠ/ΔΔΠ.
- ✓ Οι οντότητες που εμπιστεύονται τις Χρονοσφραγίδες πρέπει να επαληθεύουν ότι το τεκμήριο χρονοσήμανσης έχει υπογραφεί από ένα Ιδιωτικό Κλειδί ΜΧΣ που αντιστοιχεί σε ένα έγκυρο Πιστοποιητικό ΜΧΣ της HARICA και να ελέγχουν για πιθανές ανακλήσεις μέχρι τη στιγμή της επαλήθευσης. Αν συμβεί οποιαδήποτε ανάκληση μετά την ημερομηνία λήξης του Πιστοποιητικού της ΜΧΣ, παρέχουν οδηγίες τα προβλεπόμενα του Παραρτήματος Δ του προτύπου ETSI EN 319 421.
- ✓ Οι οντότητες που εμπιστεύονται τις Χρονοσφραγίδες πρέπει να θεωρούν οποιουσδήποτε περιορισμούς χρήσης της χρονοσφραγίδας ότι επιβάλλονται από την πολιτική χρονοσήμανσης και να θεωρούν οποιεσδήποτε άλλες προφυλάξεις ότι υπαγορεύονται από Συμβάσεις ή άλλους όρους.
- ✓ Οι οντότητες που εμπιστεύονται τις Χρονοσφραγίδες ως «Εγκεκριμένες», πρέπει να χρησιμοποιούν τον κατάλογο εμπίστευσης σύμφωνα με το άρθρο 22 παράγραφος 5 του κανονισμού (ΕΕ) αριθ. 910/2014 (eIDAS), για να αποφασίσουν αν η μονάδα Χρονοσήμανσης και η Χρονοσήμανση είναι εγκεκριμένες. Αν το δημόσιο κλειδί της ΜΧΣ καταγράφεται στην Αξιόπιστη Λίστα και η υπηρεσία η οποία εκπροσωπεί είναι μία εγκεκριμένη υπηρεσία χρονοσήμανσης, τότε οι χρονοσφραγίδες που εκδίδονται από αυτήν τη ΜΧΣ μπορούν να θεωρούνται εγκεκριμένες.

9.6.5 Δηλώσεις και Διαβεβαιώσεις Λοιπών Συμμετεχόντων

Δεν ορίζεται.

9.7 Αποποίηση ευθύνης

Δεν ορίζεται

9.8 Περιορισμοί ευθυνών

Αυτή η ρήτρα ισχύει για συμβατική ευθύνη (συμπεριλαμβανομένης οποιασδήποτε αποζημίωσης ή παραβίασης της εγγύησης), για ευθύνη από αδικοπραξία (συμπεριλαμβανομένης της αμέλειας), η εκ του Νόμου ή άλλως για μη συμμορφούμενη χρήση του πιστοποιητικού ή των σχετικών ιδιωτικών κλειδιών, την πληροφορία ανάκλησης ή οποιοδήποτε άλλο υλικό ή λογισμικό που παρέχεται και τυχόν επακόλουθες, παρεπόμενες, ειδικές ή αποτρεπτικές ζημίες που προκύπτουν από ή σχετίζονται με αυτή τη ΠΠ/ΔΔΠ, συμπεριλαμβανομένων, ενδεικτικά και όχι περιοριστικά, απώλειας δεδομένων, απώλειας επιχειρηματικής δραστηριότητας και απώλειας κέρδους.

Με εξαίρεση των όσων ορίζονται στην επόμενη παράγραφο, και στο βαθμό που επιτρέπεται από την ισχύουσα νομοθεσία, η Υποδομή Δημοσίου Κλειδιού της HARICA δεν ευθύνεται για προβλήματα ή ζημιές που μπορεί να προκύψουν από τις υπηρεσίες της σε περίπτωση λανθασμένης, απρόσεκτης ή ακατάλληλης χρήσης των πιστοποιητικών που εκδίδει. Η ΥΔΚ HARICA δεν αναλαμβάνει οποιαδήποτε οικονομική, αστική ή άλλους είδους ευθύνη για τέτοιες περιπτώσεις. Η χρήση της ΥΔΚ HARICA και των υπηρεσιών Πιστοποίησης προϋποθέτει την ανεπιφύλακτη αποδοχή

εκ μέρους των χρηστών της παρούσας ΠΠ/ΔΔΠ και το γεγονός ότι η ΥΔΚ HARICA δεν είναι υπόλογη και δεν αναλαμβάνει οποιαδήποτε οικονομική, αστική ή άλλη ευθύνη, εκτός από τις περιπτώσεις που υπάρχουν στοιχεία δόλιας συμπεριφοράς ή σοβαρής αμέλειας από την ΥΔΚ της HARICA και τους διαχειριστές της. Η ΥΔΚ της HARICA δεν είναι υπόλογη στο Συνδρομητή για οποιαδήποτε ζημία με ευθύνη του Συνδρομητή κατά την χρήση του Πιστοποιητικού εκτός της συνήθους και προβλεπόμενης χρήσης.

Οι Συνδρομητές είναι υποχρεωμένοι να αιτούνται ανάκληση Πιστοποιητικού για τους λόγους που αναφέρονται στην παράγραφο 9.6.3. Παράλειψη αιτήματος ανακλήσεως του Πιστοποιητικού, αίρει και ακυρώνει οποιαδήποτε αξίωση ευθύνης, εάν το ιδιωτικό κλειδί ή το Πιστοποιητικό χρησιμοποιείται εσφαλμένα, όταν θα έπρεπε να ανακληθεί με ενέργειες προερχόμενες από τον Συνδρομητή.

Στην περίπτωση που η ΥΔΚ της HARICA παρεκκλίνει σημαντικά από τα προβλεπόμενα που ορίζονται σε αυτό το κείμενο ΠΠ/ΔΔΠ όταν εκδίδονται «**Εγκεκριμένα Πιστοποιητικά για ηλεκτρονικές υπογραφές**», «**Εγκεκριμένα Πιστοποιητικά για ηλεκτρονικές σφραγίδες**», **«Εγκεκριμένα Πιστοποιητικά για επαλήθευση ταυτότητας ιστοχώρων»**, **Πιστοποιητικά EV (εκτεταμένου ελέγχου εγκυρότητας) για SSL ή Υπογραφή Κώδικα»**, προβλέπονται συγκεκριμένες ευθύνες/αποζημιώσεις:

- Η HARICA είναι υπόλογη μόνο για τη σωστή επαλήθευση της αίτησης και τα επακόλουθα περιεχόμενα του Πιστοποιητικού (με εξαίρεση το πεδίου "OU" όπως δηλώνεται στην παράγραφο 9.6.2).
- Η HARICA δε θα είναι υπόλογη αν ο Αιτών/Συνδρομητής υπέβαλε ψευδή ή παραποιημένα τεκμήρια κατά τον έλεγχο εγκυρότητας και πληροφορίες από αυτά τα τεκμήρια συμπεριλήφθηκαν σε Πιστοποιητικό. Σε αυτήν την περίπτωση, ο Συνδρομητής ευθύνεται για τη ζημία που μπορεί να υποστεί η HARICA και/ή η GUnet εξαιτίας των λανθασμένων στοιχείων που συμπεριλήφθηκαν σε Πιστοποιητικό ή εξαιτίας του λάθους τρόπου χρήσης του Πιστοποιητικού από τον Συνδρομητή.

Με εξαίρεση των προηγούμενων περιπτώσεων, η μέγιστη συνολική ευθύνη της HARICA σύμφωνα με αυτή την ΠΠ/ΔΔΠ, έναντι των Συνδρομητών ή Βασιζόμενων Μερών περιορίζεται σε **2.000€ κατ' ανώτατο όριο ανά Εγκεκριμένο Πιστοποιητικό για Υπογραφές/Σφραγίδες, Εγκεκριμένο Πιστοποιητικό για επαλήθευση ταυτότητας ιστοχώρου, Πιστοποιητικά EV για SSL και Πιστοποιητικά EV για Υπογραφή Κώδικα** και συνολικό μέγιστο όριο απαιτήσεων **1.000.000€,** ανεξαρτήτως της φύσης της ευθύνης και τον τύπο, το ποσό ή την έκταση της ζημίας που τυχόν υποστούν. Οι περιορισμοί ευθύνης που προβλέπονται σε αυτή την παράγραφο είναι οι ίδιοι ανεξάρτητα από τον αριθμό των Πιστοποιητικών, των συναλλαγών, ή των αξιώσεων που σχετίζονται με αυτό το Πιστοποιητικό. Οι περιορισμοί ευθύνης που παρέχονται εδώ εφαρμόζονται στο μέγιστο βαθμό που επιτρέπεται σύμφωνα με την εκάστοτε ισχύουσα νομοθεσία. Όλα αυτά καλύπτονται από ειδικό ασφαλιστικό συμβόλαιο Επαγγελματικής Ευθύνης (Professional Liability/Errors and Omissions insurance), με όριο κάλυψης τα πέντε εκατομμύρια Ευρώ (5.000.000€), περιλαμβάνοντας κάλυψη για (i) απαιτήσεις αποζημίωσης που απορρέουν από πράξη, σφάλμα, ή παράλειψη, μη σκόπιμη συμβατική παραβίαση ή αμέλεια στην έκδοση ή διατήρηση σε ισχύ, σε σχέση με Εγκεκριμένα Πιστοποιητικά, Εγκεκριμένες Υπογραφές/Σφραγίδες, Εγκεκριμένα Πιστοποιητικά για Ταυτοποίηση Ιστοχώρων,

Πιστοποιητικά Εκτεταμένης Επικύρωσης (Extended Validation) για SSL/TLS και Εκτεταμένης Επικύρωσης για υπογραφή κώδικα, και (ii) απαιτήσεις αποζημίωσης που απορρέουν από παραβίαση δικαιωμάτων διανοητικής ιδιοκτησίας οποιουδήποτε τρίτου (εξαιρουμένης της παραβίασης πνευματικών δικαιωμάτων και εμπορικού σήματος), παραβίαση ιδιωτικότητας και ζημία που προκαλείται κατά την διαφήμιση προϊόντων ή υπηρεσιών.

