Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης

Κέντρο Ηλεκτρονικής Διακυβέρνησης

Υποδομή Δημοσίου Κλειδιού

Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης

Έκδοση 4.2 (29 Σεπτεμβρίου 2017)

Πίνακας Περιεχομένων

1 Εισαγωγή

Το έγγραφο αυτό ορίζει την πολιτική και τις διαδικασίες πιστοποίησης που χρησιμοποιούνται από τις Αρχές Πιστοποίησης που συμμετέχουν στην Υποδομή Δημοσίου Κλειδιού (ΥΔΚ) του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης (ΑΠΘ). Η Υποδομή Δημοσίου Κλειδιού του ΑΠΘ ξεκίνησε το 2001 από το Κέντρο Λειτουργίας Δικτύου ΑΠΘ (για συντομία ΚΛΔ) με τη δημιουργία μιας ανεξάρτητης Κεντρικής Αρχής Πιστοποίησης (ROOT Certification Authority). Το ΚΛΔ ΑΠΘ ανέλαβε πρωτοβουλία για τη δημιουργία μιας ενιαίας Υποδομής Δημοσίου Κλειδιού όλων των Ακαδημαϊκών και Ερευνητικών φορέων της Ελλάδας. Την πρωτοβουλία αυτή χαιρέτησαν αρκετοί φορείς με κύριους το Πανεπιστήμιο Αιγαίου και το Εθνικό Δίκτυο Έρευνας και Τεχνολογίας (ΕΔΕΤ), με αποτέλεσμα μέσα στο 2006 να δημιουργηθεί η «Αρχή Πιστοποίησης Ελληνικών Ακαδημαϊκών και Ερευνητικών Ιδρυμάτων» (Hellenic Academic & Research Institutions Certification Authority – HARICA) (http://www.harica.gr). Το Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης στην προσπάθεια διεύρυνσης του κύκλου εμπιστοσύνης των Αρχών Πιστοποίησης ανάμεσα σε άλλους φορείς (στο εσωτερικό και το εξωτερικό), προχώρησε σε στάδιο μετάβασης από την ανεξάρτητη Κεντρική Αρχή Πιστοποίησης που διέθετε, σε μια Αρχή Πιστοποίησης που συμμετέχει σε σχήμα εμπιστοσύνης υπό την Κεντρική Αρχή Πιστοποίησης της HARICA. Η HARICA χρηματοδοτείται σήμερα από το Ακαδημαϊκό Διαδίκτυο (GUNET – http://www.gunet.gr). Το 2013, το ΚΛΔ ΑΠΘ συγχωνεύτηκε μαζί με άλλες κεντρικές Μονάδες Πληροφορικής και Επικοινωνιών, δημιουργώντας το «Κέντρο Ηλεκτρονικής Διακυβέρνησης» (ΚΗΔ), μια νέα Πανεπιστημιακή Διεύθυνση, που είναι πλέον υπεύθυνο για την Υποδομή Δημοσίου Κλειδιού του ΑΠΘ. Η Αρχή Πιστοποίησης ΑΠΘ λειτουργεί ως «ενδιάμεση Αρχή Πιστοποίησης» (Subordinate CA) της HARICA.

1.1 Επισκόπηση

Η παρούσα Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης περιγράφει το σύνολο κανόνων οι οποίοι εφαρμόζονται για την έκδοση πιστοποιητικών από την Αρχή Πιστοποίησης του ΑΠΘ.

Οι όροι και οι συνθήκες που περιγράφονται στην παρούσα ΠΠ/ΔΔΠ συμμορφώνονται με τους σχετικούς όρους και συνθήκες της Αρχής Πιστοποίησης HARICA, όπως περιγράφονται στην τελευταία έκδοση της ΠΠ/ΔΔΠ της HARICA, η οποία μπορεί να βρεθεί στην ηλεκτρονική διεύθυνση http://www.harica.gr/documents/CPS.php.

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

Η Αρχή Πιστοποίησης του ΑΠΘ λειτουργεί ως «Εγκεκριμένος» Πάροχος Υπηρεσιών Εμπιστοσύνης, εκδίδοντας «Εγκεκριμένα» Ψηφιακά Πιστοποιητικά για Ψηφιακές Υπογραφές σύμφωνα με τον Ευρωπαϊκό Κανονισμό 910/2014, που απορρέει από το γεγονός ότι λειτουργεί ως Ενδιάμεση Αρχή Πιστοποίησης της HARICA.

1.2 Ονομασία και αναγνώριση κειμένου

Το παρόν κείμενο ονομάζεται «Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης της Υποδομής Δημοσίου Κλειδιού του ΑΠΘ» και αποτελεί την τεκμηρίωση και τον κανονισμό λειτουργίας της Αρχής Πιστοποίησης του Αριστοτέλειου Πανεπιστημίου Θεσσαλονίκης. Σε σύντμηση πρέπει να αναφέρεται ως «ΠΠ-ΔΔΠ του ΑΠΘ» και στην αγγλική του έκδοση ως “AUTH CP-CPS”

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

Η δομή του παρόντος κειμένου βασίζεται στο πρότυπο IETF RFC-3647 με ελάχιστες διαφοροποιήσεις που είναι αναγκαίες για να περιγραφούν οι ιδιαίτερες ανάγκες του Ακαδημαϊκού χώρου. Επίσης, υπάρχουν ευθείες αναφορές στην ΠΠ-ΔΔΠ της HARICA.

