Ακαδημαϊκό Διαδίκτυο
(GUnet)

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

Αρχής Πιστοποίησης Ελληνικών Ακαδημαϊκών και Ερευνητικών Ιδρυμάτων (HARICA)

Σύμβαση Συνδρομητή ΥΔΚ και Όροι Χρήσης

Έκδοση 1.5 (31 Μαρτίου 2020)

# Πίνακας περιεχομένων

## Έλεγχος Εκδόσεων

| Version | Date | Comment |
|---|---|---|
| 1.0 | Μάιος 2017 | • Σύμβαση Συνδρομητή και Όροι Χρήσης |
| 1.1 | Φεβρουάριος 2018 | • Ενημέρωση που περιλαμβάνει υποχρεώσεις Αιτούντα για Πνευματικά Δικαιώματα |
| 1.2 | Οκτώβριος 2018 | • Ενημέρωση για θέματα Προσωπικών Δεδομένων. Προστέθηκαν σχετικές ενότητες από την ΠΠ/ΔΔΠ. |
| 1.3 | Μάρτιος 2019 | • Προσαρμογή στην ΠΠ/ΔΔΠ 3.8 |
| 1.4 | Οκτώβριος 2019 | • Προσαρμογή στην ΠΠ/ΔΔΠ 3.9 |
| 1.5 | Μάρτιος 2020 | • Προσαρμογή στην ΠΠ/ΔΔΠ 4.0 |

# 1 ΠΡΟΕΙΔΟΠΟΙΗΣΗ

ΔΙΑΒΑΣΤΕ ΠΡΟΣΕΚΤΙΚΑ ΤΗΝ ΠΑΡΟΥΣΑ ΣΥΜΒΑΣΗ ΣΥΝΔΡΟΜΗΤΗ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ («ΣΥΜΒΑΣΗ») ΠΡΙΝ ΑΙΤΗΘΕΙΤΕ, ΠΑΡΑΛΑΒΕΤΕ 'Η ΧΡΗΣΙΜΟΠΟΙΗΣΕΤΕ ΨΗΦΙΑΚΟ ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΤΗΣ ΥΔΚ HARICA.

ΑΝ ΔΕ ΣΥΜΦΩΝΕΙΤΕ ΜΕ ΤΟΥΣ ΟΡΟΥΣ ΑΥΤΗΣ ΤΗΣ ΣΥΜΒΑΣΗΣ ΜΗΝ ΑΙΤΕΙΣΤΕ, ΜΗΝ ΠΑΡΑΛΑΜΒΑΝΕΤΕ ΚΑΙ ΜΗΝ ΧΡΗΣΙΜΟΠΟΙΕΙΤΕ ΠΙΣΤΟΠΟΙΗΤΙΚΟ.

ΕΠΙΛΕΓΟΝΤΑΣ «ΣΥΜΦΩΝΩ» ΟΤΑΝ ΑΙΤΕΙΣΘΕ Ή ΑΠΟΔΕΧΕΣΘΕ Ή ΧΡΗΣΙΜΟΠΟΙΕΙΤΕ ΠΙΣΤΟΠΟΙΗΤΙΚΌ, ΣΥΜΦΩΝΕΙΤΕ ΟΤΙ ΓΙΝΕΣΤΕ ΣΥΝΔΡΟΜΗΤΗΣ ΚΑΙ ΥΠΟΚΕΙΣΤΕ ΣΤΟΥΣ ΟΡΟΥΣ ΧΡΗΣΗΣ ΠΟΥ ΠΕΡΙΓΡΑΦΟΝΤΑΙ ΣΕ ΑΥΤΗ ΤΗ ΣΥΜΒΑΣΗ ΚΑΙ ΣΤΗΝ ΠΠ/ΔΔΠ ΠΟΥ ΕΙΝΑΙ ΣΕ ΙΣΧΥ ΚΑΙ ΔΗΜΟΣΙΕΥΕΤΑΙ ΣΤΟ ΑΠΟΘΕΤΗΡΙΟ, ΚΑΙ ΣΥΜΠΕΡΙΛΑΜΒΑΝΟΝΤΑΙ ΜΕ ΑΝΑΦΟΡΑ ΣΕ ΑΥΤΗ ΤΗ ΣΥΜΒΑΣΗ ΚΑΙ ΕΙΝΑΙ ΑΝΑΠΟΣΠΑΣΤΟ ΜΕΡΟΣ ΑΥΤΗΣ.