9.9 Αποζημίωση

Ο Συνδρομητής αποζημιώνει τη HARICA και τους Συνεργάτες της και τους αντίστοιχους διευθυντές, προϊσταμένους, υπαλλήλους και αντιπροσώπους (κάθε ένας "Αποζημιωθείς") έναντι όλων των υποχρεώσεων, ζημιών, εξόδων ή δαπανών (συλλογικά "Ζημιές") που βασίζονται, άμεσα ή έμμεσα, σε παραβίαση της παρούσας Σύμβασης, τυχόν πληροφορία, ψευδή δήλωση ή παραβίαση της εγγύησης ή της διαβεβαίωσης που παρέχεται από τον Συνδρομητή ή από παρεμπόδιση ή παραβίαση εκ μέρους του Συνδρομητή ή των πελατών του δικαιωμάτων οποιουδήποτε τρίτου και είναι υπεύθυνος για την υπεράσπιση έναντι όλων των ενεργειών που γίνονται σε βάρος του Αποζημιωθέντος.

Οι υποχρεώσεις αποζημίωσης του Συνδρομητή δεν αποτελούν μοναδικό αποζημιωτικό μέτρο για την HARICA εξαιτίας της παράβασης του Συνδρομητή, αλλά είναι επιπρόσθετες σε οποιαδήποτε άλλα ένδικα βοηθήματα και αποζημιωτικές αξιώσεις μπορεί να εγείρει η HARICA κατά του Συνδρομητή βάσει της παρούσας Σύμβασης. Οι υποχρεώσεις αποζημίωσης του Συνδρομητή διατηρούνται με τη λήξη της Σύμβασης.

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

Η παρούσα ΠΠ/ΔΔΠ ισχύει για όλο το χρονικό διάστημα λειτουργίας της ΥΔΚ HARICA. Σε περίπτωση που Ενδιάμεση Αρχή Πιστοποίησης επιθυμεί να διακόψει τις υπηρεσίες της και παραιτηθεί από τη συνεργασία με την ΥΔΚ HARICA, οφείλει να ενημερώσει εγγράφως την Επιτροπή Διαχείρισης της HARICA. Ανάλογη επικοινωνία επιβάλλεται σε περιπτώσεις εκδήλωσης ενδιαφέροντος από Οργανισμό που επιθυμεί να συμμετέχει στην ΥΔΚ HARICA.

9.10.1 Περίοδος ισχύος και τερματισμός των Συμβάσεων Συνδρομητή

Περίοδος ισχύος. Εκτός εάν ορίζεται διαφορετικά από τα επιτρεπόμενα αυτής της ΠΠ/ΔΔΠ, η Σύμβαση Συνδρομητή ισχύει από την αποδοχή του Συνδρομητή και συνεχίζει να ισχύει για όσο διάστημα ισχύει Πιστοποιητικό που εκδόθηκε βάσει αυτής της Σύμβασης Συνδρομητή.

Τερματισμός. Οποιοδήποτε Μέρος μπορεί να τερματίσει γι' οποιονδήποτε λόγο τη Σύμβαση Συνδρομητή ειδοποιώντας προηγουμένως το άλλο συμβαλλόμενο μέρος με είκοσι (20) εργάσιμες ημέρες προειδοποίηση. Η HARICA μπορεί να τερματίσει τη Σύμβαση Συνδρομητή αμέσως χωρίς ειδοποίηση εάν

(i) Ο Συνδρομητής παραβιάζει ουσιωδώς τη Σύμβαση Συνδρομητή

(ii) Η HARICA ανακαλεί ένα Πιστοποιητικό σύμφωνα με αυτά που ορίζει αυτή η ΠΠ/ΔΔΠ

(iii) Η HARICA απορρίπτει την αίτηση Πιστοποιητικού Συνδρομητή

(iv) Η HARICA δεν μπορεί να επαληθεύσει επαρκώς τον Συνδρομητή σύμφωνα με τις προβλέψεις της παρούσας ΠΠ/ΔΔΠ ή εάν

(v) τα πρότυπα τεχνολογίας ή οι αλλαγές στην ισχύουσα νομοθεσία επηρεάζουν την εγκυρότητα των Πιστοποιητικών που ζήτησε ο Συνδρομητής.

9.11 Ατομικές ειδοποιήσεις και επικοινωνία μεταξύ των μερών

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

9.12 Τροποποιήσεις

Όλες οι αλλαγές στο παρόν ΠΠ/ΔΔΠ και άλλα κανονιστικά έγγραφα, ελέγχονται και πρέπει να εγκρίνονται από την ΕΔΠΠ της HARICA όπως περιγράφεται στην παράγραφο 1.5.1.

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 Διαδικασίες ενημέρωσης και περίοδος ενημέρωσης

Σε περίπτωση ουσιωδών αλλαγών στην ΠΠ/ΔΔΠ, οι Συνδρομητές θα ενημερώνονται εκ των προτέρων για τις ημερομηνίες που θα τεθούν σε ισχύ. Η ΥΔΚ HARICA, οφείλει σε περιπτώσεις ουσιωδών αλλαγών να δημοσιεύει και τις προηγούμενες κύριες εκδόσεις των κειμένων ΠΠ/ΔΔΠ στον ιστοχώρο της υπηρεσίας. Η τρέχουσα ενεργή ΠΠ/ΔΔΠ δημοσιεύεται στη διεύθυνση: https://repo.harica.gr/documents/CPS.
Η ΥΔΚ HARICA

(i) αναθεωρεί τους όρους της Σύμβασης Συνδρομητή και/ή
(ii) αλλάζει μέρος των υπηρεσιών που παρέχονται σε αυτήν οποιαδήποτε στιγμή.

Κάθε τέτοια αλλαγή κοινοποιείται στο Συνδρομητή με οποιοδήποτε πρόσφορο τρόπο και σε κάθε περίπτωση είναι δεσμευτική και ισχύει δεκατέσσερις (14) ημέρες από τη δημοσίευση των αλλαγών στην Σύμβαση Συνδρομητή ή /και στην ΠΠ/ΔΔΠ στην ιστοσελίδα της HARICA https://repo.harica.gr ή κατόπιν ειδοποίησης του Συνδρομητή μέσω ηλεκτρονικού ταχυδρομείου. Εάν ο Συνδρομητής συνεχίσει να χρησιμοποιεί το Πιστοποιητικό του ή υπηρεσίες Χρονοσήμανσης μετά την ημερομηνία αλλαγής των όρων της Σύμβασης Συνδρομητή, η HARICA θα αντιμετωπίζει την κάθε χρήση του Συνδρομητή ως αποδοχή των ενημερωμένων όρων.

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

Οποιαδήποτε αλλαγή αυτής της ΠΠ/ΔΔΠ παράγει ένα νέο αναγνωριστικό (OID) το οποίο αναφέρεται στην παράγραφο 1.2. Οι συνδρομητές θα ενημερωθούν εκ των προτέρων σε περίπτωση σημαντικών αλλαγών στην ΠΠ/ΔΔΠ.

9.13 Διαδικασίες επίλυσης διαφορών

Εάν προκύψει αντιπαράθεση ή διαφορά που σχετίζεται ή προκύπτει από την ερμηνεία της Πολιτικής Πιστοποίησης / Δήλωσης Διαδικασιών Πιστοποίησης και των πράξεων της Αρχής Πιστοποίησης, ο ενδιαφερόμενος Συνδρομητής μπορεί να υπαγάγει την διαφορά αυτή στην Επιτροπή Διαχείρισης Πολιτικής της HARICA και προσπαθεί να επιλύσει ή να διευθετήσει τη διαφορά με φιλικό τρόπο πριν από την έναρξη

οποιασδήποτε δικαστικής διαδικασίας. Η Επιτροπή Διαχείρισης Πολιτικών της HARICA είναι υπεύθυνη να διερευνήσει όλα τα θέματα που αφορούν τις καταγγελίες και τις διαφορές σχετικά με την παροχή υπηρεσιών εμπιστοσύνης. Δείτε επίσης την παράγραφο 3.1.6.

Εάν δεν διευθετηθεί φιλικά, τυχόν διαφορές που σχετίζονται ή προκύπτουν από αυτή την Πολιτική Πιστοποίησης/ Δήλωση Διαδικασιών Πιστοποίησης της Υποδομής Δημόσιου Κλειδιού της HARICA θα παραπεμφθούν και θα υποβληθούν στα αρμόδια ελληνικά δικαστήρια που είναι τα δικαστήρια της Αθήνας.

9.14 Ισχύουσα νομοθεσία

Η ΥΔΚ HARICA δημιουργήθηκε για να υπηρετήσει κυρίως την Ελληνική Ακαδημαϊκή και Ερευνητική κοινότητα. Η λειτουργία της ΥΔΚ HARICA καθώς και η ερμηνεία της Πολιτικής Πιστοποίησης/Δήλωσης Διαδικασιών Πιστοποίησης διέπεται από το ελληνικό δίκαιο.

