Ακαδημαϊκό Διαδίκτυο
(GUnet)

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

Hellenic Academic and Research Institutions Certification Authority (HARICA)

Περίληψη Δήλωσης Διαδικασιών Πιστοποίησης και Πολιτικής Πιστοποίησης της Αρχής Πιστοποίησης των Ελληνικών Ακαδημαϊκών και Ερευνητικών Ιδρυμάτων

Έκδοση 1.7 (17 Οκτωβρίου 2022)

# Πίνακας περιεχομένων

## Έλεγχος Εκδόσεων

| Version | Date | Comment |
|---|---|---|
| 1.0 | Μάιος 2017 | • Αρχικό PDS σε συμμόρφωση με τα πρότυπα ETSI EN 319 411-1, ETSI EN 319 411-2, ETSI EN 319 421 |
| 1.1 | Φεβρουάριος 2018 | • Ενημέρωση που περιλαμβάνει προσθήκη για τις υποχρεώσεις του Αιτούντα σχετικά με πνευματικά δικαιώματα |
| 1.2 | Οκτώβριος 2018 | • Ενημέρωση για θέματα Προσωπικών Δεδομένων. Προστέθηκαν σχετικές ενότητες από την ΠΠ/ΔΔΠ |
| 1.3 | Μάρτιος 2019 | • Προσαρμογή στη ΠΠ/ΔΔΠ 3.8 |
| 1.4 | Οκτώβριος 2019 | • Προσαρμογή στη ΠΠ/ΔΔΠ 3.9 |
| 1.5 | Μάρτιος 2020 | • Προσαρμογή στη ΠΠ/ΔΔΠ 4.0 |
| 1.6 | Φεβρουάριος 2021 | • Προσαρμογή στη ΠΠ/ΔΔΠ 4.3 |
| 1.7 | Οκτώβριος 2022 | • Προσαρμογή στη ΠΠ/ΔΔΠ 4.6 |

# 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**, αριθμό Γενικού Εμπορικού Μητρώου **160729401000** 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 HARICA γίνεται από το Κέντρο Ηλεκτρονικής Διακυβέρνησης του Αριστοτελείου Πανεπιστήμιου Θεσσαλονίκης. Οι φορείς που συμμετέχουν σε αυτή την Υποδομή Δημοσίου Κλειδιού, αποδέχονται ανεπιφύλακτα την παρούσα Δήλωση Διαδικασιών Πιστοποίησης/Πολιτική Πιστοποίησης και συνυπογράφουν το Μνημόνιο Συνεργασίας.

Το παρόν έγγραφο αποτελεί μία Περίληψη της Δήλωσης Διαδικασιών Πιστοποίησης και Πολιτικής Πιστοποίησης της HARICA και ακολουθεί τη δομή του προτύπου ETSI EN 319 411-1 (Παράρτημα Α). Είναι ένα συμπληρωματικό μέσο γνωστοποίησης και ενημέρωσης των Συνδρομητών και Βασιζόμενων Μερών από τη HARICA και δεν αντικαθιστά ή υποκαθιστά την τελευταία έκδοση της Πολιτικής Πιστοποίησης και Δήλωσης Διαδικασιών Πιστοποίησης (ΠΠ / ΔΔΠ) της HARICA, που δημοσιεύεται στη διεύθυνση https://repo.harica.gr/documents/CPS.

# 2 Ορισμοί και ακρωνύμια

Οι ορισμοί που βρίσκονται στο "Network and Certificate System Security Requirements" του CA/Browser Forum ενσωματώνονται με παραπομπή αποτελώντας ολοκληρωτικό κι αναπόσπαστο μέρος της παρούσας.

## *2.1 Ορισμοί*

Στο παρόν κείμενο, οι ακόλουθοι όροι και εκφράσεις με κεφαλαία έχουν την έννοια που αποδίδεται παρακάτω:

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

**Προηγμένη Ηλεκτρονική Υπογραφή:** Ηλεκτρονική υπογραφή που πληροί 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.

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

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

**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.

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

**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.

**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.

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

**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.

**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).

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

**Κυβερνητική οντότητα**: Νομική οντότητα που λειτουργεί υπό την διαχείριση της κυβέρνησης, οργανισμός, τμήμα, υπουργείο, κλάδος, ή παρόμοιο στοιχείο της κυβέρνησης μιας χώρας ή διοικητική υποδιαίρεση εντός της χώρας (όπως δήμος, γεωγραφικό διαμέρισμα, πόλη, επαρχία κλπ).