ΕΠΙΛΕΓΟΝΤΑΣ «ΣΥΜΦΩΝΩ» ΟΤΑΝ ΑΙΤΕΙΣΘΕ Ή ΑΠΟΔΕΧΕΣΘΕ Ή ΧΡΗΣΙΜΟΠΟΙΕΙΤΕ ΠΙΣΤΟΠΟΙΗΤΙΚΟ ΣΥΜΦΩΝΕΙΤΕ ΕΠΙΣΗΣ ΟΤΙ ΕΧΕΤΕ ΔΙΑΒΑΣΕΙ, ΚΑΤΑΝΟΗΣΕΙ ΚΑΙ ΑΠΟΔΕΧΘΕΙ ΤΗΝ ΔΗΛΩΣΗ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ ΠΟΥ ΕΧΕΙ ΕΚΔΟΘΕΙ ΑΠ΄Ο ΤΗΝ HARICA/GUNET ΚΑΙ ΕΙΝΑΙ ΔΙΑΘΕΣΙΜΗ ΕΔΩ https://repo.harica.gr/documents/Data-Privacy-Statement-EL.pdf.

# 2 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 στο πλαίσιο των λειτουργιών του Ιδεατού Κέντρου Διαχείρισης Δικτύων (Virtual Network Operations Center – VNOC) του ΕΔΕΤ και συνεχίζεται στο πλαίσιο 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 Δήλωση Διαδικασιών Πιστοποίησης/Πολιτική Πιστοποίησης και συνυπογράφουν το Μνημόνιο Συνεργασίας.

## *2.1 Ορισμοί και ακρωνύμια*

### 2.1.1 Ορισμοί

Σε αυτή τη Σύμβαση, οι όροι κι εκφράσεις που ακολουθούν με κεφαλαία γράμματα έχουν την αντίστοιχη έννοια που τους 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 οργανισμό, 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 δηλώνει τη δυνατότητα χρήσης συγκεκριμένου Πιστοποιητικού σε συγκεκριμένη κοινότητα και / ή υλοποίηση ΥΔΚ με κοινές προδιαγραφές ασφάλειας.

**Λίστα Ανακληθέντων Πιστοποιητικών:** Μία λίστα ανακληθέντων Πιστοποιητικών που επικαιροποιείται, 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, διαχειρίζονται, 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.

**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).

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

**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.).

**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 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 (Ελεγκτής Προσόντων) της ΠΠ/ΔΔΠ.

**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.

**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 (π.χ. 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 σοβαρές ευπάθειες, συμπεριλαμβανομένων των spyware, malware και άλλου κώδικα που εγκαθιστά χωρίς τη συγκατάθεση του χρήστη ή / και αντιστέκεται στην απομάκρυνσή του και κώδικα που μπορεί να εκμεταλλευθεί με τρόπους που δεν σχεδιάζονται από τους σχεδιαστές του για να διακυβεύσει την αξιοπιστία των πλατφορμών στις οποίες εκτελείται.

**Όροι Χρήσης:** Διατάξεις σχετικά με την 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.

### 2.1.2 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 |

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

| | | | |
|---|---|---|---|
| | | Qualified Website Authentication Certificate | QWAC |

# 3 Δηλώσεις και Διαβεβαιώσεις

## *3.1 Δηλώσεις και Διαβεβαιώσεις Συνδρομητή*

Ο Συνδρομητής έχει τις ακόλουθες υποχρεώσεις και παρέχει τις εξής διαβεβαιώσεις:

- ✓ 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 σημαντική ζημία σε εσνώματα ή άϋλα αγαθά 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 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. 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 Συνδρομητή (FQDN) και /ή οποιοδήποτε εμπορικό όνομα ή όνομα DBA, που περιέχεται σε οποιοδήποτε μέρος της αίτησης για πιστοποιητικό.
- ✓ δημιουργεί 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 λάβει το πιστοποιητικό του, ο Συνδρομητής συμφωνεί και επιβεβαιώνει ότι οι πληροφορίες που περιέχονται στο Πιστοποιητικό είναι ακριβείς.
- ✓ θα ζητήσει αμέσως την ανάκληση του Πιστοποιητικού όταν δεν χρησιμοποιείται πια και θα πρέπει να σταματήσει να το χρησιμοποιεί όταν τα δεδομένα που περιέχονται έχουν αλλάξει ή οποιαδήποτε πληροφορία του Πιστοποιητικού είναι ή γίνεται αναληθής ή ανακριβής και αν γίνεται εσφαλμένη χρήση ή υπάρχει υποψία γι' αυτήν, ή όταν υπάρχει υποψία ότι το ιδιωτικό κλειδί έχει παραβιασθεί ή χαθεί
- ✓ Ειδικά στην περίπτωση υπογραφής κώδικα, ο Συνδρομητής δεσμεύεται από την ΑΚ να παρέχει πλήρεις, ακριβείς και αληθείς πληροφορίες (π.χ. όνομα εφαρμογής, URL, περιγραφή εφαρμογής, κ.α.) στον υπογεγραμμένο κώδικα. Οι Συνδρομητές δεσμεύονται επίσης να μην υπογράψουν εσκεμμένα Ύποπτο Κώδικα και να γνωρίζουν ότι μια 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 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.
- ✓ Πρέπει να χρησιμοποιούν Χρονοσφραγίδες από ΜΧΣ της HARICA σε συνδυασμό με έγκυρο Πιστοποιητικό (που δεν έχει ανακληθεί).

## *3.2 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 σημαντική ζημία σε ενσώματα ή άϋλα αγαθά 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.

## *3.3 Εμπιστευτικότητα προσωπικών πληροφοριών*

### 3.3.1 Σχέδιο Προστασίας προσωπικών δεδομένων

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.

### 3.3.2 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.

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

### 3.3.4 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.

### 3.3.5 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.

### 3.3.6 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.

### 3.3.7 Άλλες περιστάσεις 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.

## *3.4 Διαδικασίες παρακολούθησης συναλλαγών-συμβάντων*

### 3.4.1 Τύποι συναλλαγών-συμβάντων που καταγράφονται

Τα συστήματα της ΥΔΚ HARICA καταγράφουν όλες τις συναλλαγές που σχετίζονται με αιτήσεις 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. Όλοι οι εξυπηρετητές που κάνουν τις καταγραφές συγχρονίζονται μέσω πρωτοκόλλου NTP (Network Time Protocol).

### 3.4.2 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.

### 3.4.3 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.

### 3.4.4 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.

### 3.4.5 Τύποι εγγραφών που αρχειοθετούνται

Όλα τα αρχεία συναλλαγών που αναφέρονται στην παράγραφο 3.4.1 αρχειοθετούνται με ασφάλεια, καθώς και όλα τα συνοδευτικά έγγραφα που σχετίζονται με αιτήματα έκδοσης/ανάκλησης ψηφιακών πιστοποιητικών.

### 3.4.6 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.

# 4 Περιορισμοί ευθυνών

Αυτή η ρήτρα 4 ισχύει για συμβατική ευθύνη (συμπεριλαμβανομένης οποιασδήποτε αποζημίωσης ή παραβίασης της εγγύησης), για ευθύνη από αδικοπραξία (συμπεριλαμβανομένης της αμέλειας), 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 εκάστοτε 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, 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

Με την επιφύλαξη αυτής της ρήτρας 4 και των διατάξεων που περιέχονται στην ΠΠ/ΔΔΠ, η μέγιστη συνολική ευθύνη της HARICA σύμφωνα με αυτή τη Σύμβαση, που βαρύνει τους Συνδρομητές 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.

# 5 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.

# 6 Άλλες διατάξεις

## *6.1 Περίοδος ισχύος και τερματισμός της Σύμβασης 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 για οποιονδήποτε λόγο τη Σύμβαση Συνδρομητή ειδοποιώντας προηγουμένως το άλλο συμβαλλόμενο μέρος με είκοσι (20) εργάσιμες ημέρες. 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.