9.15 Συμμόρφωση με την κείμενη νομοθεσία

Αυτή η Πολιτικής Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης της Υποδομής Δημοσίου Κλειδιού HARICA ερμηνεύεται, εκλαμβάνεται και επιβάλλεται από κάθε άποψη σύμφωνα με την ισχύουσα Ευρωπαϊκή και Ελληνική νομοθεσία. Όλες οι διαδικασίες ή οι νόμιμες ενέργειες που προκύπτουν από την Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης της Υποδομής Δημοσίου Κλειδιού της HARICA πρέπει να εκκινούνται με αποκλειστική δικαιοδοσία τα δικαστήρια της Αθήνας.

9.16 Διάφορες Διατάξεις

9.16.1 Συνολική Συμφωνία

Δεν ορίζεται.

9.16.2 Εκχώρηση

Τα Βασιζόμενα Μέρη και οι Συνδρομητές δεν θα εκχωρήσουν κανένα από τα δικαιώματα, τα συμφέροντα ή τις υποχρεώσεις τους (σύμφωνα με το νόμο ή με άλλο τρόπο) χωρίς την προηγούμενη γραπτή συγκατάθεση της HARICA. Κάθε τέτοια απόπειρα εκχώρησης είναι άκυρη. Με την επιφύλαξη των προαναφερθέντων, η παρούσα ΠΠ/ΔΔΠ είναι δεσμευτική και ενεργεί προς όφελος των συμβαλλομένων, των διαδόχων τους και των επιτρεπόμενων εκδοχέων.

9.16.3 Αυτοτέλεια

Εάν κάποια διάταξη ή διατάξεις αυτής της ΠΠ/ΔΔΠ κηρύσσονται άκυρες, παράνομες ή μη εκτελεστέες για οποιονδήποτε λόγο: (α) η εγκυρότητα, η νομιμότητα και η εκτελεστότητα των υπόλοιπων προβλέψεων αυτής της ΠΠ/ΔΔΠ (συμπεριλαμβανομένων, χωρίς περιορισμό, οποιοδήποτε μέρος, ενότητα ή εδάφιο αυτής της ΠΠ/ΔΔΠ που περιέχει οποιαδήποτε διάταξη που κηρύσσεται άκυρη, παράνομη ή μη εκτελεστή, η οποία δεν είναι η ίδια άκυρη, παράνομη ή μη εκτελεστή) δεν θα επηρεαστεί ούτε και θα καταργηθεί αλλά παραμένει εκτελεστή στο μέγιστο βαθμό που επιτρέπεται από το νόμο, β) η διάταξη ή οι διατάξεις αυτές θεωρούνται ότι έχουν τροποποιηθεί στο βαθμό που απαιτείται για να εναρμονιστούν με την ισχύουσα

νομοθεσία και να προσδώσουν τη μέγιστη δυνατή ισχύ στην παρούσα ΠΠ/ΔΔΠ και (γ) στο μέγιστο δυνατό βαθμό.

Για Πιστοποιητικά χρήσης SSL/TLS, σε περίπτωση σύγκρουσης μεταξύ αυτής της ΠΠ/ΔΔΠ και ενός νόμου, κανονισμού ή κυβερνητικής εντολής (εφεξής "Νόμος") οποιασδήποτε δικαιοδοσίας στην οποία λειτουργεί η HARICA ή εκδίδει πιστοποιητικά, η HARICA μπορεί να τροποποιήσει οποιαδήποτε απαίτηση έρχεται σε αντίθεση με το Νόμο στην ελάχιστη έκταση που είναι απαραίτητη για να καταστεί η απαίτηση αυτή έγκυρη και νόμιμη στην ισχύουσα δικαιοδοσία. Αυτό ισχύει μόνο για πράξεις ή εκδόσεις πιστοποιητικών για χρήση SSL / TLS που υπόκεινται στον εν λόγω νόμο. Στην περίπτωση αυτή, πριν από την έκδοση πιστοποιητικού βάσει της τροποποιημένης απαίτησης, η HARICA ενημερώνει αυτή την ΠΠ/ΔΔΠ και περιλαμβάνει λεπτομερή αναφορά στο νόμο που απαιτεί τροποποίηση αυτής της ΠΠ/ΔΔΠ και την ειδική τροποποίηση αυτής της ΠΠ/ΔΔΠ που εφαρμόζεται από την HARICA.

Η HARICA (πριν από την έκδοση ενός πιστοποιητικού SSL / TLS σύμφωνα με την τροποποιημένη απαίτηση) υποχρεούται να ειδοποιήσει το CA / Browser Forum για τις σχετικές πληροφορίες που προστέθηκαν πρόσφατα σε αυτή τη ΠΠ/ΔΔΠ, ώστε το CA / Browser Forum να εξετάσει ενδεχόμενες αναθεωρήσεις των απαιτήσεων / κατευθυντήριων γραμμών. Οποιεσδήποτε τροποποιήσεις στις πρακτικές της HARICA που ενεργοποιούνται βάσει αυτής της ενότητας πρέπει να διακόπτονται εάν και όταν δεν ισχύει πλέον ο Νόμος ή οι Βασικές Προδιαγραφές του CA / Browser Forum έχουν τροποποιηθεί ώστε να είναι δυνατό να συμμορφώνονται με αυτές και ταυτόχρονα με το Νόμο. Η κατάλληλη αλλαγή στις πρακτικές, η τροποποίηση της ΠΠ/ΔΔΠ της HARICA και μια ειδοποίηση προς CA/Browser Forum, όπως περιγράφεται παραπάνω, πρέπει ΝΑ γίνονται εντός 90 ημερών.

9.16.4 Εκτελεστότητα

Η παράλειψη της HARICA να επιβάλει ή να απαιτήσει την εκτέλεση οποιασδήποτε από τις διατάξεις της παρούσας ΠΠ/ΔΔΠ δεν θεωρείται ότι αποτελεί παραίτηση από αυτή τη διάταξη και δεν επηρεάζει ούτε την ισχύ της παρούσας ΠΠ/ΔΔΠ ή οποιουδήποτε μέρους αυτής ή το δικαίωμα της HARICA στη συνέχεια να εφαρμόσει την ίδια ή κάθε διάταξη αυτής της ΠΠ/ΔΔΠ οποιαδήποτε στιγμή.

9.16.5 Ανωτέρα Βία

Η επέλευση γεγονότος ανωτέρας βίας που συνεπάγεται καθυστέρηση στην εκτέλεση ή εκπλήρωση οποιαδήποτε από τις συγκεκριμένες υποχρεώσεις εκ μέρους της ΥΔΚ HARICA βάσει του παρόντος δεν θα χρησιμοποιηθεί ως δικαίωμα των Βασιζόμενων Μερών ή του Συνδρομητή ή οποιουδήποτε άλλου τρίτου να διεκδικήσουν αποζημίωση έναντι της ΥΔΚ HARICA, ούτε η ΥΔΚ HARICA ευθύνεται για τυχόν αθέτηση ή καθυστέρηση που προκλήθηκε άμεσα ή έμμεσα λόγω Ανωτέρας Βίας. Ως «Ανωτέρα Βία» νοούνται τα έκτακτα γεγονότα ή οι καταστάσεις, στο μέτρο που είναι πέρα από τον εύλογο έλεγχο της ΥΔΚ HARICA. Οι συνθήκες πέραν του εύλογου ελέγχου της ΥΔΚ HARICA περιλαμβάνουν, αλλά δεν περιορίζονται σε φυσικές καταστροφές όπως πυρκαγιά, πλημμύρα, σεισμό, στοιχεία της φύσης ή πράξεις του Θεού, πράξεις πολέμου, τρομοκρατία, ταραχές, αστικές διαταραχές, εξεγέρσεις ή επαναστάσεις στην Ελληνική Δημοκρατία, απεργίες, αποκλεισμοί, δυσχέρειες στην εργασία ή οποιαδήποτε άλλη παρόμοια αιτία πέρα από τον εύλογο έλεγχο της ΥΔΚ HARICA.

9.17 Άλλες Παροχές

Δεν ορίζεται.