**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.

**Νομικό Πρόσωπο:** Μια ένωση, εταιρία, συνεταιρισμός, ιδιοκτησία, όμιλος, οντότητα της κυβέρνησης, ή άλλος φορέας με νομική υπόσταση, ως υποκείμενο δικαιωμάτων και υποχρεώσεων στο νομικό σύστημα μιας χώρας.

**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".

**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.

**Διαπιστευμένος Ελεγκτής:** Ένα φυσικό ή νομικό πρόσωπο που πληροί τις απαιτήσεις της παραγράφου 8.2 της ΠΠ/ΔΔΠ (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 III 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.

**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.

**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.

**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.

**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.

**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.

**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.

**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 Συνδεδεμένη Οντότητα 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.

**Περίοδος Ισχύος:** Η χρονική περίοδος ισχύος ενός Πιστοποιητικού, που ορίζεται από την ημερομηνία κατά την οποία εκδίδεται το Πιστοποιητικό μέχρι την Ημερομηνία Λήξης του.

## *2.2 Ακρωνύμια*

| Ελληνικός όρος | Συντόμευση | Αγγλικός όρος | Συντόμευση |
|---|---|---|---|
| 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 |

# 3 Στοιχεία επικοινωνίας με τον Πάροχο Υπηρεσιών Εμπιστοσύνης

## *3.1 Οργανισμός που διαχειρίζεται την πολιτική*

Το κείμενο ΠΠ/ΔΔΠ καθώς και όλα τα κείμενα όρων χρήσης, συμβάσεων, μελέτες ασφάλειας και διαδικαστικά κείμενα συνδρομητών/συμβαλλόμενων, 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] Βλ. Οδηγία (ΕΕ) 2015/2366
[2] Βλ. Εξουσιοδοτημένο Κανονισμό Επιτροπής (ΕΕ) 2018/389

### *3.2 Πρόσωπο επικοινωνίας για υποστήριξη και αιτήματα ανακλήσεων*

**support at harica.gr**

Αρχή Πιστοποίησης HARICA
ΑΚΑΔΗΜΑΙΚΟ ΔΙΑΔΙΚΤΥΟ GUnet
Ε.Κ.Π.Α. - ΚΕΝΤΡΟ ΛΕΙΤΟΥΡΓΙΑΣ & ΔΙΑΧΕΙΡΙΣΗΣ ΔΙΚΤΥΟΥ
ΠΑΝΕΠΙΣΤΗΜΙΟΥΠΟΛΗ 157 84
Τηλ: +30-2310999000
Fax: +30-2310 999100

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

Η HARICA παρέχει δυνατότητα απόκρισης 24Χ7 σε υψηλής προτεραιότητας Αναφορές Προβλημάτων Πιστοποιητικών. Κάντε αναφορά προβλήματος στη διεύθυνση **"high-priority-cert-problem-report at harica.gr"**, και όπου χρειάζεται, προωθήστε το πρόβλημα στις κατάλληλες δημόσιες αρχές, και/ή ανακαλέστε το Πιστοποιητικό που σχετίζεται με το πρόβλημα. Δείτε επίσης, τις παραγράφους 4.9.3.2 και 4.9.3.3 της ΠΠ/ΔΔΠ.

# 4 Τύποι Πιστοποιητικών, διαδικασίες ανάκλησης και χρήσεις

Η ΥΔΚ HARICA εκδίδει διάφορους τύπους πιστοποιητικών. Όλα τα Πιστοποιητικά περιέχουν πεδίο με όνομα Subject (Υποκείμενο) που περιλαμβάνει πληροφορίες για το Υποκείμενο. Αυτές οι πληροφορίες επαληθεύονται από την ΥΔΚ HARICA σύμφωνα με τις διαδικασίες που περιγράφονται στην παράγραφο 3.2 της ΠΠ/ΔΔΠ της HARICA.