Ο παγκόσμια μοναδικός Αριθμός Αναγνώρισης (OID) αυτού του εγγράφου είναι: 1.3.6.1.4.1.**7709.2.0.4.2** όπου:

1.3.6.1.4.1.**7709**	Αριθμός Αναγνώρισης (OID) του ΑΠΘ, καταχωρημένος από τον οργανισμό IANA (www.iana.org)
2	Υπηρεσία Πιστοποίησης
0	Δήλωση Διαδικασιών Πιστοποίησης
4.2	Πρώτο και δεύτερο ψηφίο του αριθμού έκδοσης (version) της Δήλωσης Διαδικασιών Πιστοποίησης

1.3 Κοινότητα εφαρμογής της ΥΔΚ

Η κοινότητα που διέπεται από αυτή την Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης είναι το σύνολο των οντοτήτων που χρησιμοποιούν τα πιστοποιητικά που εκδίδονται από την ΑΠ του ΑΠΘ.

1.3.1 Αρχές Πιστοποίησης

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

Η Ιεραρχία της Υπηρεσίας Πιστοποίησης κατά τη χρονική στιγμή δημιουργίας της, αποτελούνταν από τις παρακάτω οντότητες:

1. Κεντρική Αρχή Πιστοποίησης (Central Certification Authority, AUTH-CENTRAL-CA) η οποία εκδίδει ψηφιακά πιστοποιητικά για υφιστάμενες Αρχές Πιστοποίησης που λειτουργούν υπό το νομικό πρόσωπο του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης καθώς και πιστοποιητικά τελικών

χρηστών-συσκευών (end-entity). Το πιστοποιητικό της AUTH-CENTRAL-CA έχει διάρκεια ισχύος μεταξύ οκτώ (8) και δεκαπέντε (15) ετών.

2. Ενδιάμεσες Αρχές Πιστοποίησης, που μπορούν να λειτουργούν για διαχειριστικούς λόγους του ΑΠΘ, οι οποίες εξυπηρετούν διοικητικές ή ακαδημαϊκές μονάδες του ΑΠΘ ή νομικά πρόσωπα όπου συμμετέχει το ΑΠΘ, οι οποίες συμμορφώνονται και υιοθετούν πλήρως την παρούσα Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης. Τα πιστοποιητικά των ενδιάμεσων Αρχών Πιστοποίησης έχουν διάρκεια ισχύος μεταξύ τεσσάρων (4) και οκτώ (8) ετών.

Η Αρχή Πιστοποίησης ΑΠΘ δεν επιτρέπεται να Δια-Πιστοποιήσει (cross-certify) διαφορετικές ιεραρχίες ΥΔΚ.

Όλες οι ενδιάμεσες Αρχές Πιστοποίησης του ΑΠΘ έχουν τεχνικούς περιορισμούς, όπως περιγράφονται στο κείμενο “Baseline Requirements” του CA/Browser Forum. Όλα τα Πιστοποιητικά των ενδιάμεσων Αρχών Πιστοποίησης περιλαμβάνουν επέκταση Πιστοποιητικών (name constraints) που περιορίζει τα domain names και τα directory names που λειτουργούν υπό τον έλεγχο του ΑΠΘ και συνεργαζόμενων Ιδρυμάτων.

1.3.2 Αρχές Καταχώρησης

Οι Αρχές Καταχώρισης είναι οντότητες αρμόδιες για την πιστοποίηση της ταυτότητας των εγγραφόμενων πριν από την έκδοση του πιστοποιητικού. Οι ΑΚ διαβιβάζουν με ασφαλή τρόπο τις αιτήσεις στην αρμόδια Αρχή Πιστοποίησης. Το ΚΗΔ ΑΠΘ λειτουργεί ως κεντρική Αρχή Καταχώρισης της ΥΔΚ και ελέγχει αιτήσεις συνδρομητών, ταυτοπροσωπία αιτούμενων, κατοχή domain καθώς και όλα τα καθήκοντα ελέγχου πριν την έκδοση ενός ψηφιακού πιστοποιητικού συνδρομητή.

1.3.3 Συνδρομητές

Συνδρομητές στην Υπηρεσία Πιστοποίησης είναι όσοι αιτούνται και αποκτούν ψηφιακό πιστοποιητικό υπογεγραμμένο από Αρχή Πιστοποίησης του ΑΠΘ. Συνδρομητές στην Υπηρεσία μπορούν να είναι οντότητες (φυσικά πρόσωπα που έχουν συμβατική, ακαδημαϊκή σχέση ή συνεργασία με το ΑΠΘ και συσκευές που λειτουργεί το ΑΠΘ).

Εφαρμόζονται οι κανόνες και οι διαδικασίες που περιγράφονται στην ΠΠ/ΔΔΠ της HARICA, όπως για παράδειγμα η εγγραφή μη φυσικών προσώπων ή ρόλων.

1.3.4 Οντότητες που βασίζονται στην Υπηρεσία

Οι οντότητες που βασίζονται στην Υπηρεσία είναι όλες οι οντότητες που εμπιστεύονται τις παρεχόμενες υπηρεσίες πιστοποίησης της ΑΠ ΑΠΘ και της ΑΠ HARICA, όπως ορίζεται στην ΠΠ/ΔΔΠ της HARICA.

