Υποδομή Δημοσίου Κλειδιού του Τμήματος Φυσικής Α.Π.Θ.

ΠΟΛΙΤΙΚΗ ΠΙΣΤΟΠΟΙΗΣΗΣ ΚΑΙ ΔΗΛΩΣΗ ΔΙΑΔΙΚΑΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ

ΕΚΔΟΣΗ 2.0

Μάρτιος 2009

Πίνακας Περιεχομένων

1 ΕΙΣΑΓΩΓΗ

1.1 Επισκόπηση

Το παρόν έγγραφο καθορίζει την πολιτική και τις διαδικασίες πιστοποίησης που ακολουθούνται από την Αρχή Πιστοποίησης (ΑΠ) της Υποδομής Δημοσίου Κλειδιού (ΥΔΚ) του Τμήματος Φυσικής του Αριστοτέλειου Πανεπιστημίου Θεσσαλονίκης (ΤΦ-ΑΠΘ).

Η ΥΔΚ του Τμήματος Φυσικής ΑΠΘ ξεκίνησε τη λειτουργία της ως ανεξάρτητη αρχή το 2002 ιδρύοντας την πρώτη ΑΠ του Τμήματος Φυσικής ΑΠΘ (PhysNet-CA).

Από το 2009 η ΑΠ του Τμήματος Φυσικής ΑΠΘ συμμετέχει σε σχήμα εμπιστοσύνης υπό την Κεντρική Αρχή Πιστοποίησης του Α.Π.Θ. (AUTH-CENTRAL-CA) η οποία με τη σειρά της συμμετέχει στο ευρύτερο σχήμα εμπιστοσύνης υπό την «Αρχή Πιστοποίησης Ελληνικών Ακαδημαϊκών και Ερευνητικών Ιδρυμάτων» (Hellenic Academic & Research Institutions Certification Authority – HARICA).

Το παρόν κείμενο, ακολουθεί τη δομή που ορίζεται στο RFC 3647.

1.2 Ονομασία και ταυτότητα εγγράφου

- Τίτλος Εγγράφου: **"Υποδομή Δημοσίου Κλειδιού του Τμήματος Φυσικής Α.Π.Θ. : Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης. "**
- Έκδοση: **2.0**
- Ημερομηνία Έκδοσης: **10 Μαρτίου 2009**
- O.I.D.: **1.3.6.1.4.1.13089.2.1.2.0**

Ο παγκόσμια μοναδικός Αριθμός Αναγνώρισης (OID) αυτού του εγγράφου είναι:

1.3.6.1.4.1.13089	Αριθμός Αναγνώρισης (OID) του Τμήματος Φυσικής ΑΠΘ, καταχωρημένος από τον οργανισμό IANA (www.iana.org)
2	Υποδομή Δημοσίου Κλειδιού (Public Key Infrastructure, PKI)
1	Αρχή Πιστοποίησης Τμήματος Φυσικής ΑΠΘ
2.0	Πρώτο και δεύτερο ψηφίο του αριθμού έκδοσης (version) της Πολιτικής Πιστοποίησης

1.3 Συμμετέχοντες στην Υποδομή Δημοσίου Κλειδιού

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

1.3.1 Αρχές Πιστοποίησης

Οι Αρχές Πιστοποίησης είναι οι οντότητες της Υποδομής Δημόσιου Κλειδιού που εκδίδουν τα πιστοποιητικά.

Η ΑΠ του Τμήματος Φυσικής λειτουργεί στο Υπολογιστικό Κέντρο του Τμήματος Φυσικής

Το πιστοποιητικό της Αρχής Πιστοποίησης του Τμήματος Φυσικής Α.Π.Θ. υπογράφεται από την Κεντρική Αρχή Πιστοποίησης του Α.Π.Θ. (AUTH-CENTRAL-CA)

1.3.2 Αρχές Καταχώρησης (ΑΚ)

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 Υπολογιστικό Κέντρο του Τμήματος Φυσικής, λειτουργεί ως ΑΚ της ΥΔΚ του Τμήματος Φυσικής Α.Π.Θ.

1.3.3 Συνδρομητές

Συνδρομητές δυνάμενοι να πιστοποιούνται από την ΑΠ του Τμήματος Φυσικής Α.Π.Θ. είναι :

1. φυσικά πρόσωπα σχετιζόμενα με το Τμήμα Φυσικής του Αριστοτέλειου Πανεπιστήμιου Θεσσαλονίκης
2. εξυπηρετητές, δυνάμενοι να επιτελέσουν κρυπτογραφικές διεργασίες, οι όποιες χρησιμοποιούνται σε δραστηριότητες με έμμεση ή άμεση ανάμιξη του Τμήματος Φυσικής του Αριστοτέλειου Πανεπιστήμιου Θεσσαλονίκης
3. υπηρεσίες που λειτουργούν σε εξυπηρετητές, οι όποιες χρησιμοποιούνται σε δραστηριότητες με έμμεση ή άμεση ανάμιξη του Τμήματος Φυσικής του Αριστοτέλειου Πανεπιστήμιου Θεσσαλονίκης

1.3.4 Υποστηριζόμενες Οντότητες

Οι υποστηριζόμενες οντότητες (Relying Parties) των υπηρεσιών πιστοποίησης μπορεί να είναι οποιεσδήποτε οντότητες, φυσικά ή νομικά πρόσωπα, εντός ή εκτός της ελληνικής ακαδημαϊκής κοινότητας, οι οποίες χρησιμοποιούν κατ' οποιονδήποτε τα ψηφιακά πιστοποιητικά, ψηφιακές υπογραφές, χρονοσφραγίδες κλπ) και επαφίενται στις πληροφορίες που περιέχουν.

Οι οντότητες που εμπιστεύονται την Υπηρεσία Πιστοποίησης οφείλουν αφού συμφωνήσουν με τους όρους που περιγράφονται στο παρόν κείμενο και επαληθεύσουν την εγκυρότητα ενός πιστοποιητικού που έχει εκδοθεί από την ΑΠ του Τμήματος Φυσικής να αποφασίσουν αν θα θεωρήσουν έγκυρο το περιεχόμενο του ψηφιακού πιστοποιητικού. Για την επαλήθευση της εγκυρότητας ενός πιστοποιητικού, ο χρήστης θα πρέπει να ελέγξει ότι:

- Βρίσκεται εντός της περιόδου ισχύος του, δηλαδή έχει ξεκινήσει και δεν έχει λήξει η ισχύς του,
- Είναι έγκυρα υπογεγραμμένο από έμπιστη Αρχή Πιστοποίησης
- Δεν έχει ανακληθεί για οποιοδήποτε λόγο,
- Τα στοιχεία ταυτότητας του υποκειμένου που περιέχει ταιριάζουν με τα στοιχεία που παραθέτει ο υπογράφων,
- Η χρήση για την οποία υποβάλλεται το πιστοποιητικό συμφωνεί με την χρήση για την οποία έχει εκδοθεί από την ΑΠ,
- Ακολουθούνται οι όροι και οι συνθήκες που περιγράφονται στο παρόν κείμενο.