### *4.1 Τύποι Πιστοποιητικών και διαδικασίες ανάκλησης*

Οι πληροφορίες του Υποκειμένου συντάσσονται ανάλογα με τον τύπο του πιστοποιητικού. Το όνομα Συνδρομητή 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, θα περιέχει ένα FQDN ή μια Διεύθυνση IP που είναι μια από τις τιμές που περιέχονται στην επέκταση subjectAltName του Πιστοποιητικού. Για πιστοποιητικά χρήστη, πιστοποιητικά S/MIME ή πιστοποιητικά Υπογραφής Κώδικα αυτό το πεδίο θα περιέχει στοιχεία του ονόματος του Υποκειμένου.<br>Για μη-TLS Πιστοποιητικά, αυτό το πεδίο 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 QEVCP-w, QEVCP-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.<br><br>Για τα **Πιστοποιητικά QEVCP-w, QEVCP-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 QEVCP-w, QEVCP-w-psd2 και EV.** Αυτό το πεδίο θα 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)**<br>**jurisdictionStateOrProvinceName** (OID: 1.3.6.1.4.1.311.60.2.1.2)<br>**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. |

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 e-mail του υποκειμένου που επιβεβαιώνεται με τις διαδικασίες που περιγράφονται στην παράγραφο 3.2.3 της ΠΠ/ΔΔΠ.
- commonName (OID: 2.5.4.3) (Προαιρετικό για πιστοποιητικά χρήσης SSL, απαραίτητο 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, θα περιλαμβάνει υποχρεωτικά ένα FQDN ή μία Διεύθυνση IP που είναι μία από τις τιμές που βρίσκονται στην επέκταση subjectAltName του Πιστοποιητικού. Η τιμή του πεδίου θα κωδικοποιείται ως εξής:
  - Αν η τιμή είναι μια Διεύθυνση IPv4, τότε η τιμή θα κωδικοποιείται ως IPv4Address όπως ορίζεται στο RFC 3986, ενότητα 3.2.2.
  - Αν η τιμή είναι μια Διεύθυνση IPv6, τότε η τιμή θα κωδικοποιείται ως text representation όπως ορίζεται στο RFC 5952, ενότητα 4.
  - Αν η τιμή είναι ένα FQDN ή Όνομα Χώρου Μπαλαντέρ, τότε η τιμή θα κωδικοποιείται ως χαρακτήρας-προς-χαρακτήρα αντίγραφο της εγγραφής dNSName από την επέκταση subjectAltName. Ειδικότερα, όλες οι Ετικέτες ονόματος Χώρου εντός FQDN ή του FQDN μέρους ενός Ονόματος Χώρου Μπαλαντέρ ΠΡΕΠΕΙ να κωδικοποιείται ως Ετικέτες LDH, ενώ οι Ετικέτες P-Label δε θα μετατρέπονται στην Unicode αναπαράστασή τους.
- Για τα Πιστοποιητικά χρηστών, S/MIME ή Υπογραφής Κώδικα, αυτό το πεδίο θα περιέχει πληροφορίες που εκπροσωπούν το όνομα του Υποκειμένου που επιβεβαιώνεται με τις διαδικασίες που ορίζει η παράγραφος 3.2.2.1 της ΠΠ/ΔΔΠ. 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 της ΠΠ/ΔΔΠ. 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 της ΠΠ/ΔΔΠ.
- postalCode (OID: 2.5.4.17): Η ταχυδρομική διεύθυνση του Υποκειμένου που επιβεβαιώνεται με τις διαδικασίες που ορίζει η παράγραφος 3.2.2.1 της ΠΠ/ΔΔΠ.
- 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 της ΠΠ/ΔΔΠ 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 της ΠΠ/ΔΔΠ. Το πεδίο αυτό δεν θα επιτρέπεται σε πιστοποιητικά τύπου SSL/TLS.