1.3.5 Άλλοι συμμετέχοντες

Δεν ορίζεται.

1.4 Χρήση των Πιστοποιητικών

Τα πιστοποιητικά μπορούν να χρησιμοποιηθούν από τα μέλη της ευρύτερης ακαδημαϊκής και ερευνητικής κοινότητας, αλλά και από άλλους χρήστες. Οι αποδεκτές και απαγορευμένες χρήσεις των πιστοποιητικών μπορούν να βρεθούν στην ΠΠ/ΔΔΠ της HARICA. Η Αρχή Πιστοποίησης ΑΠΘ δεν εκδίδει Πιστοποιητικά για υπογραφή κώδικα (code signing) ή χρονοσήμανση (time stamping).

1.5 Διαχείριση της Πολιτικής

1.5.1 Οργανισμός που διαχειρίζεται την Πολιτική

ca-admin@it.auth.gr
Κέντρο Ηλεκτρονικής Διακυβέρνησης ΑΠΘ
Σχολή Θετικών Επιστημών
1ος όροφος Κτιρίου Βιολογίας
Πανεπιστημιούπολη ΑΠΘ
54124 Θεσσαλονίκη,
Ελλάδα

1.5.2 Πρόσωπα Επικοινωνίας

pki@auth.gr

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

Γιάννης Σαλματζίδης [jsal@it.auth.gr]
Τηλ: 2310 998398
Fax: 2310 999100

Κέντρο Ηλεκτρονικής Διακυβέρνησης (ΚΗΔ) ΑΠΘ
Σχολή Θετικών Επιστημών
1ος όροφος Κτιρίου Βιολογίας
Πανεπιστημιούπολη ΑΠΘ
54124 Θεσσαλονίκη
Ελλάδα

1.5.3 Πρόσωπα που κρίνουν τη συμμόρφωση στην Πολιτική

pki@auth.gr

Δημήτρης Ζαχαρόπουλος [jimmy@it.auth.gr]
Τηλ: 2310 998483
Fax: 2310 998492

Γιάννης Σαλματζίδης [jsal@it.auth.gr]
Τηλ: 2310 998398
Fax: 2310 999100

Κέντρο Ηλεκτρονικής Διακυβέρνησης (ΚΗΔ) ΑΠΘ
Σχολή Θετικών Επιστημών
1ος όροφος Κτιρίου Βιολογίας
Πανεπιστημιούπολη ΑΠΘ
54124 Θεσσαλονίκη
Ελλάδα

1.5.4 Διαδικασίες έγκρισης ΠΠ/ΔΔΠ

Η ΠΠ/ΔΔΠ εγκρίνεται από την αρμόδια «Επιτροπή Διαχείρισης Πολιτικής και Διαδικασιών Πιστοποίησης της Υποδομής Δημοσίου Κλειδιού ΑΠΘ».

1.6 Ορισμοί και Ακρωνύμια

Εφαρμόζονται οι ορισμοί και τα ακρωνύμια της ΠΠ/ΔΔΠ της HARICA, όπως ορίζονται στην ενότητα 1.6 της ΠΠ/ΔΔΠ της HARICA.

2 Δημοσιοποίηση και αποθήκες

2.1 Αποθήκες

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

2.2 Δημοσιοποίηση πληροφοριών της Αρχής Πιστοποίησης

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

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

Η ηλεκτρονική και δημόσια προσβάσιμη διεύθυνση της αποθήκης της Υποδομής Δημοσίου Κλειδιού ΑΠΘ είναι http://www.pki.auth.gr/rep_dyn.

Επιπλέον, είναι δυνατή η αναζήτηση πιστοποιητικών συνδρομητών και ΛΑΠ στην υπηρεσία καταλόγου του ΑΠΘ.

2.3 Συχνότητα δημοσιοποίησης

Ισχύουν οι διατάξεις της ενότητας 2.3 της ΠΠ/ΔΔΠ της HARICA.

2.4 Έλεγχος πρόσβασης

Ισχύουν τα μέτρα ελέγχου πρόσβασης που ορίζονται στην ενότητα 2.4 της ΠΠ/ΔΔΠ της HARICA.

3 Αναγνώριση και απόδειξη ταυτότητας

3.1 Ονοματολογία

Ισχύει η ονοματολογία που ορίζεται στην ενότητα 3.1 της ΠΠ/ΔΔΠ της HARICA.

3.1.1 Τύποι ονομάτων

Ισχύουν οι διατάξεις της ενότητας 3.1.1 της ΠΠ/ΔΔΠ της HARICA.

Επιπρόσθετα, το διακριτικό «O=Aristotle University of Thessaloniki» πρέπει να συμπεριλαμβάνεται σε όλα τα πιστοποιητικά χρηστών, συσκευών, υπηρεσιών και υπογραφής κώδικα.

3.1.2 Υποχρέωση τα ονόματα να έχουν συγκεκριμένο νόημα

Ισχύουν οι διατάξεις της ενότητας 3.1.2 της ΠΠ/ΔΔΠ της HARICA.

3.1.3 Δυνατότητα έκδοσης ανώνυμων πιστοποιητικών ή πιστοποιητικών με ψευδώνυμα

Ισχύουν οι διατάξεις της ενότητας 3.1.3 της ΠΠ/ΔΔΠ της HARICA.