1.3.5 Άλλοι συμμετέχοντες

Δεν ορίζεται

1.4 Χρήση πιστοποιητικών

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

Η κατοχή ενός πιστοποιητικού της ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν συνεπάγεται απαραίτητα πρόσβαση σε κανένα είδος πόρων.

1.4.1 Επιτρεπόμενες χρήσεις των πιστοποιητικών

Τα πιστοποιητικά που εκδίδονται από την ΑΠ του Τμήματος Φυσικής Α.Π.Θ. ισχύουν μόνο στα πλαίσια των ακαδημαϊκών δραστηριοτήτων.

Ενδεικτικές εφαρμογές στις οποίες μπορούν να χρησιμοποιηθούν τα ψηφιακά πιστοποιητικά που εκδίδονται από την ΑΠ του Τμήματος Φυσικής Υπηρεσία είναι οι ακόλουθες:

α) Στην υπογραφή ενός «ηλεκτρονικού εγγράφου» από ένα φυσικό πρόσωπο με τη χρήση του ψηφιακού πιστοποιητικού του.

β) Στην υπογραφή «μηνυμάτων ηλεκτρονικού ταχυδρομείου», για την εξασφάλιση της αυθεντικότητας της διεύθυνσης ηλεκτρονικού ταχυδρομείου του αποστολέα., καθώς επίσης και στην αποστολή «ασφαλών αποδείξεων παραλαβής μηνυμάτων».

γ) Στην «ισχυρή απόδειξη της ταυτότητας» (Strong Authentication) ενός φυσικού προσώπου ή μιας συσκευής κατά την επικοινωνία τους με άλλες οντότητες, εξασφαλίζοντας επιπλέον χαρακτηριστικά ασφάλειας, ισχυρότερα από αυτά που παρέχει η κλασική μέθοδος πρόσβασης με συνθηματικό χρήστη.

δ) Στην «κρυπτογράφηση εγγράφων και μηνυμάτων» με την χρήση του δημοσίου κλειδιού κάποιας οντότητας, εξασφαλίζοντας ότι μόνο ο επιδιωκόμενος παραλήπτης και κάτοχος του αντίστοιχου ιδιωτικού κλειδιού μπορεί να αποκρυπτογραφήσει και να διαβάσει το έγγραφο ή το μήνυμα.

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

1.4.2 Απαγορευμένες χρήσεις των πιστοποιητικών

Οποιοδήποτε άλλη χρήση όπως εμπορικές ή οικονομικές συναλλαγές απαγορεύεται αυστηρά.

1.5 Πολιτική διοίκησης

1.5.1 Οργανισμός διαχείρισης του εγγράφου

Το κείμενο Πολιτικής και Δήλωσης Διαδικασιών της ΑΠ του Τμήματος Φυσικής Α.Π.Θ. διαχειρίζεται από το υπολογιστικό κέντρο του Τμήματος Φυσικής Α.Π.Θ.

Η διεύθυνση της ΑΠ του Τμήματος Φυσικής Α.Π.Θ. για λειτουργικά ζητήματα είναι :

Αρχή Πιστοποίησης Τμήματος Φυσικής Α.Π.Θ.
Τμήμα Φυσικής
Κτήριο 22d
Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
Πανεπιστημιούπολη
54124 Θεσσαλονίκη
ΕΛΛΑΣ

Τηλέφωνο: (+ 30) 231 099 8223
Fax: (+ 30) 231 099 4309
E-mail: pki@physics.auth.gr

1.5.2 Προσωπικό Επικοινωνίας

Το προσωπικό επικοινωνίας για ερωτήσεις περί του παρόντος εγγράφου, ή για οποιοδήποτε άλλο ζήτημα σχετικό με την ΑΠ του Τμήματος Φυσικής Α.Π.Θ. Είναι:

Τριαντάφυλλος Χατζηαντωνίου
Τμήμα Φυσικής
Κτήριο 22d
Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
Πανεπιστημιούπολη
54124 Θεσσαλονίκη
ΕΛΛΑΣ

Τηλέφωνο: (+ 30) 231 099 8223
Fax: (+ 30) 231 099 4309
E-mail: daffy@physics.auth.gr

1.5.3 Προσωπικό υπεύθυνο για τον καθορισμό της καταλληλότητας των διαδικασιών και της πολιτικής

Το προσωπικό που είναι υπεύθυνο για τον καθορισμό καταλληλότητας Πολιτικής Πιστοποίησης (Certification Policy, CP) των διαδικασιών και της πολιτικής της Α.Π. του Τμήματος Φυσικής Α.Π.Θ. Είναι :

Τριαντάφυλλος Χατζηαντωνίου
Τμήμα Φυσικής
Κτήριο 22d
Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
Πανεπιστημιούπολη
54124 Θεσσαλονίκη
ΕΛΛΑΣ

Τηλέφωνο: (+ 30) 231 099 8223
Fax: (+ 30) 231 099 4309
E-mail: daffy@physics.auth.gr

1.5.4 Επικαιροποίηση του κειμένου Πολιτικής και Δήλωσης Διαδικασιών

Κάθε αλλαγή του παρόντος κειμένου θα συνοδεύεται με αλλαγή του ΑΑ

1.6 Ορισμοί και ακρωνύμια

Ελληνικός όρος	***Ακρωνύμιο***	***Αγγλικός όρος***	***Ακρωνύμιο***
Αναγνώριση		Identification	
Απόδειξη ταυτότητας		Authentication	
Αποθήκη Δεδομένων		Data Repository	
Αριθμός Αναγνώρισης Εγγράφου	ΑΑ	Object Identification Number	OID
Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης	ΑΠΘ		ΑΠΘ
Αρχή Καταχώρησης	ΑΚ	Registration Authority	RA
Αρχή Πιστοποίησης	ΑΠ	Certification Authority	CA
Αρχή Πιστοποίησης Τμήματος Φυσικής Α.Π.Θ.	PhysNet-CA	School of Physics Certification Authority	PhysNet-CA
Ψηφιακό Πιστοποιητικό		Digital Certificate	
Δήλωση Διαδικασιών Πιστοποίησης	ΔΔΠ	Certification Practice Statement	CPS