- organizationName (OID: 2.5.4.10): Θα περιέχει το όνομα της οντότητας στο subject του πιστοποιητικού όπως έχει επαληθευτεί σύμφωνα με την ενότητα 3.2.2.1 της ΠΠ/ΔΔΠ ή το DBA της Υποκείμενης ΑΠ όπως έχει επαληθευθεί σύμφωνα με την ενότητα 3.2.2.2 της ΠΠ/ΔΔΠ. 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 της ΠΠ/ΔΔΠ. 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) (Προαιρετικό): Η πόλη, χωριό ή τοπική περιοχή του Υποκειμένου που επιβεβαιώνεται με τις διαδικασίες που ορίζει η παράγραφος 3.2.2.1 της ΠΠ/ΔΔΠ. Είναι υποχρεωτικό πεδίο για TLS OV/EV Πιστοποιητικά αν το stateOrProvinceName λείπει, αλλιώς είναι προαιρετικό.
- stateOrProvinceName (OID: 2.5.4.8) (Προαιρετικό): Η πολιτεία, νομός, περιφερειακή ενότητα του Υποκειμένου που επιβεβαιώνεται με τις διαδικασίες που ορίζει η παράγραφος 3.2.2.1 της ΠΠ/ΔΔΠ. 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 της ΠΠ/ΔΔΠ.
- Subject Public Key Information: Περιέχει το Δημόσιο κλειδί και αναγνωρίζει τον αλγόριθμο δημιουργίας του και το μέγεθός του. Πιστοποιητικά που χρησιμοποιούνται για Υπογραφή Κώδικα θα 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, QEVCP-w) (Προαιρετικό για Πιστοποιητικά LCP, NCP, NCP+, QCP-n, QCP-n-qscd, QNCP-w):
    - Για EV και QEVCP-w περιέχει τον Αριθμό Μητρώου του Νομικού Εκπροσώπου του Υποκειμένου.
        - Για Ιδιωτικές Επιχειρήσεις, αυτό το πεδίο θα 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**EL-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, QCP-l-qscd, QNCP-w-OV 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**EL-123456789".
- Legal Entity Identifier της Νομικής Οντότητας με την ακόλουθη κωδικοποίηση: "**LEIXG**-123456789" που επαληθεύτηκε σύμφωνα με την ενότητα 3.2.2.1.1 της ΠΠ/ΔΔΠ.

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 περιλαμβάνουν πληροφορίες που έχουν επαληθευθεί/επιβεβαιωθεί από την HARICA.

### 4.1.1 Πιστοποιητικά SSL/TLS

Με την έκδοση ενός Πιστοποιητικού SSL/TLS, η ΥΔΚ HARICA δηλώνει ότι ακολούθησε τις διαδικασίες που περιγράφονται στην ΠΠ/ΔΔΠ της για να επαληθεύσει ότι, κατά την ημερομηνία έκδοσης του Πιστοποιητικού, όλες οι πληροφορίες σχετικά με το Υποκείμενο ήταν ακριβείς. Η HARICA δεν πρέπει να περιλαμβάνει ένα Όνομα Χώρου ή μία διεύθυνση IP σε χαρακτηριστικό Υποκειμένου εκτός από τις περιπτώσεις που ορίζονται στην παράγραφο 3.2.2.4 ή στην παράγραφο 3.2.2.5 της ΠΠ/ΔΔΠ. 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.

### 4.1.2 Πιστοποιητικά Χρήστη/Υπογραφής Κώδικα

Με την έκδοση Πιστοποιητικού Χρήστη/Υπογραφής κώδικα, η ΥΔΚ HARICA δηλώνει ότι ακολούθησε τις διαδικασίες που περιγράφονται στην ΠΠ/ΔΔΠ της για να επαληθεύσει ότι, κατά την ημερομηνία έκδοσης του Πιστοποιητικού, όλες οι πληροφορίες σχετικά με το Υποκείμενο ήταν ακριβείς. Η HARICA δεν πρέπει να περιλαμβάνει τα commonName, emailAddress μέσα σε ένα χαρακτηριστικό Υποκειμένου εκτός από τις περιπτώσεις που ορίζονται στην παράγραφο 3.2.3 της ΠΠ/ΔΔΠ. Επειδή τα χαρακτηριστικά που σχετίζονται με το όνομα του Υποκειμένου όσον αφορά τα φυσικά πρόσωπα (π.χ. givenName (2.5.4.42) και surname (2.5.4.4)) δεν υποστηρίζονται ευρέως από τα λογισμικά εφαρμογών, η ΥΔΚ HARICA μπορεί να χρησιμοποιεί το πεδίο subject:organizationName για να εκφράσει το όνομα του Υποκειμένου που αντιστοιχεί σε φυσικό πρόσωπο ή σε Διακριτό τίτλος (DBA).