3.1.4 Κανόνες σύνταξης των ονομάτων

Ισχύουν οι διατάξεις της ενότητας 3.1.4 της ΠΠ/ΔΔΠ της HARICA.

Επιπρόσθετα, το διακριτικό «O=Aristotle University of Thessaloniki» πρέπει να συμπεριλαμβάνεται σε όλα τα πιστοποιητικά χρηστών, συσκευών και υπηρεσιών.

3.1.5 Μοναδικότητα ονομάτων

Ισχύουν οι διατάξεις της ενότητας 3.1.5 της ΠΠ/ΔΔΠ της HARICA.

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

Αρμόδιο για θέματα επίλυσης διαφορών σχετικά με την κυριότητα ονομάτων στην ΥΔΚ ΑΠΘ είναι το Γραφείο Πρυτανείας του ΑΠΘ, στο οποίο εισηγείται σχετικά η «Επιτροπή Διαχείρισης Πολιτικής και Διαδικασιών Πιστοποίησης της Υποδομής Δημοσίου Κλειδιού ΑΠΘ».

3.2 Αρχική Επαλήθευση ταυτότητας

Ισχύουν οι μέθοδοι για την απόδειξη κατοχής ιδιωτικού κλειδιού και απόδειξη ταυτότητας οργανισμού που ορίζονται στην ενότητα 3.2 της ΠΠ/ΔΔΠ της HARICA, όπου τον οργανισμό αποτελεί το Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης.

Επιπλέον, η μέθοδος που υποστηρίζεται από το Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης για τον έλεγχο κυριότητας μίας e-mail διεύθυνσης είναι η χρήση αρχιτεκτονικής Single Sign On (SSO) που βασίζεται στο πρότυπο SAML, όπως ορίζεται στην ΠΠ/ΔΔΠ της HARICA.

Η έκδοση ψηφιακών πιστοποιητικών SSL/TLS επιτρέπεται μόνο για ζώνη DNS (domain) που ανήκει στο Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης ή συνεργαζόμενους με το ΑΠΘ φορείς. Προκειμένου ένας χρήστης να μπορεί να αιτηθεί πιστοποιητικό συσκευής (SSL/TLS), πρέπει να είναι κάτοχος πιστοποιητικού χρήστη το οποίο χρησιμοποιεί για να πιστοποιήσει την ταυτότητά του. Έπειτα, αποστέλλεται ένα μήνυμα e-mail σε εξουσιοδοτημένο Διαχειριστή του Κέντρου Ηλεκτρονικής Διακυβέρνησης του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης ο οποίος ελέγχει αν είναι έγκυρο το FQDN του αιτήματος καθώς και αν ο χρήστης που αιτείται το πιστοποιητικό είναι διαχειριστής του συγκεκριμένου FQDN μέσω του μητρώου χρηστών/υπολογιστών που τηρείται στο Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης. Μόνο οι μέθοδοι ελέγχου κατοχής domain που περιγράφονται στην ενότητα 3.2.2.4 της ΠΠ/ΔΔΠ της HARICA επιτρέπεται να χρησιμοποιηθούν.

3.3 Επαλήθευση ταυτότητας για έκδοση νέων κλειδιών-πιστοποιητικών

Η ΥΔΚ ΑΠΘ χειρίζεται τα αιτήματα έκδοσης νέων κλειδιών-πιστοποιητικών σύμφωνα με την ενότητα 3.3 της ΠΠ/ΔΔΠ της HARICA.

3.4 Επαλήθευση ταυτότητας για αιτήματα ανάκλησης

Η ΥΔΚ ΑΠΘ χειρίζεται τα αιτήματα ανάκλησης σύμφωνα με την ενότητα 3.4 της ΠΠ/ΔΔΠ της HARICA.

4 Απαιτήσεις λειτουργίας, κύκλος ζωής πιστοποιητικών

4.1 Αιτήσεις για πιστοποιητικά

Μία αίτηση για έκδοση πιστοποιητικού μπορεί να κατατεθεί από ένα συνδρομητή σύμφωνα με την ΠΠ/ΔΔΠ της HARICA από την ιστοσελίδα της Αρχής Καταχώρησης, http://www.pki.auth.gr/ ή μέσω της ΑΚ της σχολής ή του τμήματός του.

4.2 Επεξεργασία αιτήσεων πιστοποιητικών

Οι αιτήσεις πιστοποιητικών επεξεργάζονται σύμφωνα με τη διαδικασία που ορίζεται στην ενότητα 4.2 της ΠΠ/ΔΔΠ της HARICA.

4.3 Έκδοση πιστοποιητικών

Τα πιστοποιητικά εκδίδονται σύμφωνα με τη διαδικασία που ορίζεται στην ενότητα 4.3 της ΠΠ/ΔΔΠ της HARICA.

4.4 Αποδοχή πιστοποιητικών

Η αποδοχή πιστοποιητικών γίνεται σύμφωνα με τη διαδικασία που ορίζεται στην ενότητα 4.4 της ΠΠ/ΔΔΠ της HARICA.

4.5 Ζεύγος κλειδιών και χρήσεις των πιστοποιητικών

Η χρήση των πιστοποιητικών που εκδίδονται από την ΥΔΚ του ΑΠΘ και των σχετικών ζευγών κλειδιών ορίζεται στην ενότητα 4.5 της ΠΠ/ΔΔΠ της HARICA.