Ελληνικός όρος	***Ακρωνύμιο***	***Αγγλικός όρος***	***Ακρωνύμιο***
Δημόσιο Κλειδί		Public Key	
Διακεκριμένο Όνομα	ΔΟ	Distinguished Name	DN
Εξυπηρετητή			
Ιδιωτικό Κλειδί		Private Key	
Κεντρική Αρχή Πιστοποίησης ΑΠΘ	AUTH-CENTRAL-CA		AUTH-CENTRAL-CA
κλειδιού			
Κοινό Όνομα	ΚΟ	Common Name	CN
κρυπτογραφίας δημοσίου		Standards	
Κρυπτογραφικά πρότυπα		Public-Key Cryptography	PKCS
Λίστα Ανάκλησης Πιστοποιητικών	ΛΑΠ	Certificate Revocation List	CRL
Όνομα Οργανισμού		OrganizationName	O
Όνομα Χώρας		CountryName	C
Οργανωτική Μονάδα		Organizational Unit	OU
Πιστοποιητικό		Certificate	
Πολιτική Πιστοποίησης	ΠΠ	Certificate Policy	CP
Συνδρομητής		Subscriber	
Υποδομή Δημοσίου Κλειδιού	ΥΔΚ	Public Key Infrastructure	PKI
Υποκείμενο Πιστοποιητικού		Certificate Subject	
Υπολογιστικό Κέντρο ΤΦ-ΑΠΘ	ΥΚ-ΤΦ-ΑΠΘ		ΥΚ-ΤΦ-ΑΠΘ
Υποστηριζόμενη Οντότητα		Relying Party	
Ψηφιακό Πιστοποιητικό		Certification Authority	
Ψηφιακό Πιστοποιητικό		Server Digital Certificates	
Ψηφιακό Πιστοποιητικό Φυσικού Προσώπου		Personal Identity Digital Certificate	
		Domain Name System	DNS
		Fully Qualified Domain Name	FQDN

2 ΕΥΘΥΝΗ ΔΗΜΟΣΙΟΠΟΙΗΣΗΣ ΚΑΙ ΑΠΟΘΗΚΕΥΣΗΣ

2.1 Μηχανισμοί Αποθήκευσης

Η ΑΠ του Τμήματος Φυσικής ΑΠΘ διαθέτει κεντρική αποθήκη δεδομένων όπου αποθηκεύονται τα κείμενα πολιτικής, πιστοποιητικά Αρχών Πιστοποίησης και τελικά πιστοποιητικά συνδρομητών/συσκευών

Όλοι οι on-line και off-line μηχανισμοί αποθήκευσης της ΑΠ του Τμήματος Φυσικής Α.Π.Θ. διαχειρίζονται από το Υπολογιστικό Κέντρο του Τμήματος Φυσικής του Αριστοτέλειου Πανεπιστήμιου Θεσσαλονίκης.

Η διεύθυνση επικοινωνίας της ΑΠ του Τμήματος Φυσικής Α.Π.Θ. για ζητήματα σχετικά με τους μηχανισμούς αποθήκευσης είναι :

ΑΡΧΗ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΜΗΜΑΤΟΣ ΦΥΣΙΚΗΣ Α.Π.Θ.
Τμήμα Φυσικής
Κτήριο 22d
Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης
Πανεπιστημιούπολη
54124 Θεσσαλονίκη
ΕΛΛΑΣ

Τηλέφωνο: (+ 30) 231 099 8223
Fax: (+ 30) 231 099 4309
Email: pki@physics.auth.gr

2.2 Δημοσιοποίηση της πληροφορίας πιστοποίησης

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. είναι υποχρεωμένη να συντηρεί μια on-line αποθήκη, διαθέσιμη σε όλα τα εμπλεκόμενα μέλη μέσω ιστοσελίδας του παγκόσμιου δικτυακού ιστού (www) στην διεύθυνση : http://pki.physics.auth.gr στην οποία περιέχονται :

1. το πιστοποιητικό του κλειδιού υπογραφής της ΑΠ του Τμήματος Φυσικής Α.Π.Θ.
2. τον τελευταίο κατάλογο πιστοποιητικών που έχουν ανακληθεί (CRL)
3. αντίγραφο της τελευταίας έκδοσης του παρόντος εγγράφου της Πολιτικής Πιστοποίησης και Δήλωσης των Διαδικασιών Πιστοποίησης (CP/CPS)
4. οποιαδήποτε άλλη πληροφορία σχετική με πιστοποιητικά που αναφέρονται στην συγκεκριμένη πολιτική.

2.3 Χρόνος ή συχνότητα δημοσιοποίησης

Όλες οι προς δημοσιοποίηση πληροφορίες στην αποθήκη θα δημοσιοποιούνται ευθύς ως καθίστανται διαθέσιμες στην ΑΠ. Πληροφορία σχετική με την ανάκληση ενός πιστοποιητικού θα δημοσιοποιούνται όπως περιγράφεται στην παράγραφο 4.9.7 του παρόντος.

2.4 Έλεγχος πρόσβασης στα αποθηκευτικά μέσα

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν επιβάλλει οποιουσδήποτε περιορισμούς πρόσβασης στις πληροφορίες που είναι διαθέσιμες στην ιστοσελίδα της, που περιλαμβάνει το πιστοποιητικό της ΑΠ, τον πιο πρόσφατο κατάλογο πιστοποιητικών που έχουν ανακληθεί (CRL) και ένα αντίγραφο του παρόντος εγγράφου που περιγράφει την πολιτική και τις διαδικασίες πιστοποίησης (CP/CPS).

Η ΑΠ του Τμήματος Φυσικής μπορεί να επιβάλει περιορισμένη πρόσβαση στην αποθήκη κατά την κρίση των διαχειριστών της ΥΔΚ του Τμήματος Φυσικής, για λόγους προστασίας της διαθεσιμότητάς της από επιθέσεις.

Η ιστοσελίδα της ΑΠ του Τμήματος Φυσικής Α.Π.Θ. συντηρείται με στόχο την μέγιστη διαθεσιμότητά της. Εξαιρώντας το κλείσιμο για λόγους συντήρησης καθώς και απρόβλεπτα περιστατικά, η ιστοσελίδα πρέπει να είναι διαθέσιμη σε εικοσιτετράωρη βάση, επί επταήμερο την εβδομάδα.