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 ===

=== BEGIN HARICA ROOT CA 2015 ===

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 0 (0x0)
    Signature Algorithm: sha256WithRSAEncryption
    Issuer: C=GR, L=Athens, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and
Research Institutions RootCA 2015
    Validity
      Not Before: Jul  7 10:11:21 2015 GMT
      Not After : Jun 30 10:11:21 2040 GMT
    Subject: C=GR, L=Athens, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and
Research Institutions RootCA 2015
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
        Public-Key: (4096 bit)
        Modulus:
          00:c2:f8:a9:3f:1b:89:fc:3c:3c:04:5d:3d:90:36:
          b0:91:3a:79:3c:66:5a:ef:6d:39:01:49:1a:b4:b7:
          cf:7f:4d:23:53:b7:90:00:e3:13:2a:28:a6:31:f1:
          91:00:e3:28:ec:ae:21:41:ce:1f:da:fd:7d:12:5b:
          01:83:0f:b9:b0:5f:99:e1:f2:12:83:80:4d:06:3e:
          df:ac:af:e7:a1:88:6b:31:af:f0:8b:d0:18:33:b8:
          db:45:6a:34:f4:02:80:24:28:0a:02:15:95:5e:76:
          2a:0d:99:3a:14:5b:f6:cb:cb:53:bc:13:4d:01:88:
          37:94:25:1b:42:bc:22:d8:8e:a3:96:5e:3a:d9:32:
          db:3e:e8:f0:10:65:ed:74:e1:2f:a7:7c:af:27:34:
          bb:29:7d:9b:b6:cf:09:c8:e5:d3:0a:fc:88:65:65:
          74:0a:dc:73:1c:5c:cd:40:b1:1c:d4:b6:84:8c:4c:
          50:cf:68:8e:a8:59:ae:c2:27:4e:82:a2:35:dd:14:
          f4:1f:ff:b2:77:d5:87:2f:aa:6e:7d:24:27:e7:c6:
          cb:26:e6:e5:fe:67:07:63:d8:45:0d:dd:3a:59:65:
          39:58:7a:92:99:72:3d:9c:84:5e:88:21:b8:d5:f4:
          2c:fc:d9:70:52:4f:78:b8:bd:3c:2b:8b:95:98:f5:
          b3:d1:68:cf:20:14:7e:4c:5c:5f:e7:8b:e5:f5:35:
          81:19:37:d7:11:08:b7:66:be:d3:4a:ce:83:57:00:
          3a:c3:81:f8:17:cb:92:36:5d:d1:a3:d8:75:1b:e1:
          8b:27:ea:7a:48:41:fd:45:19:06:ad:27:99:4e:c1:
          70:47:dd:b5:9f:81:53:12:e5:b1:8c:48:5d:31:43:
          17:e3:8c:c6:7a:63:96:4b:29:30:4e:84:4e:62:19:
          5e:3c:ce:97:90:a5:7f:01:eb:9d:e0:f8:8b:89:dd:
          25:98:3d:92:b6:7e:ef:d9:f1:51:51:7d:2d:26:c8:
          69:59:61:e0:ac:6a:b8:2a:36:11:04:7a:50:bd:32:
          84:be:2f:dc:72:d5:d7:1d:16:47:e4:47:66:20:3f:
          f4:96:c5:af:8e:01:7a:a5:0f:7a:64:f5:0d:18:87:
          d9:ae:88:d5:fa:84:c1:3a:c0:69:28:2d:f2:0d:68:
          51:aa:e3:a5:77:c6:a4:90:0e:a1:37:8b:31:23:47:
          c1:09:08:eb:6e:f7:78:9b:d7:82:fc:84:20:99:49:
          19:b6:12:46:b1:fb:45:55:16:a9:a3:65:ac:9c:07:
          0f:ea:6b:dc:1f:2e:06:72:ec:86:88:12:e4:2d:db:
          5f:05:2f:e4:f0:03:d3:26:33:e7:80:c2:cd:42:a1:
          17:34:0b
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Basic Constraints: critical
        CA:TRUE
      X509v3 Key Usage: critical
        Certificate Sign, CRL Sign
      X509v3 Subject Key Identifier:
        71:15:67:C8:C8:C9:BD:75:5D:72:D0:38:18:6A:9D:F3:71:24:54:0B
  Signature Algorithm: sha256WithRSAEncryption
    75:bb:6d:54:4b:aa:10:58:46:34:f2:62:d7:16:36:5d:08:5e:
    d5:6c:c8:87:bd:b4:2e:46:f2:31:f8:7c:ea:42:b5:93:16:55:
    dc:a1:0c:12:a0:da:61:7e:0f:58:58:73:64:72:c7:e8:45:8e:
    dc:a9:f2:26:3f:c6:79:8c:b1:53:08:33:81:b0:56:13:be:e6:
    51:5c:d8:9b:0a:4f:4b:9c:56:53:02:e9:4f:f6:0d:60:ea:4d:
    42:55:e8:7c:1b:21:21:d3:1b:3a:cc:77:f2:b8:90:f1:68:c7:
    f9:5a:fe:fa:2d:f4:bf:c9:f5:45:1b:ce:38:10:2a:37:8a:79:
    a3:b4:e3:09:6c:85:86:93:ff:89:96:27:78:81:8f:67:e3:46:
```

74:54:8e:d9:0d:69:e2:4a:f4:4d:74:03:ff:b2:77:ed:95:67:
97:e4:b1:c5:ab:bf:6a:23:e8:d4:94:e2:44:28:62:c4:4b:e2:
f0:d8:e2:29:6b:1a:70:7e:24:61:93:7b:4f:03:32:25:0d:45:
24:2b:96:b4:46:6a:bf:4a:0b:f7:9a:8f:c1:ac:1a:c5:67:f3:
6f:34:d2:fa:73:63:8c:ef:16:b0:a8:a4:46:2a:f8:eb:12:ec:
72:b4:ef:f8:2b:7e:8c:52:c0:8b:84:54:f9:2f:3e:e3:55:a8:
dc:66:b1:d9:e1:5f:d8:b3:8c:59:34:59:a4:ab:4f:6c:bb:1f:
18:db:75:ab:d8:cb:92:cd:94:38:61:0e:07:06:1f:4b:46:10:
f1:15:be:8d:85:5c:3b:4a:2b:81:79:0f:b4:69:9f:49:50:97:
4d:f7:0e:56:5d:c0:95:6a:c2:36:c3:1b:68:c9:f5:2a:dc:47:
9a:be:b2:ce:c5:25:e8:fa:03:b9:da:f9:16:6e:91:84:f5:1c:
28:c8:fc:26:cc:d7:1c:90:56:a7:5f:6f:3a:04:bc:cd:78:89:
0b:8e:0f:2f:a3:aa:4f:a2:1b:12:3d:16:08:40:0f:f1:46:4c:
d7:aa:7b:08:c1:0a:f5:6d:27:de:02:8f:ca:c3:b5:2b:ca:e9:
eb:c8:21:53:38:a5:cc:3b:d8:77:37:30:a2:4f:d9:6f:d1:f2:
40:ad:41:7a:17:c5:d6:4a:35:89:b7:41:d5:7c:86:7f:55:4d:
83:4a:a5:73:20:c0:3a:af:90:f1:9a:24:8e:d9:8e:71:ca:7b:
b8:86:da:b2:8f:99:3e:1d:13:0d:12:11:ee:d4:ab:f0:e9:15:
76:02:e4:e0:df:aa:20:1e:5b:61:85:64:40:a9:90:97:0d:ad:
53:d2:5a:1d:87:6a:00:97:65:62:b4:be:6f:6a:a7:f5:2c:42:
ed:32:ad:b6:21:9e:be:bc

=== END HARICA ROOT CA 2015 ===

=== BEGIN HARICA ECC ROOT CA 2015 ===

Certificate:
Data:
Version: 3 (0x2)
Serial Number: 0 (0x0)
Signature Algorithm: ecdsa-with-SHA256
Issuer: C=GR, L=Athens, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research Institutions ECC RootCA 2015
Validity
Not Before: Jul 7 10:37:12 2015 GMT
Not After : Jun 30 10:37:12 2040 GMT
Subject: C=GR, L=Athens, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic and Research Institutions ECC RootCA 2015
Subject Public Key Info:
Public Key Algorithm: id-ecPublicKey
Public-Key: (384 bit)
pub:
04:92:a0:41:e8:4b:82:84:5c:e2:f8:31:11:99:86:
64:4e:09:25:2f:9d:41:2f:0a:ae:35:4f:74:95:b2:
51:64:6b:8d:6b:e6:3f:70:95:f0:05:44:47:a6:72:
38:50:76:95:02:5a:8e:ae:28:9e:f9:2d:4e:99:ef:
2c:48:6f:4c:25:29:e8:d1:71:5b:df:1d:c1:75:37:
b4:d7:fa:7b:7a:42:9c:6a:0a:56:5a:7c:69:0b:aa:
80:09:24:6c:7e:c1:46
ASN1 OID: secp384r1
X509v3 extensions:
X509v3 Basic Constraints: critical
CA:TRUE
X509v3 Key Usage: critical
Certificate Sign, CRL Sign
X509v3 Subject Key Identifier:
B4:22:0B:82:99:24:01:0E:9C:BB:E4:0E:FD:BF:FB:97:20:93:99:2A
Signature Algorithm: ecdsa-with-SHA256
30:64:02:30:67:ce:16:62:38:a2:ac:62:45:a7:a9:95:24:c0:
1a:27:9c:32:3b:c0:c0:d5:ba:a9:e7:f8:04:43:53:85:ee:52:
21:de:9d:f5:25:83:3e:9e:58:4b:2f:d7:67:13:0e:21:02:30:
05:e1:75:01:de:68:ed:2a:1f:4d:4c:09:08:0d:ec:4b:ad:64:
17:28:e7:75:ce:45:65:72:21:17:cb:22:41:0e:8c:13:98:38:
9a:54:6d:9b:ca:e2:7c:ea:02:58:22:91

=== END HARICA ECC ROOT CA 2015 ===

11 ΠΑΡΑΡΤΗΜΑ Β (Περιγράμματα Κοινών Πιστοποιητικών HARICA)

Φιλικό όνομα	Τα ID πολιτικής	Χρήσεις κλειδιού	Άλλες επεκτάσεις
Πιστοποιητικό Ενδιάμεσης ΑΠ HARICA	**2.5.29.32.0 (anyPolicy)** ή το OID της ΠΠ/ΔΔΠ στην περίπτωση ΑΠ εξωτερικής λειτουργίας	Χρήση Κλειδιού: Ψηφιακή Υπογραφή, **Υπογραφή Πιστοποιητικού, Υπογραφή ΛΑΠ** Βελτιωμένη Χρήση Κλειδιού: **Ανάλογα με το είδος των Πιστοποιητικών που παράγονται**	Καμία
Πιστοποιητικό OCSP	**1.3.6.1.4.1.26513.1.1.7**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή** Βελτιωμένη Χρήση Κλειδιού: **Υπογραφή OCSP**	**OCSP No Check**
S/MIME Μόνο (LCP)	**0.4.0.2042.1.3, 1.3.6.1.4.1.26513.1.1.2.1**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή, Κλειδί Κρυπτογράφησης (Key Encipherment[3])** Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), Προστασία Email**	Καμία
Πιστοποιητικό IV Επαλήθευσης ταυτότητας πελάτη με S/MIME (LCP)	**0.4.0.2042.1.3, 1.3.6.1.4.1.26513.1.1.2.3.3**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή, Κλειδί Κρυπτογράφησης (Key Encipherment[3]**) Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), Προστασία Email**	Καμία

[3] Η τιμή «Κλειδί Κρυπτογράφησης» (“Key Encipherment”) περιλαμβάνεται σε πιστοποιητικά που χρησιμοποιούν αλγόριθμο δημοσίου κλειδιού RSA. Δεν συμπεριλαμβάνεται στα πιστοποιητικά που χρησιμοποιούν κλειδιά ECDSA.

Πιστοποιητικό OV Επαλήθευσης ταυτότητας Πελάτη με S/MIME (LCP)	**0.4.0.2042.1.3, 1.3.6.1.4.1.26513.1.1.2.2.3**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή, Κλειδί Κρυπτογράφησης**[3] Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), Προστασία Email**	Καμία
Πιστοποιητικό IV Επαλήθευσης ταυτότητας Πελάτη με S/MIME (NCP)	**0.4.0.2042.1.1, 1.3.6.1.4.1.26513.1.1.2.3.1**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή, Κλειδί Κρυπτογράφησης**[3] Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), Προστασία Email, MS Document Signing**	Καμία