4.6 Ανανέωση πιστοποιητικών

Η ΥΔΚ ΑΠΘ χειρίζεται την ανανέωση πιστοποιητικών σύμφωνα με τη διαδικασία που ορίζεται στην ενότητα 4.6 της ΠΠ/ΔΔΠ της HARICA.

4.7 Επανέκδοση κλειδιών

Η ΥΔΚ ΑΠΘ χειρίζεται την επανέκδοση κλειδιών σύμφωνα με τη διαδικασία που ορίζεται στην ενότητα 4.7 της ΠΠ/ΔΔΠ της HARICA.

4.8 Μεταβολή πιστοποιητικών

Ισχύουν οι διατάξεις της ενότητας 4.8 της ΠΠ/ΔΔΠ της HARICA.

4.9 Αναστολή και ανάκληση πιστοποιητικών

Η ΥΔΚ ΑΠΘ χειρίζεται την αναστολή και ανάκληση πιστοποιητικών σύμφωνα με τη διαδικασία που ορίζεται στην ενότητα 4.9 της ΠΠ/ΔΔΠ της HARICA.

4.10 Υπηρεσίες ελέγχου κατάστασης πιστοποιητικών

Χρησιμοποιούνται οι υπηρεσίες ελέγχου κατάστασης πιστοποιητικών που ορίζονται στην ενότητα 4.10 της ΠΠ/ΔΔΠ της HARICA.

4.11 Λήξη συνδρομής

Ισχύουν οι διατάξεις της ενότητας 4.11 της ΠΠ/ΔΔΠ της HARICA.

4.12 Συνοδεία ιδιωτικού κλειδιού (key escrow) και επαναφορά κλειδιού

Η ΥΔΚ ΑΠΘ χειρίζεται τη συνοδεία ιδιωτικού κλειδιού και την επαναφορά κλειδιού σύμφωνα με την ενότητα 4.12 της ΠΠ/ΔΔΠ της HARICA.

5 Διοικητικοί, τεχνικοί και λειτουργικοί έλεγχοι

5.1 Φυσική ασφάλεια και έλεγχος πρόσβασης

Η Αρχή Πιστοποίησης του ΑΠΘ βρίσκεται υπό τη διαχείριση του Κέντρου Ηλεκτρονικής Διακυβέρνησης (ΚΗΔ), του ΑΠΘ.

Ισχύουν οι κανόνες φυσικής ασφάλειας και οι έλεγχοι πρόσβασης που ορίζονται στην ενότητα 5.1 της ΠΠ/ΔΔΠ της HARICA.

5.2 Έλεγχος διαδικασιών

Ισχύουν οι έλεγχοι διαδικασιών που ορίζονται στην ενότητα 5.2 της ΠΠ/ΔΔΠ της HARICA.

5.3 Έλεγχος ασφαλείας προσωπικού

Ισχύουν οι έλεγχοι ασφάλειας προσωπικού που ορίζονται στην ενότητα 5.3 της ΠΠ/ΔΔΠ της HARICA.

5.4 Διαδικασίες παρακολούθησης συναλλαγών – συμβάντων

Ισχύουν οι διαδικασίες παρακολούθησης συναλλαγών-συμβάντων που ορίζονται στην ενότητα 5.4 της ΠΠ/ΔΔΠ της HARICA.

5.5 Αρχειοθέτηση εγγραφών

Ισχύουν οι διαδικασίες αρχειοθέτησης εγγραφών που ορίζονται στην ενότητα 5.5 της ΠΠ/ΔΔΠ της HARICA.

5.6 Ριζική αλλαγή κλειδιού

Ισχύουν οι διαδικασίες ριζικής αλλαγής κλειδιού που ορίζονται στην ενότητα 5.6 της ΠΠ/ΔΔΠ της HARICA.

5.7 Ανάκαμψη από παραβίαση ασφάλειας και καταστροφή

Ισχύουν οι διαδικασίες ανάκαμψης από παραβίαση ασφάλειας και καταστροφή που ορίζονται στην ενότητα 5.7 της ΠΠ/ΔΔΠ της HARICA.

5.8 Τερματισμός Αρχής Πιστοποίησης – Αρχής Καταχώρησης

Ισχύουν οι διαδικασίες τερματισμού Αρχής Πιστοποίησης – Αρχής Καταχώρησης που ορίζονται στην ενότητα 5.8 της ΠΠ/ΔΔΠ της HARICA.

6 Έλεγχοι ασφάλειας τεχνικού επιπέδου

6.1 Δημιουργία ζεύγους κλειδιών και εγκατάσταση

Ισχύουν οι διατάξεις και οι έλεγχοι της ενότητας 6.1 της ΠΠ/ΔΔΠ της HARICA.

6.2 Προστασία ιδιωτικών κλειδιών

Ισχύουν οι διατάξεις και οι έλεγχοι της ενότητας 6.2 της ΠΠ/ΔΔΠ της HARICA.

6.3 Άλλα θέματα διαχείρισης ζεύγους κλειδιών

Ισχύουν οι διατάξεις και οι έλεγχοι της ενότητας 6.3 της ΠΠ/ΔΔΠ της HARICA.

6.4 Δεδομένα ενεργοποίησης

Ισχύουν οι διατάξεις και οι έλεγχοι της ενότητας 6.4 της ΠΠ/ΔΔΠ της HARICA.