3 ΑΝΑΓΝΩΡΙΣΗ ΚΑΙ ΑΠΟΔΕΙΞΗ ΤΑΥΤΟΤΗΤΑΣ

3.1 Ονοματολογία

Τα ονόματα υποκειμένων των υποψηφίων πιστοποιητικών θα ακολουθούν τα πρότυπα X.500:

3.1.1 Τύποι ονομάτων

3.1.1.1 Πιστοποιητικά φυσικών προσώπων

Στα πιστοποιητικά φυσικών προσώπων το όνομα του υποκειμένου πρέπει να συμπεριλαμβάνει το διακεκριμένο ονοματεπώνυμο στα λατινικά του φυσικού προσώπου στο πεδίο "CN", το όνομα του οργανισμού στο πεδίο "o" (o=Aristotle University of Thessaloniki) και το διακεκριμένο όνομα της μονάδας σε πεδίο "ou" (ou=School of Physics). Επίσης, στο πεδίο "emailAddress" θα υπάρχει κατ' ελάχιστο μία διεύθυνση e-mail που θα ανήκει στο υποκείμενο, με επίθεμα "@physics.auth.gr"

3.1.1.2 Πιστοποιητικά συσκευών

Στα πιστοποιητικά συσκευών το όνομα υποκειμένου πρέπει να συμπεριλαμβάνει το πλήρες διακεκριμένο όνομα της συσκευής κατά την υπηρεσία ονοματολογίας (DNS FQDN) στο πεδίο "CN" (με επίθεμα το domain "physics.auth.gr"), το διακεκριμένο όνομα του οργανισμού στο πεδίο "o" (o=Aristotle University of Thessaloniki) και το διακεκριμένο όνομα της μονάδας σε πεδίο "ou" (ou=School of Physics). Επίσης, στο πεδίο "emailAddress" θα υπάρχει κατ' ελάχιστο μία διεύθυνση e-mail που θα ανήκει στον διαχειριστή του υποκειμένου, με επίθεμα "auth.gr".

3.1.1.3 Πιστοποιητικά υπηρεσιών

Στα πιστοποιητικά υπηρεσιών το όνομα υποκειμένου πρέπει να συμπεριλαμβάνει το πλήρες διακεκριμένο όνομα της υπηρεσίας κατά την υπηρεσία ονοματολογίας (DNS FQDN) στο πεδίο "CN" (με επίθεμα το domain "physics.auth.gr"), το διακεκριμένο όνομα του οργανισμού στο πεδίο "o" (o=Aristotle University of Thessaloniki) και το διακεκριμένο όνομα της μονάδας σε πεδίο "ou" (ou=School of Physics). Επίσης, στο πεδίο "emailAddress" θα υπάρχει κατ' ελάχιστο μία διεύθυνση e-mail που θα ανήκει στον διαχειριστή του υποκειμένου, με επίθεμα "auth.gr".

3.1.2 Υποχρέωση τα ονόματα να έχουν νόημα

Τα ονόματα υποκειμένων πρέπει να αντιπροσωπεύουν τον συνδρομητή κατά τέτοιο τρόπο ώστε να είναι ευνόητα από τους ανθρώπους και πρέπει να έχουν μια λογική σχέση με το πιστοποιούμενο όνομα του συνδρομητή.

3.1.3 Ανωνυμία ή ψευδωνυμία των συνδρομητών

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν εκδίδει ή υπογράφει ανώνυμα ή ψευδώνυμα πιστοποιητικά.

3.1.4 Κανόνες σύνταξης των ονομάτων

Επιτρεπτοί χαρακτήρες: a-z A-Z 0-9 . , ( ) / = : κενά διαστήματα.

Η κωδικοποίηση των χαρακτήρων πρέπει να είναι μία από τις παρακάτω:

- PrintableString
- T61String
- IA5String

Βλέπε επίσης παράγραφο 3.1.1

3.1.5 Μοναδικότητα ονομάτων

Το όνομα υποκειμένου που αναγράφεται σε ένα πιστοποιητικό πρέπει να είναι σαφές και μοναδικό μεταξύ όλων των πιστοποιητικών που εκδίδονται από την ΑΠ του Τμήματος Φυσικής Α.Π.Θ. Σε περίπτωση πιστοποιητικών φυσικών προσώπων, επιπλέον αριθμοί ή γράμματα θα προστίθενται στο πραγματικό όνομα έτσι ώστε να διασφαλίζεται η μοναδικότητα του ονόματος μεταξύ των πιστοποιητικών που έχουν εκδοθεί από την ΑΠ του Τμήματος Φυσικής Α.Π.Θ.

3.1.6 Διαδικασία επίλυσης διαφορών σχετικά με την κυριότητα ονόματος και τον ρόλο των εμπορικών σημάτων.

Αρμόδιο για θέματα επίλυσης διαφορών σχετικά με την κυριότητα ονομάτων στην ΥΔΚ του Τμήματος Φυσικής ΑΠΘ είναι το Διοικητικό συμβούλιο του Τμήματος και σε αδυναμία του το Πρυτανικό συμβούλιο του ΑΠΘ.

3.2 Αρχική επαλήθευση ταυτότητας

3.2.1 Μέθοδος απόδειξης κατοχής κλειδιού

Η ΑΚ του Τμήματος Φυσικής Α.Π.Θ. ελέγχει την κατοχή του ιδιωτικού κλειδιού που σχετίζεται με το εκάστοτε αίτημα έκδοσης πιστοποιητικού, κατά την διάρκεια της αρχικής επαλήθευσης της ταυτότητας. Ο αιτών θα πρέπει να υπογράψει το αίτημα έκδοσης πιστοποιητικού (ή ένα οποιοδήποτε ηλεκτρονικό μήνυμα που θα αποστείλει προς την ΥΔΚ του Τμήματος Φυσικής) με το ιδιωτικό κλειδί του αιτούντος. Η εγκυρότητα της υπογραφής με βάση το δημόσιο κλειδί που εμπεριέχεται στο αίτημα επιβεβαιώνει την κατοχή του ιδιωτικού κλειδιού.

3.2.2 Απόδειξη της ταυτότητας του οργανισμού:

Η Αρχή Καταχώρισης πρέπει να επιβεβαιώνει ότι ο συνδρομητής σχετίζεται με το Τμήμα Φυσικής του Αριστοτελείου Πανεπιστήμιου Θεσσαλονίκης, το όνομα του οποίου περιλαμβάνεται στο πιστοποιητικό.

Ο συνδρομητής πρέπει να προσκομίσει:

α) επίσημο πιστοποιητικό στο οποίο βεβαιώνεται η σχέση του με το Τμήμα Φυσικής ή

β) θεωρημένο έγγραφο από τη Γραμματεία του Τμήματος Φυσικής το οποίο επιβεβαιώνει τη σχέση του συνδρομητή με το Τμήμα Φυσικής.