Οι Συνδρομητές υποχρεούνται να παρέχουν πλήρεις, ακριβείς και αληθείς πληροφορίες (π.χ. όνομα εφαρμογής, URL πληροφοριών, περιγραφή της εφαρμογής κλπ.) στον

υπογεγραμμένο κώδικα. Οι Συνδρομητές δεσμεύονται επίσης να μην υπογράψουν εσκεμμένα Ύποπτο Κώδικα και να αναγνωρίσουν ότι μια τέτοια ενέργεια θα επιτρέψει στη HARICA να ανακαλέσει αυτόματα το πιστοποιητικό υπογραφής

### 4.1.3 Πιστοποιητικό για ηλεκτρονικές υπογραφές

Με την έκδοση Πιστοποιητικού για Προηγμένες ηλεκτρονικές υπογραφές σύμφωνα με την πολιτική QCP-n policy ή ενός Πιστοποιητικού για Εγκεκριμένες ηλεκτρονικές υπογραφές σύμφωνα με την πολιτική QCP-n-qscd, η ΥΔΚ HARICA συμπεριλαμβάνει τουλάχιστον τα χαρακτηριστικά “commonName”, “Country”, “givenName” και “surname” στο πεδίο SubjectDN. Αν αυτά τα χαρακτηριστικά δεν εξασφαλίζουν επαρκώς τη μοναδικότητα του ονόματος του Υποκειμένου στο πλαίσιο της Εκδούσας ΑΠ, τότε θα πρέπει να υπάρχει το serialNumber.

### 4.1.4 Πιστοποιητικά για ηλεκτρονικές σφραγίδες

Με την έκδοση Πιστοποιητικού για Προηγμένες ηλεκτρονικές σφραγίδες σύμφωνα με την πολιτική QCP-l ή ενός Πιστοποιητικού για Εγκεκριμένες ηλεκτρονικές σφραγίδες σύμφωνα με την πολιτική QCP-l-qscd, η HARICA περιλαμβάνει τουλάχιστον τα χαρακτηριστικά “commonName”, “Country”, "organizationName" και "OrganizationIdentifier” στο πεδίο SubjectDN.

### 4.1.5 Τεκμήρια Χρονοσήμανση

Η ΥΔΚ HARICA εκδίδει επίσης Τεκμήρια Χρονοσήμανσης και Εγκεκριμένα Τεκμήρια Χρονοσήμανσης. Τα Εγκεκριμένα Τεκμήρια Χρονοσήμανσης συμμορφώνονται με τον Ευρωπαϊκό Κανονισμό Νο 910/2014 (e-IDAS). Και οι δύο τύποι των Τεκμηρίων Χρονοσήμανσης αποδεικνύουν μία έκφανση του χρόνου πριν από ένα συγκεκριμένο χρονικό σημείο.

## *4.2 Χρήση των πιστοποιητικών*

### 4.2.1 Κατάλληλες χρήσεις των πιστοποιητικών

Τα Πιστοποιητικά της 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 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

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 περιγράφηκαν 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 του με άλλες οντότητες, εξασφαλίζοντας επιπλέον χαρακτηριστικά ασφάλειας, ισχυρότερα από αυτά που παρέχει η κλασική μέθοδος πρόσβασης με συνθηματικό χρήστη.

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.

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.

Η 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-Εγκεκριμένες» ηλεκτρονικές χρονο-σφραγίδες.

### 4.2.2 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 4.2.1 της ΠΠ/ΔΔΠ.

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.

# 5 Περιορισμοί εμπιστοσύνης

Η HARICA δεν έχει άλλους περιορισμούς εμπιστοσύνης εκτός από όσα περιγράφονται στις κατάλληλες και απαγορευμένες χρήσεις πιστοποιητικού που περιγράφονται στην παράγραφο 3.2.1 και 3.2.2 και στην ΠΠ/ΔΔΠ.

Η περίοδος διατήρησης των αρχειοθετημένων αρχείων καταγραφής (logs) περιγράφεται στην παράγραφο 5.5.2 της ΠΠ/ΔΔΠ.