Πιστοποιητικό OV Επαλήθευσης ταυτότητας Πελάτη με S/MIME (NCP)	**0.4.0.2042.1.1, 1.3.6.1.4.1.26513.1.1.2.2.1**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή, Κλειδί Κρυπτογράφησης**[3] Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), Προστασία Email, MS Document Signing**	Καμία
Πιστοποιητικό IV Επαλήθευσης ταυτότητας Πελάτη (LCP)	**0.4.0.2042.1.3, 1.3.6.1.4.1.26513.1.1.5.1.3**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή** Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication)**	Καμία
Πιστοποιητικό OV Επαλήθευσης ταυτότητας Πελάτη (LCP)	**0.4.0.2042.1.3, 1.3.6.1.4.1.26513.1.1.5.2.3**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή** Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication)**	Καμία

Πιστοποιητικό IV Επαλήθευσης ταυτότητας Πελάτη (NCP)	**0.4.0.2042.1.1, 1.3.6.1.4.1.26513.1.1.5.1.1**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή** Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication)**	Καμία
Πιστοποιητικό OV Επαλήθευσης ταυτότητας Πελάτη (NCP)	**0.4.0.2042.1.1, 1.3.6.1.4.1.26513.1.1.5.2.1**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή** Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication)**	Καμία
Εγκεκριμένο Πιστοποιητικό για Προηγμένες ηλεκτρονικές υπογραφές	**0.4.0.194112.1.0 (QCP-n) 1.3.6.1.4.1.26513.1.1.4.1**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή, Κλειδί Κρυπτογράφησης**[3] (επιτρέπεται όταν συνδυάζεται με S/MIME) Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), MS Document Signing**, **Smartcard Logon,** Προστασία Email (προαιρετικό)	**QcStatements:** id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS, id-etsi-qct-esign, id-etsi-qcs-SemanticsId-Natural(προαιρετικό)
Εγκεκριμένο Πιστοποιητικό για Εγκεκριμένες ηλεκτρονικές υπογραφές	**0.4.0.194112.1.2 (QCP-n-qscd) 1.3.6.1.4.1.26513.1.1.4.2**	Χρήση Κλειδιού: **Non Repudiation, Digital Signature** Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), MS Document Signing**, Προστασία Email (προαιρετικό)	**QcStatements:** id-etsi-qcs-QcCompliance, id-etsi-qcs-QcSSCD, id-etsi-qcs-QcPDS, id-etsi-qct-esign, id-etsi-qcs-SemanticsId-Natural (προαιρετικό) **SmartcardUser** (προαιρετικό)

Εγκεκριμένο Πιστοποιητικό για Προηγμένη ηλεκτρονική σφραγίδα	**0.4.0.194112.1.1 (QCP-l)** **1.3.6.1.4.1.26513.1.1.4.3**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή, Κλειδί Κρυπτογράφησης**[3] (επιτρέπεται όταν συνδυάζεται με S/MIME) Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), MS Document Signing**, Προστασία Email (προαιρετικό)	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS, id-etsi-qct-eseal, id-etsi-qcs-SemanticsId-Legal(προαιρετικό), id-etsi-psd2-qcStatement (προαιρετικό)
Εγκεκριμένο Πιστοποιητικό για Εγκεκριμένη ηλεκτρονική σφραγίδα	**0.4.0.194112.1.3 (QCP-l-qscd)** **1.3.6.1.4.1.26513.1.1.4.4**	Χρήση Κλειδιού: **Non Repudiation, Digital Signature** Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), MS Document Signing**, Προστασία Email (προαιρετικό)	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcSSCD, id-etsi-qcs-QcPDS, id-etsi-qct-eseal, id-etsi-qcs-SemanticsId-Legal(προαιρετικό), id-etsi-psd2-qcStatement (προαιρετικό)
Εγκεκριμένο Πιστοποιητικό για Προηγμένη ηλεκτρονική σφραγίδα PSD2	**0.4.0.194112.1.1 (QCP-l)** **1.3.6.1.4.1.26513.1.1.4.5 (QCP-l-psd2)**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή, Κλειδί Κρυπτογράφησης**[3] (επιτρέπεται όταν συνδυάζεται με S/MIME) Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), MS Document Signing**, Προστασία Email (προαιρετικό)	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS, id-etsi-qct-eseal, id-etsi-qcs-SemanticsId-Legal(προαιρετικό), id-etsi-psd2-qcStatement

Εγκεκριμένο Πιστοποιητικό για Εγκεκριμένη ηλεκτρονική σφραγίδα PSD2	**0.4.0.194112.1.3 (QCP-l-qscd)** **1.3.6.1.4.1.26513.1.1.4.6 (QCP-l-psd2-qscd)**	Χρήση Κλειδιού: **Non Repudiation, Digital Signature** Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), MS Document Signing**, Προστασία Email (προαιρετικό)	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcSSCD, id-etsi-qcs-QcPDS, id-etsi-qct-eseal, id-etsi-qcs-SemanticsId-Legal(προαιρετικό), id-etsi-psd2-qcStatement
Εγκεκριμένο Πιστοποιητικό για Επαλήθευσης ταυτότητας Web	**0.4.0.194112.1.4 (QCP-w),** **2.23.140.1.1,** **1.3.6.1.4.1.26513.1.1.1.5**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή, Κλειδί Κρυπτογράφησης**[3] Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), Έλεγχος ταυτότητας TLS Εξυπηρετητή Web (TLS Web Server Authentication)**	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS, id-etsi-qct-web, id-etsi-qcs-SemanticsId-Legal(προαιρετικό)
Εγκεκριμένο Πιστοποιητικό για Επαλήθευσης ταυτότητας Web PSD2	**0.4.0.19495.3.1 (QCP-w-psd2),** **2.23.140.1.1,** **1.3.6.1.4.1.26513.1.1.1.6**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή, Κλειδί Κρυπτογράφησης**[3] Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), Έλεγχος ταυτότητας TLS Εξυπηρετητή Web (TLS Web Server Authentication)**	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS, id-etsi-qct-web, id-etsi-qcs-SemanticsId-Legal(προαιρετικό), id-etsi-psd2-qcStatement
Χρονοσήμανση	**0.4.0.2023.1.1(BTSP),** **1.3.6.1.4.1.26513.1.1.6.1**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή** Βελτιωμένη Χρήση Κλειδιού: **Χρονοσήμανση**	Καμία

Εγκεκριμένη Χρονοσήμανση	**0.4.0.2023.1.1(BTSP), 1.3.6.1.4.1.26513.1.1.6.2**	Χρήση Κλειδιού: **Non Repudiation, Digital Signature** Βελτιωμένη Χρήση Κλειδιού: **Χρονοσήμανση**	**QcStatements**: id-etsi-qcs-QcCompliance, id-etsi-qcs-QcPDS
Υπογραφή Κώδικα IV	**0.4.0.2042.1.1 (NCP), 2.23.140.1.4.1, 1.3.6.1.4.1.26513.1.3.2.1**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή** Βελτιωμένη Χρήση Κλειδιού: **Υπογραφή Κώδικα**, Lifetime Signing (προαιρετικό)	Καμία
Υπογραφή Κώδικα OV	**0.4.0.2042.1.1 (NCP), 2.23.140.1.4.1, 1.3.6.1.4.1.26513.1.3.1.1**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή** Βελτιωμένη Χρήση Κλειδιού: **Υπογραφή Κώδικα**, Lifetime Signing (προαιρετικό)	Καμία
Πιστοποιητικό Υπογραφής Κώδικα IV σε ασφαλή Διάταξη Δημιουργίας Υπογραφής	**0.4.0.2042.1.2 (NCP+), 2.23.140.1.4.1, 1.3.6.1.4.1.26513.1.3.2.2**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή** Βελτιωμένη Χρήση Κλειδιού: **Υπογραφή Κώδικα**, Lifetime Signing (προαιρετικό)	Καμία
Πιστοποιητικό Υπογραφής Κώδικα OV σε ασφαλή Διάταξη Δημιουργίας Υπογραφής	**0.4.0.2042.1.2 (NCP+), 2.23.140.1.4.1, 1.3.6.1.4.1.26513.1.3.1.2**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή** Βελτιωμένη Χρήση Κλειδιού: **Υπογραφή Κώδικα**, Lifetime Signing (προαιρετικό)	Καμία
Πιστοποιητικό Υπογραφής Κώδικα EV	**0.4.0.2042.1.2 (NCP+), 2.23.140.1.3, 1.3.6.1.4.1.26513.1.3.3**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή** Βελτιωμένη Χρήση Κλειδιού: **Υπογραφή Κώδικα**, Lifetime Signing (προαιρετικό)	Καμία

Πιστοποιητικό DV SSL/TLS	**0.4.0.2042.1.6 (DVCP), 2.23.140.1.2.1, 1.3.6.1.4.1.26513.1.1.1.1**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή, Κλειδί Κρυπτογράφησης**[3] Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), Έλεγχος ταυτότητας TLS Εξυπηρετητή Web (TLS Web Server Authentication)**	Καμία
Πιστοποιητικό OV SSL/TLS	**0.4.0.2042.1.7 (OVCP), 2.23.140.1.2.2, 1.3.6.1.4.1.26513.1.1.1.2**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή, Κλειδί Κρυπτογράφησης**[3] Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), Έλεγχος ταυτότητας TLS Εξυπηρετητή Web (TLS Web Server Authentication)**	Καμία
Πιστοποιητικό IV SSL/TLS	**0.4.0.2042.1.8 (IVCP), 2.23.140.1.2.3, 1.3.6.1.4.1.26513.1.1.1.3**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή, Κλειδί Κρυπτογράφησης**[3] Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), Έλεγχος ταυτότητας TLS Εξυπηρετητή Web (TLS Web Server Authentication)**	Καμία
Πιστοποιητικό EV SSL/TLS	**0.4.0.2042.1.4 (EVCP), 2.23.140.1.1, 1.3.6.1.4.1.26513.1.1.1.4**	Χρήση Κλειδιού: **Ψηφιακή Υπογραφή, Κλειδί Κρυπτογράφησης**[3] Βελτιωμένη Χρήση Κλειδιού: **Έλεγχος ταυτότητας TLS πελάτη Web (TLS Web Client Authentication), Έλεγχος ταυτότητας TLS Εξυπηρετητή Web (TLS Web Server Authentication)**	Καμία

12 ΠΑΡΑΡΤΗΜΑ Γ (ΙΕΡΑΡΧΙΑ ΤΗΣ HARICA)