3.2.3 Επικύρωση μεμονωμένης ταυτότητας

- **Φυσικά Πρόσωπα:** Το υποκείμενο πρέπει να έλθει σε προσωπική επαφή με την ΑΚ του Τμήματος Φυσικής Α.Π.Θ. με σκοπό τον έλεγχο της ταυτότητός του και της εγκυρότητας της αίτησης. Η υπαγόμενη επικύρωση επιτελείται δια της παρουσίασης ενός έγκυρου εγγράφου που φέρει φωτογραφία του αιτούντος (δελτίο Αστυνομικής ταυτότητας, διαβατήριο, δίπλωμα οδήγησης, Βιβλιάριο Σπουδών, φοιτητική ταυτότητα). Για την αποστολή ηλεκτρονικής αίτησης έκδοσης ψηφιακών πιστοποιητικών το υποκείμενο μπορεί να χρησιμοποιήσει οποιοδήποτε ιδρυματικό λογαριασμό ηλεκτρονικής αλληλογραφίας διαθέτει (π.χ. *user*@physics.auth.gr ή *user*@auth.gr).
- **Ψηφιακή οντότητα ή Υπηρεσία:** Η οντότητα πρέπει να διαθέτει ήδη μια έγκυρη καταχώρηση στο DNS κάτω από τη ζώνη "physics.auth.gr" και να είναι μέρος της ηλεκτρονικής υποδομής του Τμήματος Φυσικής.

3.2.4 Μη ελεγμένες πληροφορίες συνδρομητή

Τα πιστοποιητικά που εκδίδονται δεν περιλαμβάνουν μη επιβεβαιωμένα στοιχεία του συνδρομητή.

3.2.5 Επικύρωση ιδιότητας αιτούμενου

Ο συνδρομητής που ζητά την υπηρεσία από την ΑΠ του Τμήματος Φυσικής Α.Π.Θ., πρέπει να παρουσιάσει έγκυρα έγγραφα που αποδεικνύουν τη σχέση του με το Τμήμα Φυσικής Α.Π.Θ.

3.2.6 Κριτήρια διαλειτουργικότητος

Δεν ορίζεται.

3.3 Ταυτοποίηση και επικύρωση για αιτήσεις επανέκδοσης κλειδιών

3.3.1 Ταυτοποίηση και επικύρωση επανέκδοσης κλειδιών, ρουτίνας

Ο χρήστης μπορεί να αιτηθεί επανέκδοση κλειδιού πριν από τη λήξη του μέσω ψηφιακά υπογεγραμμένου e-mail με το τρέχον ισχύον πιστοποιητικό του. Η επανέκδοση κλειδιού μετά από τη λήξη του, ακολουθεί την ίδια διαδικασία επικύρωσης με αυτήν του νέου πιστοποιητικού.

3.3.2 Επαλήθευση ταυτότητας και επικύρωση αίτησης επανέκδοσης κλειδιών κατόπιν ανάκλησης

Ένα ανακληθέν κλειδί δεν δύναται να επικυρωθεί ξανά. Η επικύρωση ενός νέου αιτήματος πιστοποιητικού ακολουθεί τους κανόνες που καθορίζονται στις παραγράφους 3.2.2 και 3.2.3 .

3.4 Επαλήθευση ταυτότητας για αίτημα ανάκλησης

Αιτήματα ανάκλησης πιστοποιητικών πρέπει να υποβάλλονται μέσω ηλεκτρονικού ταχυδρομείου στη διεύθυνση pki@physics.auth.gr. Σε περίπτωση που το αίτημα ανάκλησης είναι για πιστοποιητικό φυσικού προσώπου, το e-mail πρέπει να υπογράφεται από το ιδιωτικό κλειδί που αντιστοιχεί στο προς ανάκληση πιστοποιητικό, το οποίο πρέπει να έχει ισχύ, να μην έχει λήξει και να μην έχει ανακληθεί από την ΑΠ του Τμήματος Φυσικής Α.Π.Θ.

Για αιτήματα ανάκλησης πιστοποιητικών Η/Υ ή υπηρεσιών, το e-mail πρέπει να υπογράφεται από το ιδιωτικό κλειδί που αντιστοιχεί στο πιστοποιητικό του φυσικού προσώπου που είναι υπεύθυνο για τον Η/Υ ή την υπηρεσία. Εάν η δυνατότητα ηλεκτρονικού ταχυδρομείου δεν είναι δυνατή, τότε το αίτημα πιστοποιείται σύμφωνα με τη διαδικασία που περιγράφεται στην παράγραφο 3.2.3 .

4 ΛΕΙΤΟΥΡΓΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ, ΚΥΚΛΟΣ ΖΩΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

4.1 Αίτημα πιστοποιητικών

4.1.1 Ποιος έχει δικαίωμα υποβολής αιτήματος έκδοσης πιστοποιητικού

Το υποκείμενο πρέπει :

1. να είναι αποδεκτός συνδρομητής, όπως περιγράφεται στην παράγραφο 1.3.3
2. να διάβασε και να αποδέχεται τις πολιτικές και τις διαδικασίες που περιγράφονται στο παρόν έγγραφο
3. να χρησιμοποιεί ασφαλή κωδικό ενεργοποίησης για το προσωπικό του κλειδί.

4.1.2 Ποια είναι η διαδικασία κατάθεσης αιτήματος για έκδοση πιστοποιητικού

Το Διακεκριμένο Όνομα του πιστοποιητικού του αιτούντος πρέπει να είναι σύμφωνο με όσα αναφέρονται στην παράγραφο 3.2 . Η πιστοποίηση της ταυτότητας του χρήστη πρέπει να έχει γίνει σύμφωνα με όσα ορίζονται στο κεφάλαιο 3. Ο συνδρομητής καταθέτει την αίτηση έκδοσης πιστοποιητικού με ηλεκτρονικό ταχυδρομείο στη διεύθυνση pki@physics.auth.gr .

4.2 Διαδικασία επεξεργασίας αιτημάτων πιστοποιητικών

4.2.1 Διαδικασίες ελέγχου της ταυτότητος και ιδιότητας του αιτούντος

Όλα τα αιτήματα έκδοσης πιστοποιητικών θα ελέγχονται από την Αρχή Καταχώρησης του Τμήματος Φυσικής Α.Π.Θ. Κατόπιν έγκρισης, το αίτημα πιστοποιητικού θα διαβιβάζεται στην ΑΠ προκειμένου να εκδοθεί το τελικό πιστοποιητικό.