Για τα Τεκμήρια Χρονοσήμανσης, η ΥΔΚ HARICA συμμορφώνεται με τις απαιτήσεις που ορίζει το πρότυπο ETSI EN 319 421 και περιλαμβάνει πεδίο "`accuracy`" με ελάχιστη ακρίβεια ενός (1) δευτερολέπτου με την πηγή ΣΠΩ (UTC). Αν ανιχνευτεί ότι ο χρόνος που θα εμφανιζόταν σε μια χρονο-σφραγίδα αποκλίνει ή διαφέρει από το συγχρονισμό με την ΣΠΩ (UTC), η Μονάδα Χρονοσήμανσης σταματά την έκδοση χρονο-σφραγίδας.

# 6 Υποχρεώσεις Συνδρομητή

Κάθε Συνδρομητής υποχρεούται κι εγγυάται τα ακόλουθα:

- ✓ έχει διαβάσει, αποδέχεται και συμμορφώνεται με την Πολιτική Πιστοποίησης / Δήλωση Διαδικασιών Πιστοποίησης της HARICA. Οι Συνδρομητές είναι υποχρεωμένοι να χρησιμοποιούν τα πιστοποιητικά αποκλειστικά για τους σκοπούς που περιγράφονται στην ενότητα 1.4.1 της 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 είναι ελεύθερη πνευματικών δικαιωμάτων τρίτων ή δικαιωμάτων διανοητικής ιδιοκτησίας, δεν περιέχει δεδομένα τα οποία με οποιονδήποτε 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. Τα δεδομένα που καλύπτονται από αυτές τις υποχρεώσεις κι εγγυήσεις περιλαμβάνουν αλλά δεν περιορίζονται σε οποιοδήποτε όνομα χώρου, περιοχή χώρου ονομάτων, Διακεκριμένο Όνομα (DN), ή Πλήρες Πιστοποιημένο Όνομα Χώρου (FQDN) και /ή οποιοδήποτε εμπορικό όνομα ή όνομα DBA, που περιέχεται σε οποιοδήποτε μέρος της αίτησης για πιστοποιητικό.
- ✓ θα δημιουργεί ένα ζεύγος κλειδιών (ιδιωτικό και δημόσιο) χρησιμοποιώντας ένα αξιόπιστο και ασφαλές σύστημα και θα λάβει όλες τις απαραίτητες προφυλάξεις για την προστασία του ιδιωτικού κλειδιού του από καταστροφή, απώλεια ή κλοπή.
- ✓ αφού λάβει το πιστοποιητικό του, ο Συνδρομητής θα συμφωνεί και επιβεβαιώνει ότι οι πληροφορίες που περιέχονται στο Πιστοποιητικό είναι ακριβείς.
- ✓ θα ζητήσει αμέσως ανάκληση Πιστοποιητικού όταν δεν χρησιμοποιείται πια ή όταν τα δεδομένα που περιέχονται έχουν αλλάξει ή όταν υπάρχει υποψία ότι το ιδιωτικό κλειδί έχει παραβιασθεί ή χαθεί. Εάν δεν ζητηθεί ανάκληση του Πιστοποιητικού, αναγνωρίζει κι αποδέχεται ότι ουδεμία αξίωση αναζήτησης ευθύνης διαθέτει, σε περίπτωση κατάχρησης του ιδιωτικού κλειδιού ή του Πιστοποιητικού, ενώ θα έπρεπε να είχε ανακληθεί.
- ✓ Για TLS Πιστοποιητικά, όταν ο Συνδρομητής ζητά ανάκληση, θα πρέπει να επιλέγεται ο καταλληλότερος λόγος ανάκλησης, όπως περιγράφεται στην ενότητα 4.9.1.1 της ΠΠ/ΔΔΠ.
- ✓ **Ακρίβεια των Πληροφοριών:** Η υποχρέωση και εγγύηση να παρέχουν πάντα ακριβείς και πλήρεις πληροφορίες στην HARICA, τόσο κατά την αίτηση για πιστοποιητικό αλλά και όποτε κι όπως αλλιώς ζητηθεί από την HARICA σε

σχέση με την έκδοση του πιστοποιητικού (-ων) που παρέχεται 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.