HARICA "Unconstrained" και "Technically Constrained" Subordinate CAs, σύμφωνα με την ενότητα 7.1.5.

12.1 Unconstrained Subordinate CAs

- Hellenic Academic and Research Institutions ECC RootCA 2015
  - HARICA EV TLS ECC SubCA R1
  - HARICA QWAC ECC SubCA R1
  - HARICA SSL ECC SubCA R2

- Hellenic Academic and Research Institutions RootCA 2011
  - HARICA SSL Intermediate CA R1

- Hellenic Academic and Research Institutions RootCA 2015
  - HARICA EV TLS RSA SubCA R1
  - HARICA QWAC RSA SubCA R1
  - HARICA SSL RSA SubCA R3

12.2 Technically Constrained Subordinate CAs

- Hellenic Academic and Research Institutions ECC RootCA 2015
  1. HARICA Administration Client ECC SubCA R2
  2. HARICA Administration SSL ECC SubCA R2
  3. HARICA Client Authentication ECC SubCA R2
  4. HARICA Code Signing ECC SubCA R2
  5. HARICA EV Code Signing ECC SubCA R1
  6. HARICA Qualified Legal Entities ECC SubCA R2
  7. HARICA Qualified Natural Entities ECC SubCA R2
  8. HARICA S/MIME ECC SubCA R2

- Hellenic Academic and Research Institutions RootCA 2011
  1. Academy of Athens Client CA R1
  2. Aristotle University of Thessaloniki Central CA R5
  3. Athens University of Economics and Business CA R2
  4. CEDEFOP CA R1
  5. Democritus University of Thrace CA R1
  6. Eastern Macedonia and Thrace Institute of Technology CA R1
  7. Greek Academic Network CA R2
  8. Greek School Network CA R2
  9. HARICA Client Authentication RSA SubCA R1
  10. HARICA Qualified Legal Entities SubCA R1
  11. HARICA Qualified Natural Entities SubCA R1
  12. HARICA S_MIME RSA SubCA R1
  13. Harokopio University CA R1
  14. HEAL-LINK Hellenic Academic Libraries Link CA R2

15. Hellenic Academic and Research Institutions AdminCA R6
16. Institute of Accelerating Systems and Applications Client CA R1
17. Institute of Accelerating Systems and Applications SSL CA R1
18. International Hellenic University CA R1
19. Ionian University Client CA R1
20. Ionian University SSL CA R1
21. National and Kapodistrian University of Athens CA R2
22. Panteion University of Social and Political Sciences CA R1
23. Piraeus University of Applied Sciences CA R1
24. Technical University of Crete CA R1
25. Technological Educational Institute of Epirus CA R3
26. Technological Educational Institute of Western Greece CA R1
27. Technological Educational Institution of Central Macedonia CA R3
28. Technological Educational Institution of Thessaloniki CA R3
29. Technological Educational Institution of Thessaly CA R2
30. University of Crete CA R3
31. University of Ioannina CA R2
32. University of Macedonia CA R1
33. University of Patras CA R1
34. University of Piraeus CA R1
35. University of the Peloponnese CA R2
36. University of Western Macedonia CA R3

- Hellenic Academic and Research Institutions RootCA 2015
    1. ACER Client RSA SubCA R2
    2. Academy of Athens SSL SubCA R2
    3. Aristotle University of Thessaloniki SSL RSA SubCA R2
    4. Athens University of Economics and Business TLS RSA SubCA R1
    5. CEDEFOP TLS RSA SubCA R1
    6. Democritus University of Thrace TLS RSA SubCA R1
    7. Ecclesiastical Academy of Vella SSL RSA SubCA R2
    8. GRNET TLS RSA SubCA R1
    9. GRnet SSL RSA SubCA R2
    10. Greek Federation of Judicial Officers Client RSA SubCA R4
    11. Greek School Network TLS RSA SubCA R1
    12. Greek Universities Network TLS RSA SubCA R1
    13. HARICA Client Authentication RSA SubCA R2
    14. HARICA EV Code Signing RSA SubCA R1
    15. HARICA Institutional Client SubCA R1
    16. HARICA Qualified Legal Entities SubCA R2
    17. HARICA Qualified Legal Entities SubCA R3
    18. HARICA Qualified Natural Entities SubCA R2
    19. HARICA Qualified Natural Entities SubCA R3
    20. HARICA S_MIME RSA SubCA R2
    21. HARICA S_MIME RSA SubCA R3
    22. HEAL-LINK Hellenic Academic Libraries Link TLS RSA SubCA R1
    23. Harokopio University TLS RSA SubCA R1
    24. Hellenic Academic and Research Institutions AdminCA R5
    25. Hellenic Academic and Research Institutions Code Signing CA R1

26. Inst. of Accelerating Systems and Applications TLS RSA SubCA R1
27. International Hellenic University TLS RSA SubCA R1
28. Ionian University TLS RSA SubCA R1
29. Ministry of Digital Governance (Hellenic Republic) SubCA R1
30. National Technical University of Athens TLS RSA SubCA R1
31. National and Kapodistrian University of Athens TLS RSA SubCA R1
32. Panteion Univ. of Social and Political Sciences TLS RSA SubCA R1
33. Technical University of Crete TLS RSA SubCA R1
34. University of Crete TLS RSA SubCA R1
35. University of Ioannina TLS RSA SubCA R1
36. University of Macedonia TLS RSA SubCA R1
37. University of Patras TLS RSA SubCA R1
38. University of Piraeus TLS RSA SubCA R1
39. University of West Attica TLS RSA SubCA R1
40. University of Western Macedonia TLS RSA SubCA R1
41. University of the Aegean TLS RSA SubCA R1
42. University of the Peloponnese TLS RSA SubCA R1

12.3 Internally-operated Subordinate CAs with Keys Destroyed and externally audited

- Hellenic Academic and Research Institutions ECC RootCA 2015
  1. HARICA Administration Client ECC SubCA R1
  2. HARICA Administration Client ECC SubCA R2

- Hellenic Academic and Research Institutions RootCA 2011
  1. Ecclesiastical Academy of Vella Client RSA SubCA R1
  2. Ecclesiastical Academy of Vella SSL RSA SubCA R1

- Hellenic Academic and Research Institutions RootCA 2015
  1. Academy of Athens Client SubCA R2
  2. Academy of Athens Client RSA SubCA R3
  3. University of the Aegean Client RSA SubCA R1
  4. Athens University of Economics and Business Client RSA SubCA R1
  5. Aristotle University of Thessaloniki Client RSA SubCA R1
  6. Aristotle University of Thessaloniki Client RSA SubCA R2
  7. Aristotle University of Thessaloniki Client RSA SubCA R3
  8. CEDEFOP Client RSA SubCA R1
  9. Democritus University of Thrace Client RSA SubCA R1
  10. Ecclesiastical Academy of Vella Client RSA SubCA R2
  11. Ecclesiastical Academy of Vella of Ioannina Client RSA SubCA R3
  12. GRnet Client RSA SubCA R1
  13. GRnet Client RSA SubCA R2
  14. GRNET Client RSA SubCA R3
  15. GRNET Client RSA SubCA R4
  16. Greek Universities Network Client RSA SubCA R1
  17. HEAL-LINK Hellenic Academic Libraries Link Client RSA SubCA R1
  18. Harokopio University Client RSA SubCA R1

19. Inst. of Accelerating Sys and Applications Client RSA SubCA R2
20. International Hellenic University Client RSA SubCA R1
21. Ionian University Client RSA SubCA R2
22. National Technical University of Athens Client RSA SubCA R1
23. Greek Federation of Judicial Officers Client SubCA R1
24. Greek Federation of Judicial Officers Client SubCA R2
25. Greek Federation of Judicial Officers Client RSA SubCA R3
26. Panteion Univ. of Social and Political Sciences Client SubCA R1
27. Greek School Network Client RSA SubCA R1
28. Technical University of Crete Client RSA SubCA R1
29. University of Piraeus Client RSA SubCA R1
30. University of West Attica Client RSA SubCA R1
31. National and Kapodistrian Univ. of Athens Client RSA SubCA R1
32. University of Crete Client RSA SubCA R1
33. University of Ioannina Client RSA SubCA R1
34. University of Macedonia Client RSA SubCA R1
35. University of the Peloponnese Client RSA SubCA R1
36. University of Western Macedonia Client RSA SubCA R1
37. University of Patras Client RSA SubCA R1

13 ΠΑΡΑΡΤΗΜΑ Δ “CAA Contact Tag”

Οι παρακάτω μέθοδοι επιτρέπουν στους κατόχους Χώρων Ονομάτων να δημοσιεύουν στοιχεία επικοινωνίας στο DNS για τους σκοπούς επαλήθευσης ελέγχου Χώρου Ονομάτων.

13.1 Μέθοδοι CAA

13.1.1 Ιδιότητα CAA contactemail

ΣΥΝΤΑΞΗ: contactemail <rfc6532emailaddress>

Η ιδιότητα CAA contactemail δέχεται ως παράμετρο μια διεύθυνση email. Ολόκληρη η τιμή της παραμέτρου ΠΡΕΠΕΙ να είναι μια έγκυρη διεύθυνση ηλεκτρονικού ταχυδρομείου όπως ορίζεται στην ενότητα 3.2 του RFC 6532, χωρίς επιπλέον προσθήκες ή δομικά στοιχεία, διαφορετικά δεν μπορεί να χρησιμοποιηθεί.

Ακολουθεί ένα παράδειγμα όπου ο κάτοχος του Ονόματος Χώρου όρισε στοιχεία επικοινωνίας χρησιμοποιώντας μία διεύθυνση email.