4.2.2 Έγκριση ή απόρριψη έκδοσης πιστοποιητικών

Οι διαδικασίες που πρέπει να ακολουθηθούν σε οποιοδήποτε αίτημα έκδοσης πιστοποιητικού από την Αρχή Πιστοποίησης του Τμήματος Φυσικής Α.Π.Θ. προκειμένου να εγκριθεί είναι οι ακόλουθες:

1. η έκδοση πιστοποιητικού πρέπει να επικυρώνεται αρχικά από την ΑΚ όπως περιγράφεται στην παράγραφο 4.2.1 .
2. το υποκείμενο πρέπει να είναι μια αποδεκτή οντότητα συνδρομητή, όπως ορίζεται από την παρούσα Πολιτική.
3. το αίτημα πρέπει να υπακούει στο ονοματικό σχήμα (naming scheme) της ΑΠ του Τμήματος Φυσικής Α.Π.Θ
4. το συγκεκριμένο όνομα πρέπει να είναι σαφές και μοναδικό
5. το κλειδί πρέπει να έχει μέγεθος τουλάχιστον 1024 bits.

Εάν το αίτημα πιστοποίησης δεν ικανοποιεί ένα ή περισσότερα από τα ανωτέρω κριτήρια, θα απορρίπτεται, και θα ανακοινώνεται στον ενδιαφερόμενο με υπογεγραμμένο e-mail από τον διαχειριστή της ΑΚ με κοινοποίηση στο pki@physics.auth.gr

4.2.3 Χρόνος επεξεργασίας για την έκδοση πιστοποιητικού

Κάθε αίτηση πιστοποιητικού θα ικανοποιείται σε διάστημα που δεν ξεπερνά τις τρεις (3) εργάσιμες ημέρες.

4.3 Έκδοση πιστοποιητικών

4.3.1 Διαδικασίες ΑΠ κατά την έκδοση πιστοποιητικών

Τα πιστοποιητικά εκδίδονται μετά την ασφαλή μεταφορά των αιτήσεων από την Αρχή Καταχώρισης στην ΑΠ και μετά από έλεγχο του διακεκριμένου ονόματος του πιστοποιητικού.

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

Η ΑΠ ενημερώνει το συνδρομητή για την έκδοση ή απόρριψη έκδοσης του πιστοποιητικού με ηλεκτρονικό ταχυδρομείο.

4.4 Αποδοχή των πιστοποιητικών

4.4.1 Συμπεριφορά που αποτελεί την παραλαβή του πιστοποιητικού

Οι συνδρομητές οφείλουν να παραλάβουν το πιστοποιητικό τους μέσα σε διάστημα τριάντα (30) ημερών από την ημερομηνία της έκδοσής του. Σε αντίθετη περίπτωση το πιστοποιητικό ανακαλείται.

Αμέσως μετά την παραλαβή του πιστοποιητικού οι συνδρομητές οφείλουν να αποστείλουν ηλεκτρονικό μήνυμα υπογεγραμμένο με το πιστοποιητικό τους στο οποίο να δηλώνουν ότι παρέλαβαν το πιστοποιητικό.

4.4.2 Δημοσίευση πιστοποιητικών από την ΑΠ

Η ΑΠ του Τμήματος φυσικής δημοσιοποιεί τα πιστοποιητικά μόνο μετά την παραλαβή τους από τους συνδρομητές.

4.4.3 Ενημέρωση άλλων οντοτήτων για την έκδοση πιστοποιητικών

Δεν προβλέπεται ενημέρωση άλλων οντοτήτων σχετικά με την έκδοση πιστοποιητικών.

4.5 Ζεύγος κλειδιών και χρήση του πιστοποιητικού

4.5.1 Ιδιωτικό κλειδί συνδρομητή και χρήση του πιστοποιητικού

Τα ιδιωτικά κλειδιά των συνδρομητών μαζί με τα πιστοποιητικά που εκδίδονται από την ΑΠ του Τμήματος Φυσικής Α.Π.Θ. μπορούν να χρησιμοποιηθούν για:

1. την υπογραφή / επαλήθευση και την κρυπτογράφηση / αποκρυπτογράφηση (S/MIME) των e-mail
2. την επικύρωση (authentication) Η/Υ-εξυπηρετητών και την κρυπτογράφηση των επικοινωνιών
3. σκοπούς επικύρωσης (authentication) σε Ηλεκτρονικές-Ψηφιακές υποδομές.

4.5.2 Δημόσιο κλειδί υποστηριζόμενων οντοτήτων και χρήση του

πιστοποιητικού

Οι υποστηριζόμενες οντότητες μπορούν να χρησιμοποιούν το δημόσιο κλειδί και τα πιστοποιητικά των συνδρομητών για:

1. Επαλήθευση ψηφιακά υπογεγραμμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου μέσω πρωτοκόλλου S/MIME
2. Κρυπτογράφηση μηνυμάτων ηλεκτρονικού ταχυδρομείου μέσω πρωτοκόλλου S/MIME
3. Επαλήθευση ψηφιακά υπογεγραμμένων κειμένων/κώδικα εφαρμογών
4. Επαλήθευση ψηφιακών χρονοσφραγίδων σε κείμενα
5. Κρυπτογράφηση αρχείων και δεδομένων καθώς και καναλιών επικοινωνίας
6. Έλεγχος ταυτότητας (authentication)
7. Έλεγχος δικαιώματος πρόσβασης (authorization)

Τα υποστηριζόμενα μέρη οφείλουν να μεταφορτώνουν την λίστα ανακληθέντων πιστοποιητικών (ΛΑΠ) κατ' ελάχιστον καθημερινά και να εφαρμόζουν τους περιορισμούς της κατά τη διάρκεια επικύρωσης των πιστοποιητικών.

4.6 Ανανέωση πιστοποιητικών

4.6.1 Περιπτώσεις ανανέωσης πιστοποιητικών

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν ανανεώνει τα πιστοποιητικά των συνδρομητών. Οι συνδρομητές οφείλουν να ακολουθήσουν τη διαδικασία έκδοσης νέου πιστοποιητικού όπως ορίζεται στην παράγραφο 4.3 .

4.6.2 Ποιος μπορεί να αιτηθεί ανανέωση

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν ανανεώνει τα πιστοποιητικά των συνδρομητών. Οι συνδρομητές οφείλουν να ακολουθήσουν τη διαδικασία έκδοσης νέου πιστοποιητικού όπως ορίζεται στην παράγραφο 4.3 .