Στην περίπτωση Συνδρομητών Υπογραφής Κώδικα, επιπλέον των ανωτέρω υποχρεώσεων και εγγυήσεων:

- ✓ **Προστασία Ιδιωτικού Κλειδιού:** Όπου το κλειδί είναι διαθέσιμο εκτός μίας Υπηρεσίας Υπογραφής, για να διατηρείται ο αποκλειστικός έλεγχος, η εμπιστευτικότητα και η κατάλληλη προστασία, ανά πάσα στιγμή σύμφωνα με την ενότητα 6.2.7.4 της ΠΠ/ΔΔΠ, το Ιδιωτικό Κλειδί που αντιστοιχεί στο Δημόσιο Κλειδί που πρέπει να περιλαμβάνεται στο αιτούμενο Πιστοποιητικό (και τυχόν συσχετισμένα δεδομένα ενεργοποίησης ή συσκευή, π.χ. κωδικός πρόσβασης ή token). Η HARICA θα παρέχει στον Συνδρομητή τεκμηρίωση σχετικά με τον τρόπο προστασίας ενός Ιδιωτικού Κλειδιού. Η HARICA ΜΠΟΡΕΙ να παρέχει αυτήν την τεκμηρίωση ως white paper ή ως μέρος της Σύμβασης Συνδρομητή. Ο Συνδρομητής θα δηλώσει ότι θα δημιουργήσει και θα λειτουργήσει οποιαδήποτε συσκευή αποθηκεύει ιδιωτικά κλειδιά με ασφαλή τρόπο, όπως περιγράφεται σε ένα έγγραφο καλών πρακτικών για πιστοποιητικά υπογραφής κώδικα, το οποίο Η HARICA θα παρέχει στον Συνδρομητή κατά τη διαδικασία παραγγελίας. Η HARICA θα υποχρεώσει τον Συνδρομητή να χρησιμοποιεί κωδικούς πρόσβασης που δημιουργούνται τυχαία με τουλάχιστον 16 χαρακτήρες που περιέχουν κεφαλαία, πεζά γράμματα, αριθμούς και σύμβολα για τη μεταφορά ιδιωτικών κλειδιών.
- ✓ **Επαναχρησιμοποίηση Ιδιωτικού Κλειδιού:** Μην υποβάλετε αίτηση για Πιστοποιητικό Υπογραφής Κώδικα εάν το Δημόσιο Κλειδί στο Πιστοποιητικό χρησιμοποιείται ή πρόκειται να χρησιμοποιηθεί σε Πιστοποιητικό μη-Υπογραφής Κώδικα
- ✓ **Χρήση:** Να χρησιμοποιείτε το Πιστοποιητικό και το σχετικό Ιδιωτικό Κλειδί μόνο για εξουσιοδοτημένους και νόμιμους σκοπούς, συμπεριλαμβανομένης της μη χρήσης του Πιστοποιητικού για την υπογραφή Ύποπτου Κωδικού και τη χρήση του Πιστοποιητικού και του Ιδιωτικού Κλειδιού αποκλειστικά σύμφωνα με όλους τους ισχύοντες νόμους και αποκλειστικά σύμφωνα με τη Σύμβαση Συνδρομητή ή τους Όρους Χρήσης

Ανάλογα με το είδος του Πιστοποιητικού που έχει εκδοθεί και την αντίστοιχη ιεραρχία Πιστοποιητικών, οι Συνδρομητές και η HARICA πρέπει να συμμορφώνονται με τις **απαιτήσεις αναστολής και ανάκλησης πιστοποιητικών** όπως περιγράφονται στην ενότητα 4.9 της ΠΠ/ΔΔΠ.

# 7 Υποχρεώσεις των Βασιζόμενων Μερών (Relying Parties) για έλεγχο της κατάστασης Πιστοποιητικών και άλλες υποχρεώσεις

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 πληροφορίες της υπηρεσίας εμπιστοσύνης και το οποίο χρησιμοποιεί κατ' 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 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 δικαιολογημένες πεποιθήσεις.

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 τη HARICA.
- ✓ Ακολουθούνται οι όροι και οι προϋποθέσεις που περιγράφονται στην ΠΠ/ΔΔΠ.

Οι ακόλουθες δηλώσεις και διαβεβαιώσεις ισχύουν για τα Βασιζόμενα Μέρη:

- ✓ 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.

# 8 Περιορισμένη εγγύηση και αποποίηση ευθυνών / 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 της ΠΠ/ΔΔΠ. 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.

Αν η 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 πεδίο "OU" όπως δηλώνεται στην παράγραφο 9.6.2 της ΠΠ/ΔΔΠ).
- 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.