```
$ORIGIN example.com.

      CAA 0 contactemail "domainowner@example.com"
```

Η ιδιότητα contactemail ΜΠΟΡΕΙ να είναι κρίσιμη, αν ο κάτοχος του Ονόματος Χώρου δεν θέλει να εκδίδονται Πιστοποιητικά για αυτό το Όνομα Χώρου από Αρχές Πιστοποίησης που δεν γνωρίζουν πώς να ερμηνεύσουν το συγκεκριμένο πεδίο.

13.1.2 Ιδιότητα CAA contactphone

ΣΥΝΤΑΞΗ: contactphone <rfc3966 Global Number>

Η ιδιότητα CAA contactphone δέχεται ως παράμετρο ένα τηλεφωνικό αριθμό. Ολόκληρη η τιμή της παραμέτρου ΠΡΕΠΕΙ να είναι ένα έγκυρο “Global Number” όπως ορίζεται στην ενότητα 5.1.4 του RFC 3966, διαφορετικά δεν μπορεί να χρησιμοποιηθεί. Τα “Global Numbers” ΠΡΕΠΕΙ να ξεκινούν με το σύμβολο + και τον κωδικό χώρας και ενδέχεται να περιέχουν χαρακτήρες για οπτικό διαχωρισμό.

Ακολουθεί ένα παράδειγμα όπου ο κάτοχος του Ονόματος Χώρου όρισε στοιχεία επικοινωνίας χρησιμοποιώντας έναν αριθμό τηλεφώνου.

```
$ORIGIN example.com.

      CAA 0 contactphone "+1 (555) 123-4567"
```

Η ιδιότητα contactphone ΜΠΟΡΕΙ να είναι κρίσιμη, αν ο κάτοχος του Ονόματος Χώρου δεν θέλει να εκδίδονται Πιστοποιητικά για αυτό το Όνομα Χώρου από Αρχές Πιστοποίησης που δεν γνωρίζουν πώς να ερμηνεύσουν το συγκεκριμένο πεδίο.

13.2 Μέθοδος DNS TXT

13.2.1 Email Επαφής Εγγραφής DNS TXT

Η εγγραφή DNS TXT ΠΡΕΠΕΙ να εισαχθεί στο subdomain `"_validation-contactemail"` του Ονόματος Χώρου του οποίου ελέγχεται η εγκυρότητα. Η πλήρης τιμή RDATA για τη συγκεκριμένη εγγραφή TXT ΠΡΕΠΕΙ να είναι μια έγκυρη διεύθυνση ηλεκτρονικού ταχυδρομείου όπως ορίζεται στην ενότητα 3.2 του RFC 6532, χωρίς επιπλέον προσθήκες ή δομικά στοιχεία, διαφορετικά δεν μπορεί να χρησιμοποιηθεί.

13.2.2 Τηλέφωνο Επαφής Εγγραφής DNS TXT

Η εγγραφή DNS TXT ΠΡΕΠΕΙ να εισαχθεί στο subdomain `"_validation-contactemail"` του Ονόματος Χώρου του οποίου ελέγχεται η εγκυρότητα. Η πλήρης τιμή RDATA για τη συγκεκριμένη εγγραφή TXT ΠΡΕΠΕΙ να είναι ένας έγκυρος Παγκόσμιος Αριθμός τηλεφώνου όπως ορίζεται στην ενότητα 5.1.4 του RFC 6532, διαφορετικά δεν μπορεί να χρησιμοποιηθεί.

14 ΠΑΡΑΡΤΗΜΑ Ε ΕΚΔΟΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΓΙΑ .ONION DOMAIN NAMES

Το παράρτημα αυτό ορίζει αποδεκτές διαδικασίες επαλήθευσης για να είναι εφικτή η εισαγωγή ενός ή περισσοτέρων ειδικής χρήσης ".onion" Domain Names, όπως περιγράφονται στο RFC 7686.

1. Το Domain Name ΠΡΕΠΕΙ να περιέχει τουλάχιστον δύο ονόματα/ετικέτες (labels) όπου το πιο δεξί όνομα έχει την τιμή "onion", και το όνομα/ετικέτα αμέσως προηγουμένως είναι ένα έγκυρο Version 3 Onion Address, όπως ορίζεται στην ενότητα 6 του Tor Rendezvous Specification - Version 3 που βρίσκεται στη διεύθυνση https://spec.torproject.org/rend-spec-v3.
2. Η HARICA ΠΡΕΠΕΙ να ελέγξει ότι ο Αιτούμενος ελέγχει το .onion Domain Name χρησιμοποιώντας τουλάχιστον μια από τις μεθόδους που ακολουθούν:
    a. χρησιμοποιώντας την μέθοδο ελέγχου Domain 3.2.2.4.6 ή 3.2.2.4.18.
    b. ζητώντας τον Αιτούμενο να αποστείλει ένα Αίτημα Πιστοποιητικού που θα είναι υπογεγραμμένο με το κλειδί που αντιστοιχεί στο .onion δημόσιο κλειδί, αν το τμήμα Attributes του certificationRequestInfo περιέχει:
        i. Ένα attribute caSigningNonce που περιέχει μια Τυχαία Τιμή που έχει δημιουργήσει η HARICA και
        ii. Ένα attribute applicantSigningNonce που περιέχει μια μοναδική τιμή με τουλάχιστον 64 bits εντροπίας που έχει δημιουργήσει ο Αιτούμενος.

Τα signing nonce attributes έχουν την ακόλουθη δομή:

```
caSigningNonce ATTRIBUTE ::= {

| WITH SYNTAX | OCTET STRING |
| --- | --- |
| EQUALITY MATCHING RULE | octetStringMatch |
| SINGLE VALUE | TRUE |
| ID | { cabf-caSigningNonce } |

}

cabf-caSigningNonce OBJECT IDENTIFIER ::= { cabf 41 }

applicantSigningNonce ATTRIBUTE ::= {

| WITH SYNTAX | OCTET STRING |
| --- | --- |
| EQUALITY MATCHING RULE | octetStringMatch |
| SINGLE VALUE | TRUE |
| ID | { cabf-applicantSigningNonce } |