6.5 Έλεγχοι ασφαλείας υπολογιστών

Ισχύουν οι διατάξεις και οι έλεγχοι της ενότητας 6.5 της ΠΠ/ΔΔΠ της HARICA.

6.6 Έλεγχοι ασφαλείας κύκλου ζωής

Ισχύουν οι διατάξεις και οι έλεγχοι της ενότητας 6.6 της ΠΠ/ΔΔΠ της HARICA.

6.7 Έλεγχοι ασφαλείας δικτύου

Ισχύουν οι διατάξεις και οι έλεγχοι της ενότητας 6.7 της ΠΠ/ΔΔΠ της HARICA.

6.8 Χρονοσφραγίδες – Χρονοσήμανση

Ισχύουν οι διατάξεις και οι έλεγχοι της ενότητας 6.8 της ΠΠ/ΔΔΠ της HARICA.

7 Περίγραμμα (profile) πιστοποιητικού, ΛΑΠ και OCSP

7.1 Περίγραμμα πιστοποιητικού

Χρησιμοποιείται το περίγραμμα πιστοποιητικού σύμφωνα με το RFC5280 “Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile”.

7.1.1 Περιορισμοί ονομάτων

Ισχύουν οι διατάξεις της ενότητας 7.1.1 της ΠΠ/ΔΔΠ της HARICA.

7.1.2 Επεκτάσεις Πιστοποιητικών

Ισχύουν οι διατάξεις της ενότητας 7.1.2 της ΠΠ/ΔΔΠ της HARICA.

7.1.3 Αναγνωριστικά των Αλγορίθμων που χρησιμοποιούνται

Ισχύουν οι διατάξεις της ενότητας 7.1.3 της ΠΠ/ΔΔΠ της HARICA.

7.1.4 Μορφή Ονομάτων

Ισχύουν οι διατάξεις της ενότητας 7.1.4 της ΠΠ/ΔΔΠ της HARICA. Η ΑΠ ΑΠΘ δεν εκδίδει Πιστοποιητικά υπογραφής Κώδικα ή Χρονοσήμανσης.

7.1.5 Περιορισμοί Ονομάτων

Η ΑΠ ΑΠΘ εφαρμόζει περιορισμό ονομάτων σε όλες τις Ενδιάμεσες Αρχές Πιστοποίησης σύμφωνα με το RFC5280. Η επέκταση αυτή, δεν είναι μαρκαρισμένη ως «κρίσιμη» (critical) και περιορίζει όλα τα πιστοποιητικά στο “auth.gr” domain.

Επιτρέπεται η έκδοση πιστοποιητικών για εξυπηρετητές για Ακαδημαϊκούς και Ερευνητικούς σκοπούς για άλλα domains, μέσω ειδικής ενδιάμεσης Αρχής Πιστοποίησης που λειτουργεί υπό τη διαχείριση της HARICA.

7.1.6 Αναγνωριστικό πολιτικής πιστοποίησης

Το αναγνωριστικό της πολιτικής πιστοποίησης, OID (Object Identifier): 1.3.6.1.4.1.**7709.2.0.4.2**, με την οποία συμμορφώνεται η «Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης της Υποδομής Δημοσίου Κλειδιού του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης, έκδοση 4.2» περιλαμβάνεται στα πιστοποιητικά. Επιπλέον, ισχύουν οι διατάξεις της ενότητας 7.1.6 της ΠΠ/ΔΔΠ της HARICA.

7.1.7 Χρήση των περιορισμών πολιτικής

Δεν ορίζεται.

7.1.8 Σύνταξη και μορφή περιορισμών πολιτικής

Η εγκεκριμένη πολιτική είναι το URI που δείχνει στη δημοσιευμένη ΠΠ/ΔΔΠ της ΑΠ ΑΠΘ.

7.1.9 Επεξεργασία μορφής κρίσιμων επεκτάσεων Πολιτικής Πιστοποίησης

Δεν ορίζεται.

7.2 Περίγραμμα ΛΑΠ

Χρησιμοποιείται το περίγραμμα ΛΑΠ που ορίζεται στην ενότητα 7.2 της ΠΠ/ΔΔΠ της HARICA.

7.3 Περίγραμμα OCSP

Χρησιμοποιείται το περίγραμμα OCSP που ορίζεται στην ενότητα 7.3 της ΠΠ/ΔΔΠ της HARICA.

8 Έλεγχοι συμμόρφωσης και άλλες εκτιμήσεις

Η ΥΔΚ ΑΠΘ καλύπτει τις τεχνικές προδιαγραφές των ακόλουθων προτύπων/κανονισμών:

- 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 TS 101 456 “Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates”,
- ETSI TS 102 042 standard “Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates”,
- Προεδρικό Διάταγμα 150/2001 και
- Κανονισμός (EU) Αρ. 910/2014 (e-IDAS) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ.

Επίσης, η ΑΠ ΑΠΘ έχει ενσωματώσει στις τρέχουσες διαδικασίες της (CP/CPS), οδηγίες και διαδικασίες από το κείμενο “Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates” της σύμπραξης CA/Browser Forum (www.cabforum.org).