### *8.1 Αποζημιώσεις*

Ο Συνδρομητής αποζημιώνει τη HARICA και τις Συνδεδεμένες Οντότητες 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 παρούσας Σύμβασης.

## 9 Κείμενες συμβάσεις, ΔΔΠ, ΠΠ

Βλ. την ΠΠ/ΔΔΠ της ΥΔΚ HARICA στην ιστοσελίδα https://repo.harica.gr/documents/CPS

## 10 Πολιτική Απορρήτου

### *10.1 Πληροφορίες που χαρακτηρίζονται εμπιστευτικές*

Οι Αρχές Καταχώρησης 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

της ΠΠ/ΔΔΠ 7.1.4.7 (Αριθμός Μητρώου Κοινωνικής Ασφάλισης, Αριθμός Ταυτότητας, Αριθμός Φορολογικού Μητρώου, Αριθμός Διαβατηρίου), τότε αυτές οι πληροφορίες δεν θεωρούνται εμπιστευτικές.

## *10.2 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. Τα Πιστοποιητικά Συνδρομητών δημοσιεύονται στο Αποθετήριο Πιστοποιητικών της HARICA στην οποία εφαρμόζονται περιορισμοί για την προστασία από πλήθος επιθέσεων.

## *10.3 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.

## *10.4 Ενημέρωση και συγκατάθεση χρήσης εμπιστευτικών πληροφοριών*

Εκτός αν αναφέρεται άλλως στην 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.

## *10.5 Γνωστοποίηση πληροφοριών σε δικαστικές ή δημόσιες αρχές*

Οι μη εμπιστευτικές πληροφορίες που τηρεί κάθε Αρχή Πιστοποίησης και Καταχώρησης 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. ενότητα 1.5 στην ΠΠ/ΔΔΠ). 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.

## *10.6 Άλλες πληροφορίες γνωστοποίησης περιστατικών*

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.

#### 10.6.1.1 Δημοσιότητα

Με την αποδοχή των Όρων, ο Συνδρομητής παραχωρεί στην HARICA το δικαίωμα να χρησιμοποιεί την επωνυμία ή/και το λογότυπο του Συνδρομητή, να αναγνωρίζεται ως πελάτης στον ιστότοπο της HARICA ή σε άλλο μάρκετινγκ ή διαφημιστικό υλικό χωρίς προηγούμενη ειδοποίηση.

Οι συνδρομητές μπορούν να εξαιρεθούν ενημερώνοντας τη HARICA στο support@harica.gr, εντός των πρώτων 30 ημερών από την εγγραφή τους

# 11 Πολιτική επιστροφών

Δεν ορίζεται.

# 12 Κείμενη νομοθεσία, καταγγελίες κι επίλυση διαφορών

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 των δικαστηρίων της Αθήνας.

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 τη διαφορά αυτή στην Επιτροπή Διαχείρισης Πολιτικής Πιστοποίησης και Διαδικασιών της HARICA και προσπαθεί να επιλύσει ή να διευθετήσει τη διαφορά με φιλικό τρόπο πριν από την έναρξη οποιασδήποτε δικαστικής διαδικασίας. Η Επιτροπή Διαχείρισης Πολιτικής Πιστοποίησης και Διαδικασιών 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 της ΠΠ/ΔΔΠ.

Εάν δεν διευθετηθεί φιλικά, τυχόν διαφορές που σχετίζονται ή προκύπτουν από 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.

# 13 Άδειες Παρόχου Υπηρεσιών Εμπιστοσύνης και Αποθετηρίων, σήματα αξιοπιστίας και έλεγχος

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 ενδοευρωπαϊκή 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", και
- "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates 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.

Η HARICA ελέγχεται σε ετήσια βάση και πιστοποιείται από ανεξάρτητο Ελεγκτή (δηλ. έναν διαπιστευμένο Φορέα Αξιολόγησης Συμμόρφωσης). Οι αναφορές του ελέγχου υποβάλλονται στους Προμηθευτές Λογισμικού Εφαρμογών και στον Εθνικό Φορέα Εποπτείας (ΕΕΤΤ). Σύνοψη των αναφορών διατίθεται επίσης, στην ιστοσελίδα https://www.harica.gr/About/Compliance.