4.6.3 Επεξεργασία αιτήματος ανανέωσης πιστοποιητικού

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν ανανεώνει τα πιστοποιητικά των συνδρομητών. Οι συνδρομητές οφείλουν να ακολουθήσουν τη διαδικασία έκδοσης νέου πιστοποιητικού όπως ορίζεται στην παράγραφο 4.3 .

4.6.4 Ανακοίνωση νέας έκδοσης πιστοποιητικού στον συνδρομητή

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν ανανεώνει τα πιστοποιητικά των συνδρομητών. Οι συνδρομητές οφείλουν να ακολουθήσουν τη διαδικασία έκδοσης νέου πιστοποιητικού όπως ορίζεται στην παράγραφο 4.3 .

4.6.5 Συμπεριφορά που αποτελεί αποδοχή ανανέωσης πιστοποιητικού

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν ανανεώνει τα πιστοποιητικά των συνδρομητών. Οι συνδρομητές οφείλουν να ακολουθήσουν τη διαδικασία έκδοσης νέου πιστοποιητικού όπως ορίζεται στην παράγραφο 4.3 .

4.6.6 Δημοσιοποίηση ανανέωσης πιστοποιητικού από την ΑΠ

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν ανανεώνει τα πιστοποιητικά των συνδρομητών. Οι συνδρομητές οφείλουν να ακολουθήσουν τη διαδικασία έκδοσης νέου πιστοποιητικού όπως ορίζεται στην παράγραφο 4.3 .

4.6.7 Ανακοίνωση ανανέωσης πιστοποιητικού από την ΑΠ σε άλλες οντότητες

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν ανανεώνει τα πιστοποιητικά των συνδρομητών. Οι συνδρομητές οφείλουν να ακολουθήσουν τη διαδικασία έκδοσης νέου πιστοποιητικού όπως ορίζεται στην παράγραφο 4.3 .

4.7 Επανέκδοση κλειδιών (re-key)

4.7.1 Περιπτώσεις επανέκδοσης κλειδιών

Οι συνδρομητές οφείλουν να επανεκδώσουν το ζεύγος κλειδιών τους στις ακόλουθες περιπτώσεις:

1. λήξη του υπογεγραμμένου από την ΑΠ του Τμήματος Φυσικής Α.Π.Θ. πιστοποιητικού τους
2. ανάκληση του πιστοποιητικού τους από την ΑΠ του Τμήματος Φυσικής Α.Π.Θ.
3. παραβίαση του ιδιωτικού τους κλειδιού.

4.7.2 Ποιος μπορεί να αιτηθεί πιστοποίηση νέου δημοσίου κλειδιού

Ομοίως με την παράγραφο 4.1.1 .

4.7.3 Επεξεργασία αιτήματος επανέκδοσης κλειδιού πιστοποιητικού

Ο συνδρομητής μπορεί στο διάστημα που απομένει ως τη λήξη της ισχύος του υπάρχοντος πιστοποιητικού του, να αποστείλει καινούρια αίτηση υπογραφής πιστοποιητικού μέσω ηλεκτρονικού ταχυδρομείου, εφόσον το ηλεκτρονικό μήνυμα έχει υπογραφεί ψηφιακά από το εν ισχύ πιστοποιητικό του. Σε κάθε άλλη περίπτωση ο συνδρομητής πρέπει να ακολουθήσει την ίδια διαδικασία όπως για ένα νέο πιστοποιητικό. Τουλάχιστον μια φορά κάθε 3 έτη ο συνδρομητής πρέπει να περάσει από την ίδια διαδικασία επικύρωσης με αυτήν που περιγράφεται για την απόκτηση ενός νέου πιστοποιητικού.

Σε περίπτωση που η αίτηση για ένα νέο πιστοποιητικό οφείλεται σε ανάκληση ή παραβίαση του πιστοποιητικού ο συνδρομητής πρέπει να ακολουθήσει την ίδια διαδικασία όπως αυτή περιγράφεται για την απόκτηση ενός νέου.

4.7.4 Ενημέρωση συνδρομητών για τα πιστοποιητικά που στα οποία επανεκδόθηκε κλειδί

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

4.7.5 Αποδοχή πιστοποιητικών στα οποία επανεκδόθηκε κλειδί

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

4.7.6 Δημοσιοποίηση πιστοποιητικών στα οποία επανεκδόθηκε κλειδί

Το πιστοποιητικό με το νέο κλειδί δημοσιεύεται, σύμφωνα με τις διαδικασίες της αποθήκης όπως

περιγράφονται στην παράγραφο 4.4.2 .

4.7.7 Ενημέρωση άλλων οντοτήτων για την έκδοση πιστοποιητικών με νέο κλειδί

Δεν προβλέπεται ενημέρωση άλλων οντοτήτων για τα πιστοποιητικά στα οποία επανεκδόθηκε το κλειδί.

4.8 Μεταβολή πιστοποιητικών

4.8.1 Περιπτώσεις όπου μπορεί να γίνει μεταβολή πιστοποιητικών

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν επιτρέπει την μεταβολή των πιστοποιητικών των συνδρομητών. Οι συνδρομητές οφείλουν να ακολουθήσουν τη διαδικασία επανέκδοσης κλειδιού όπως ορίζεται στην παράγραφο 4.3 .

4.8.2 Ποιος μπορεί να αιτηθεί μεταβολή

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν επιτρέπει την μεταβολή των πιστοποιητικών των συνδρομητών. Οι συνδρομητές οφείλουν να ακολουθήσουν τη διαδικασία επανέκδοσης κλειδιού όπως ορίζεται στην παράγραφο 4.3 .

4.8.3 Επεξεργασία αιτήματος μεταβολής πιστοποιητικού

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν επιτρέπει την μεταβολή των πιστοποιητικών των συνδρομητών. Οι συνδρομητές οφείλουν να ακολουθήσουν τη διαδικασία επανέκδοσης κλειδιού όπως ορίζεται στην παράγραφο 4.3 .

4.8.4 Ανακοίνωση νέας έκδοσης μεταβολής στον συνδρομητή

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν επιτρέπει την μεταβολή των πιστοποιητικών των συνδρομητών. Οι συνδρομητές οφείλουν να ακολουθήσουν τη διαδικασία επανέκδοσης κλειδιού όπως ορίζεται στην παράγραφο 4.3 .

4.8.5 Συμπεριφορά που αποτελεί αποδοχή μεταβολής πιστοποιητικού

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν επιτρέπει την μεταβολή των πιστοποιητικών των συνδρομητών. Οι συνδρομητές οφείλουν να ακολουθήσουν τη διαδικασία επανέκδοσης κλειδιού όπως ορίζεται στην παράγραφο 4.3 .