9 Διοικητικά και Νομικά θέματα

9.1 Κόστη εγγραφής

Δεν καταβάλλονται τέλη για τις παρεχόμενες υπηρεσίες. Επιπρόσθετα, ισχύουν οι διατάξεις της ενότητας 9.1 της ΠΠ/ΔΔΠ της HARICA.

9.2 Οικονομική ευθύνη

Η ΥΔΚ ΑΠΘ δεν αναλαμβάνει ούτε και αποδέχεται οποιαδήποτε οικονομική ευθύνη εκτός αν άλλως ορίζεται ειδικότερα στο παρόν. Επιπρόσθετα, ισχύουν οι διατάξεις της ενότητας 9.1 της ΠΠ/ΔΔΠ της HARICA.

9.3 Εμπιστευτικότητα πληροφοριών εμπορικού χαρακτήρα

Η ΥΔΚ ΑΠΘ δεν χειρίζεται πληροφορίες εμπορικού χαρακτήρα.

9.4 Εμπιστευτικότητα πληροφοριών προσωπικού χαρακτήρα

Ισχύουν οι διατάξεις της ενότητας 9.4 της ΠΠ/ΔΔΠ της HARICA.

Για τη διάθεση στις δικαστικές αρχές εμπιστευτικών πληροφοριών ή προσωπικών δεδομένων των εγγραφόμενων, θα γίνεται αίτηση σύμφωνα με την ισχύουσα νομοθεσία και μέσω της Πρυτανείας του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης

9.5 Δικαιώματα πνευματικής ιδιοκτησίας

Ισχύουν οι διατάξεις της ενότητας 9.5 της ΠΠ/ΔΔΠ της HARICA.

9.6 Αντιπροσωπεύσεις και εξουσιοδοτήσεις

Ισχύουν οι διατάξεις της ενότητας 9.6 της ΠΠ/ΔΔΠ της HARICA.

9.7 Αποκηρύξεις και Εγγυήσεις

Ισχύουν οι διατάξεις της ενότητας 9.7 της ΠΠ/ΔΔΠ της HARICA.

9.8 Περιορισμοί ευθυνών

Ισχύουν οι διατάξεις της ενότητας 9.8 της ΠΠ/ΔΔΠ της HARICA.

9.9 Αποζημιώσεις

Ισχύουν οι διατάξεις της ενότητας 9.9 της ΠΠ/ΔΔΠ της HARICA.

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

Ισχύουν οι διατάξεις της ενότητας 9.10 της ΠΠ/ΔΔΠ της HARICA.

9.11 Ατομικές ειδοποιήσεις και επικοινωνία μεταξύ των αποτελούμενων μερών

Ισχύουν οι διατάξεις της ενότητας 9.11 της ΠΠ/ΔΔΠ της HARICA.

9.12 Τροποποιήσεις

Ισχύουν οι διατάξεις της ενότητας 9.12 της ΠΠ/ΔΔΠ της HARICA.

9.13 Διαδικασίες επίλυσης διαφορών

Σε περίπτωση καταγγελίας ή διαφωνίας σε σχέση με ή σύμφωνα με την ερμηνεία της παρούσας ΠΠ/ΔΔΠ και τη λειτουργία της Αρχής Πιστοποίησης ΑΠΘ, ο ενδιαφερόμενος συνδρομητής μπορεί να απευθυνθεί

στην Επιτροπή Υποδομής Δημοσίου Κλειδιού ΑΠΘ και θα προσπαθήσει να επιλύσει ή να συμβιβάσει τη διαφωνία με αμοιβαία αποδεκτό τρόπο πριν προχωρήσουν νομικές διαδικασίες. Η Επιτροπή Υποδομής Δημοσίου Κλειδιού ΑΠΘ είναι υπεύθυνη για τη διερεύνηση όλων των περιστατικών παραπόνων και διαφωνιών σε σχέση με την παροχή των υπηρεσιών εμπιστοσύνης. Δείτε επίσης την ενότητα 3.1.6.

Σε περίπτωση μη επίλυσης διαφωνίας με αμοιβαία αποδεκτό τρόπο, οποιεσδήποτε διαφωνίες προκύπτουν σε σχέση με την παρούσα ΠΠ/ΔΔΠ της ΑΠ ΑΠΘ, θα υποβληθούν για επίλυση σε Ελληνικά Δικαστήρια. Αρμόδια ορίζονται τα δικαστήρια της Θεσσαλονίκης.

9.14 Ισχύουσα νομοθεσία

Ισχύουν οι διατάξεις της ενότητας 9.14 της ΠΠ/ΔΔΠ της HARICA.

9.15 Συμμόρφωση με την κείμενη νομοθεσία

Ισχύουν οι διατάξεις της ενότητας 9.15 της ΠΠ/ΔΔΠ της HARICA.

9.16 Διάφορες Παροχές – Δεσμεύσεις

Ισχύουν οι διατάξεις της ενότητας 9.16 της ΠΠ/ΔΔΠ της HARICA.