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.

## *6.2 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.php

## *6.3 Τροποποιήσεις στη Σύμβαση Συνδρομητή*

Η ΥΔΚ HARICA (i) αναθεωρεί τους όρους της παρούσας Σύμβασης 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 παρούσα Σύμβαση 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 μετά την ημερομηνία αλλαγής των όρων της παρούσας Συμφωνίας, η HARICA θα αντιμετωπίζει την κάθε χρήση του Συνδρομητή ως αποδοχή των ενημερωμένων όρων. Η παρούσα συμφωνία μπορεί να διορθωθεί ή να τροποποιηθεί μόνο από το ΕΔΠΠ της HARICA εκτός από τις περιπτώσεις που αναφέρονται ρητά στο παρόν.

## *6.4 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.

## *6.5 Διαδικασίες επίλυσης διαφορών*

Εάν προκύψει αντιπαράθεση ή διαφορά που σχετίζεται ή προκύπτει από την ερμηνεία της Πολιτικής Πιστοποίησης / Δήλωσης Διαδικασιών Πιστοποίησης, των πράξεων της Αρχής Πιστοποίησης και/ή την παρούσα Σύμβαση, ο Συνδρομητής μπορεί να υπαγάγει τη 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.

## *6.6 Συμμόρφωση με την κείμενη νομοθεσία*

Αυτή η Σύμβαση 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 αυτή τη Σύμβαση πρέπει να εκκινούνται ενώπιον των δικαστηρίων της Αθήνας. Και τα δύο μέρη συμφωνούν με τον τόπο και την αποκλειστική δικαιοδοσία τα δικαστήρια της Αθήνας στην Ελλάδα.

## *6.7 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.

## *6.8 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.

## *6.9 Πλήρης Σύμβαση*

Αυτή η Σύμβαση και όλα τα έγγραφα που αναφέρονται σε αυτήν αποτελούν την πλήρη σύμβαση μεταξύ των μερών, αντικαθιστώντας όλες τις άλλες συμβάσεις που ενδέχεται να υπάρχουν σε σχέση με το υποκείμενο.

## *6.10 Προστασία Δεδομένων*

Ο Συνδρομητής αναγνωρίζει το γεγονός ότι η HARICA/GUNET έχει δώσει στον Συνδρομητή ικανοποιητικές πληροφορίες σε σχέση με την Πολιτική Προστασίας Δεδομένων που έχει υλοποιήσει η HARICA καθώς και τα δικαιώματά του ως υποκείμενο των δεδομένων, όπως επίσης ότι έχει διαβάσει, κατανοήσει και αποδέχεται την Δήλωση Προστασίας Προσωπικών Δεδομένων που έχει εκδοθεί από την HARICA/GUNET ως "Υπεύθυνος Επεξεργασίας", η οποία βρίσκεται στο https://repo.harica.gr/documents/Data-Privacy-Statement-EL.pdf.

Επιπλέον, ο Συνδρομητής αποδέχεται ότι ορισμένα δεδομένα που έχει παράσχει κατά τη διαδικασία της αίτησης θα ενσωματωθούν σε ένα ψηφιακό πιστοποιητικό, το οποίο ενδέχεται να δημοσιευθεί σε ένα κατάλογο πιστοποιητικών. Οι πληροφορίες αυτές μπορεί να χρησιμοποιηθούν για τη διαδικασία ανάκλησης και για τη λειτουργία των υπηρεσιών διαχείρισης πιστοποιητικών.

Ο Συνδρομητής κατανοεί ότι με την παροχή συγκεκριμένων πληροφοριών κατά τη διαδικασία αίτησης Πιστοποιητικού, συναίνει με τη δημοσιοποίηση συγκεκριμένων πληροφοριών για τους σκοπούς που είναι απαραίτητοι για την εκτέλεση αυτής της Σύμβασης Συνδρομητή και την παροχή των υπηρεσιών ή προϊόντων εμπιστοσύνης, και κατανοεί ότι έχει το δικαίωμα διόρθωσης κάθε σχετικής προσωπικής πληροφορίας.