}

cabf-applicantSigningNonce OBJECT IDENTIFIER ::= { cabf 42 }
```

Η Τυχαία Τιμή παραμένει έγκυρη για χρήση σε μια επιβεβαιωτική απάντηση έως τριάντα (30) ημέρες από τη δημιουργία της.

Η HARICA μπορεί να εισάγει έναν χαρακτήρα μπαλαντέρ στην επέκταση Subject Alternative Name και στο πεδίο Subject Common Name ως τον πιο αριστερό χαρακτήρα στο .onion Domain Name, εφόσον επιτρέπεται σύμφωνα με την ενότητα 3.2.2.6.

3. Όταν το Πιστοποιητικό περιλαμβάνει ένα FQDN όπου η τιμή "onion" είναι το πιο δεξί μέρος του Domain Name, το the Domain Name αυτό δεν θα θεωρείται ως «Εσωτερικό Όνομα» (Internal Name), εφόσον το Πιστοποιητικό εκδόθηκε σε συμφωνία με τα οριζόμενα σε αυτό το Παράρτημα.

15 ΠΑΡΑΡΤΗΜΑ ΣΤ ΑΝΑΓΝΩΡΙΣΤΙΚΑ ΠΟΛΙΤΙΚΩΝ HARICA

Στην HARICA έχει ανατεθεί ένας προσωπικός εταιρικός αριθμός από τον Οργανισμό IANA με ID **26513** http://oidref.com/1.3.6.1.4.1.26513.

{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) 26513(26513)}

Ακολουθεί η πλήρης λίστας των OIDs Πολιτικής της HARICA για κάθε τύπο πιστοποιητικού, όπου συμπεριλαμβάνεται η συμβατότητα με άλλες εσωτερικές αναγνωρισμένες πολιτικές OIDs διαφόρων προτύπων.

OID						**Περιγραφή**
1.3.6.1.4.1.26513	**1**	**0**				
						Παροχή Υπηρεσιών Πιστοποίησης
						Κεντρική Πολιτική Πιστοποίησης / Δήλωση Διαδικασιών Πιστοποίησης
			3			Πρώτο ψηφίο του αριθμού έκδοσης της Κεντρικής Πολιτικής Πιστοποίησης / Δήλωσης Διαδικασιών Πιστοποίησης
				8		Δεύτερο ψηφίο του αριθμού έκδοσης της Κεντρικής Πολιτικής Πιστοποίησης / Δήλωσης Διαδικασιών Πιστοποίησης
		1				**Πολιτική Πιστοποίησης / Δήλωση Διαδικασιών Πιστοποίησης για συγκεκριμένο είδος πιστοποιητικού**
			1	**Έλεγχος Ταυτότητας εξυπηρετητή**		
				1		Έλεγχος εγκυρότητας Domain (DV) συμβατός με: - CA/B Forum OID 2.23.140.1.2.1 - ETSI EN 319 411-1 OID 0.4.0.2042.1.6
				2		Έλεγχος εγκυρότητας Οργανισμού (OV) συμβατός με : - CA/B Forum OID 2.23.140.1.2.2 - ETSI EN 319 411-1 OID 0.4.0.2042.1.7

				3		Έλεγχος εγκυρότητας Φυσικού προσώπου (IV) συμβατός με: - CA/B Forum OID 2.23.140.1.2.3 - ETSI EN 319 411-1 OID 0.4.0.2042.1.8
				4		Εκτεταμένος Έλεγχος εγκυρότητας (EV) συμβατός με: - CA/B Forum OID 2.23.140.1.1 - ETSI EN 319 411-1 OID 0.4.0.2042.1.4
				5		Εγκεκριμένος Έλεγχος ταυτότητας Ιστοχώρου (QCP-w) συμβατός με: - CA/B Forum OID 2.23.140.1.1 - ETSI EN 319 411-2 OID 0.4.0.194112.1.4
				6		Εγκεκριμένος Έλεγχος ταυτότητας Ιστοχώρου για PSD2 (QCP-w-psd2) συμβατός με: - ETSI TS 119 495 OID 0.4.0.19495.3.1
			2	**Υπογραφή Email**		
				1		Απλός Έλεγχος εγκυρότητας Email (LCP) συμβατός με: - ETSI EN 319 411-1 OID 0.4.0.2042.1.3
				2		Έλεγχος εγκυρότητας Οργανισμού (OV)
					1	Έλεγχος εγκυρότητας Οργανισμού (OV-NCP) συμβατός με: - ETSI EN 319 411-1 OID 0.4.0.2042.1.1
					2	Έλεγχος εγκυρότητας Οργανισμού (OV-NCP+) συμβατός με: - ETSI EN 319 411-1 0.4.0.2042.1.2
					3	Έλεγχος εγκυρότητας Οργανισμού (OV-LCP) συμβατός με: - ETSI EN 319 411-1 OID 0.4.0.2042.1.3
				3		Έλεγχος εγκυρότητας Φυσικού προσώπου (IV)
					1	Έλεγχος εγκυρότητας Φυσικού προσώπου (IV-NCP) συμβατός με: - ETSI EN 319 411-1 OID 0.4.0.2042.1.1
					2	Έλεγχος εγκυρότητας Φυσικού προσώπου (IV-NCP+) συμβατός με: - ETSI EN 319 411-1 0.4.0.2042.1.2
					3	Έλεγχος εγκυρότητας Φυσικού προσώπου (IV-LCP) συμβατός με: - ETSI EN 319 411-1 OID 0.4.0.2042.1.3
			3	**Υπογραφή Κώδικα**		
				1		Έλεγχος εγκυρότητας Οργανισμού (OV)
					1	Έλεγχος εγκυρότητας Οργανισμού (OV-NCP) συμβατός με: - Απαιτήσεις CA/B Forum OID 2.23.140.1.4.1 - ETSI EN 319 411-1 OID 0.4.0.2042.1.1
					2	Έλεγχος εγκυρότητας Οργανισμού (OV-NCP+) συμβατός με: - Απαιτήσεις CA/B Forum OID 2.23.140.1.4.1 - ETSI EN 319 411-1 OID 0.4.0.2042.1.2

				2		Έλεγχος εγκυρότητας Φυσικού προσώπου (IV)
					1	Έλεγχος εγκυρότητας Φυσικού προσώπου (IV-NCP) συμβατός με: - Απαιτήσεις CA/B Forum OID 2.23.140.1.4.1 - ETSI EN 319 411-1 OID 0.4.0.2042.1.1
					2	Έλεγχος εγκυρότητας Φυσικού προσώπου (IV-NCP+) συμβατός με: - Απαιτήσεις CA/B Forum OID 2.23.140.1.4.1 - ETSI EN 319 411-1 OID 0.4.0.2042.1.2
				3		Εκτεταμένος Έλεγχος εγκυρότητας (EV) συμβατός με: - Απαιτήσεις CA/B Forum Υπογραφής Κώδικα EV OID 2.23.140.1.3 - ETSI EN 319 411-1 OID 0.4.0.2042.1.2
			4	**Υπογραφή εγγράφου**		
				1		Εγκεκριμένα Πιστοποιητικά για Προηγμένες Ηλεκτρονικές Υπογραφές (QCP-n) συμβατό με: - ETSI EN 319 411-2 OID 0.4.0.194112.1.0 - Regulation (EU) 910/2014
				2		Εγκεκριμένα Πιστοποιητικά για Εγκεκριμένες Ηλεκτρονικές Υπογραφές (QCP-n-qscd) συμβατό με: - ETSI EN 319 411-2 OID 0.4.0.194112.1.2 - Regulation (EU) 910/2014
				3		Εγκεκριμένα Πιστοποιητικά για Προηγμένες Ηλεκτρονικές Σφραγίδες (QCP-l) συμβατό με: - ETSI EN 319 411-2 OID 0.4.0.194112.1.1 - Regulation (EU) 910/2014
				4		Εγκεκριμένα Πιστοποιητικά για Εγκεκριμένες Ηλεκτρονικές Σφραγίδες (QCP-l-qscd) συμβατό με: - ETSI EN 319 411-2 OID 0.4.0.194112.1.3 - Regulation (EU) 910/2014
				5		Εγκεκριμένα Πιστοποιητικά για Προηγμένες Ηλεκτρονικές Σφραγίδες PSD2 (QCP-l-psd2) συμβατό με: - ETSI EN 319 411-2 OID 0.4.0.194112.1.1 - Regulation (EU) 910/2014 - Directive (EU) 2015/2366
				6		Εγκεκριμένα Πιστοποιητικά για Εγκεκριμένες Ηλεκτρονικές Σφραγίδες PSD2 (QCP-l-psd2-qscd) συμβατό με: - ETSI EN 319 411-2 OID 0.4.0.194112.1.3 - Regulation (EU) 910/2014 - Directive (EU) 2015/2366
			5	**Έλεγχος ταυτότητας Πελάτη**		
				1		Έλεγχος εγκυρότητας Φυσικού προσώπου (IV)
					1	Έλεγχος εγκυρότητας Φυσικού προσώπου (IV-NCP) συμβατός με: - ETSI EN 319 411-1 OID 0.4.0.2042.1.1

					2	Έλεγχος εγκυρότητας Φυσικού προσώπου (IV-NCP+) συμβατός με: - ETSI EN 319 411-1 0.4.0.2042.1.2
					3	Έλεγχος εγκυρότητας Φυσικού προσώπου (IV-LCP) συμβατός με: - ETSI EN 319 411-1 OID 0.4.0.2042.1.3
				2		Έλεγχος εγκυρότητας Οργανισμού (OV)
					1	Έλεγχος εγκυρότητας Οργανισμού (OV-NCP) συμβατός με: - ETSI EN 319 411-1 OID 0.4.0.2042.1.1
					2	Έλεγχος εγκυρότητας Οργανισμού (OV-NCP+) συμβατός με: - ETSI EN 319 411-1 OID 0.4.0.2042.1.2
					3	Έλεγχος εγκυρότητας Οργανισμού (OV-LCP) συμβατός με: - ETSI EN 319 411-1 OID 0.4.0.2042.1.3
			6	**Χρονοσήμανση**		
				1		Απλή Χρονοσήμανση (BTST) συμβατή με: - ETSI EN 319 421 OID 0.4.0.2023.1.1
				2		Εγκεκριμένη Χρονοσήμανση (QTST) συμβατή με: - ETSI EN 319 421 OID 0.4.0.2023.1.1 - Regulation (EU) 910/2014
			7	**Πιστοποιητικό OCSP**		
			8	**Εξ αποστάσεως ΕΔΔΥ**		