10 ΠΑΡΑΡΤΗΜΑ Α (ΚΕΝΤΡΙΚΗ ΑΠ ΑΠΘ)

```
=== BEGIN AUTH CENTRAL CA R5 ===

Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            18:dd:87:ae:1f:4b:b6:79
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=GR, O=Hellenic Academic and Research Institutions Cert. Authority, CN=Hellenic Academic
and Research Institutions RootCA 2011
        Validity
            Not Before: May  5 13:35:54 2015 GMT
            Not After : May  3 13:35:54 2023 GMT
        Subject: C=GR, O=Aristotle University of Thessaloniki, CN=Aristotle University of Thessaloniki
Central CA R5
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:e3:bc:e8:96:27:d8:2f:a2:0e:89:1c:ac:71:7c:
                    2f:c2:7d:a8:a5:29:2a:72:a4:a0:67:eb:63:3c:33:
                    74:a3:cc:a5:89:f1:5d:3c:80:f1:ea:b0:60:bc:8e:
                    99:cd:90:2e:70:f8:8a:45:08:90:dc:cd:37:8e:4d:
                    50:03:98:96:5a:ca:b3:f7:7b:34:dc:25:0b:f6:87:
                    b6:8f:25:9e:a5:ad:ea:61:f8:6c:d7:49:ce:65:a6:
                    f1:a4:6f:cf:ad:73:40:cb:a2:0c:98:35:1c:ad:42:
                    ab:9c:47:b6:7c:0c:08:59:07:ed:eb:4b:6f:33:14:
                    b3:a4:e1:8c:3f:f1:2a:1d:e3:54:45:53:9b:1c:bf:
                    87:74:6d:3c:e4:b6:3b:ec:01:c1:94:91:69:57:63:
                    6a:e9:e1:03:f9:66:04:8d:68:7e:91:1e:b2:cb:6d:
                    28:d2:a2:dd:aa:1d:52:18:42:8c:c3:59:33:c9:1b:
                    43:22:2b:24:8b:cb:60:fb:9e:32:ec:5a:ab:80:19:
                    bb:97:a4:d9:eb:88:9c:7b:23:b2:31:ea:fa:cd:bf:
                    1c:9e:ee:35:7a:33:ba:9c:cd:0d:6c:27:c4:13:3f:
                    ad:2e:ec:59:03:82:31:6d:c9:d0:37:59:37:2d:19:
                    a9:46:a7:45:95:30:86:da:f2:6f:c4:cf:f2:98:d7:
                    72:29
```

```
            Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                74:91:84:CD:8F:9B:C5:C8:FB:3E:A3:74:F2:4E:74:BB:F9:9A:EE:46
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crlv1.harica.gr/HaricaRootCA2011/crlv1.der.crl

            X509v3 Authority Key Identifier:
                keyid:A6:91:42:FD:13:61:4A:23:9E:08:A4:29:E5:D8:13:04:23:EE:41:25

            Authority Information Access:
                OCSP - URI:http://ocsp.harica.gr
                CA Issuers - URI:http://www.harica.gr/certs/HaricaRootCA2011.crt

            X509v3 Certificate Policies:
                Policy: 1.3.6.1.4.1.7709.2.0.3.6
                  CPS: http://www.pki.auth.gr/documents/CPS.php
                  User Notice:
                    Organization: Hellenic Academic and Research Institutions Certification Authority
                    Number: 1
                    Explicit Text: This certificate is subject to Greek laws and our CPS. This Certificate
must only be used for academic, research or educational purposes.

            X509v3 Name Constraints:
                Permitted:
                  DNS:auth.gr
                  email:auth.gr
                  email:.auth.gr

    Signature Algorithm: sha256WithRSAEncryption
        a6:4b:c3:e8:7a:ef:1b:cc:51:7a:65:ee:94:3e:70:7e:72:07:
        b6:a4:94:87:a7:dc:48:9c:6f:ca:f0:19:95:46:5f:ae:c9:46:
        8c:18:76:27:37:49:21:e1:8f:74:1f:55:4a:ea:63:e3:d0:e0:
        3c:14:2a:23:e1:9b:c3:c2:af:4a:e5:05:2f:fe:b9:8d:f2:35:
        84:fe:ff:e8:a9:4a:35:64:bb:97:fd:fc:06:be:e0:59:7f:93:
        23:f9:54:ad:11:0d:c3:13:25:17:1a:40:ea:1a:ff:14:6e:f7:
        83:2c:bc:20:f5:bc:cc:e5:b4:e7:ec:6e:b6:82:b9:8c:ae:9e:
        bf:19:c3:50:5f:ad:c8:23:13:77:2e:3e:9d:7d:5d:67:b5:a8:
        89:1e:a3:be:a3:b6:e4:fe:6f:90:1c:07:22:be:a3:90:ed:ee:
        44:cb:ae:cf:0c:d4:10:8c:7d:dd:35:12:a0:0d:d9:68:0e:5b:
        67:05:44:5a:72:d2:77:0d:e1:6e:c1:c3:85:6f:6e:7d:04:a6:
        1b:2c:33:22:bd:58:fb:38:c5:24:3e:75:4e:40:03:6a:a7:01:
        16:bc:f8:c3:39:44:43:58:db:77:ba:ad:f8:f8:e9:c1:e3:d2:
        58:41:4c:ed:b1:fd:f8:b2:6a:20:aa:1e:ae:ad:03:f9:3b:38:
        12:60:dd:f1
=== END AUTH CENTRAL CA R5 ===
```

11 ΠΑΡΑΡΤΗΜΑ Β (Περιγράμματα Πιστοποιητικών ΥΔΚ ΑΠΘ)

Χρησιμοποιούνται τα περιγράμματα που ορίζονται στο Παράρτημα Β της ΠΠ/ΔΔΠ της HARICA.