4.8.6 Δημοσιοποίηση μεταβολής πιστοποιητικού από την ΑΠ

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν επιτρέπει την μεταβολή των πιστοποιητικών των συνδρομητών. Οι συνδρομητές οφείλουν να ακολουθήσουν τη διαδικασία επανέκδοσης κλειδιού όπως ορίζεται στην παράγραφο 4.3 .

4.8.7 Ανακοίνωση μεταβολής πιστοποιητικού από την ΑΠ σε άλλες οντότητες

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν επιτρέπει την μεταβολή των πιστοποιητικών των συνδρομητών. Οι συνδρομητές οφείλουν να ακολουθήσουν τη διαδικασία επανέκδοσης κλειδιού όπως ορίζεται στην παράγραφο 4.3 .

4.9 Ανάκληση και αναστολή πιστοποιητικού

4.9.1 Περιπτώσεις ανάκλησης

Ένα πιστοποιητικό θα ανακαλείται στις ακόλουθες περιπτώσεις:

1. το υποκείμενο του πιστοποιητικού έχει πάψει να αποτελεί επιλέξιμη τελική οντότητα για την πιστοποίηση, όπως περιγράφεται στο παρόν κείμενο πολιτικής
2. το υποκείμενο δεν χρειάζεται πλέον το πιστοποιητικό
3. το ιδιωτικό κλειδί έχει χαθεί ή έχει παραβιαστεί
4. η πληροφορία στο πιστοποιητικό είναι λανθασμένη ή ανακριβής
5. το σύστημα για το οποίο το πιστοποιητικό έχει εκδοθεί έχει αποσυρθεί
6. το υποκείμενο απέτυχε να συμμορφωθεί με τους κανόνες του παρόντος κειμένου πολιτικής.

4.9.2 Ποίος μπορεί να αιτηθεί ανάκληση

Την ανάκληση πιστοποιητικού μπορεί να αιτηθεί:

1. ο συνδρομητής του πιστοποιητικού
2. οποιαδήποτε άλλη οντότητα μπορεί να αποδείξει παραβίαση του ιδιωτικού κλειδιού ή τροποποίηση των στοιχείων του συνδρομητή.

4.9.3 Διαδικασία αίτησης ανάκλησης

Η οντότητα που αιτείται ανάκληση επικυρώνει την αίτηση ανάκλησης υπογράφοντάς την με ένα έγκυρο πιστοποιητικό της ΑΠ του Τμήματος Φυσικής Α.Π.Θ. Διαφορετικά η επικύρωση επιτελείται με την διαδικασία που περιγράφεται στην παράγραφο 3.2.3 .

4.9.4 Χρόνος μέσα στον οποίο ο συνδρομητής μπορεί να καταθέσει αίτημα ανάκλησης

Δεν ορίζεται.

4.9.5 Χρόνος μέσα στον οποίο η ΑΠ οφείλει να επεξεργασθεί την αίτηση ανάκλησης

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. θα επεξεργάζεται όλες της αιτήσεις ανάκλησης εντός μίας (1) εργάσιμης ημέρας.

4.9.6 Απαίτηση ελέγχου των ανακλήσεων από τις υποστηριζόμενες οντότητες

Οι υποστηριζόμενες οντότητες οφείλουν να μεταφορτώνουν την λίστα ανακληθέντων πιστοποιητικών (ΛΑΠ) από την online αποθήκη [παράγραφος 2.2] κατ' ελάχιστον καθημερινά και να εφαρμόζουν τους περιορισμούς της κατά τη διαδικασία επικύρωσης των πιστοποιητικών.

4.9.7 Συχνότητα έκδοσης λίστας ανακληθέντων πιστοποιητικών (ΛΑΠ)

1. οι λίστες ανακληθέντων πιστοποιητικών (ΛΑΠ) θα δημοσιοποιούνται στην on-line αποθήκη κατά την έκδοση, τουλάχιστον μία φορά κάθε τριάντα (30) ημέρες

2. ο ελάχιστος χρόνος ζωής της λίστας ανακληθέντων πιστοποιητικών ανέρχεται σε επτά (7) ημέρες
3. οι λίστες ανακληθέντων πιστοποιητικών εκδίδονται τουλάχιστον επτά (7) ημέρες πριν την λήξη τους.

4.9.8 Ενημέρωση αποθήκης και ΛΑΠ

Βλέπε παράγραφο 4.9.7 .

4.9.9 Έλεγχος κατάστασης πιστοποιητικών σε πραγματικό χρόνο (on-line)

Επί του παρόντος δεν διατίθεται υπηρεσία ελέγχου λίστας ανάκλησης πραγματικού χρόνου (Online Certificate Service Provision, OCSP) από την ΑΠ του Τμήματος Φυσικής Α.Π.Θ.

4.9.10 Απαιτήσεις on-line ελέγχου ανάκλησης

Επί του παρόντος δεν διατίθεται υπηρεσία ελέγχου λίστας ανάκλησης πραγματικού χρόνου (Online Certificate Service Provision, OCSP) από την ΑΠ του Τμήματος Φυσικής Α.Π.Θ.

4.9.11 Άλλες μορφές ανακοίνωσης ανακληθέντων πιστοποιητικών

Οι λίστες ανακληθέντων πιστοποιητικών (ΛΑΠ) θα δημοσιοποιούνται στην on-line αποθήκη.

4.9.12 Ειδικές περιπτώσεις παραβίασης του κλειδιού

Δεν ορίζονται.

4.9.13 Περιπτώσεις αναστολής πιστοποιητικών

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν προβαίνει σε αναστολή πιστοποιητικών.

4.9.14 Ποιος μπορεί να αιτηθεί αναστολή πιστοποιητικού

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν προβαίνει σε αναστολή πιστοποιητικών.

4.9.15 Διαδικασία αιτήσεως αναστολής πιστοποιητικού

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν προβαίνει σε αναστολή πιστοποιητικών.

4.9.16 Περιορισμοί κατά την περίοδο αναστολής πιστοποιητικού

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν προβαίνει σε αναστολή πιστοποιητικών.

4.10 Υπηρεσία ελέγχου κατάστασης πιστοποιητικού

4.10.1 Λειτουργικά χαρακτηριστικά

Η ΑΠ του Τμήματος Φυσικής διαχειρίζεται μια on-line αποθήκη που περιέχει όλες τις ΛΑΠ που έχουν δημοσιευθεί. Αμέσως μετά από κάθε ανάκληση, θα ενημερώνεται ο κατάλογος ανακληθέντων πιστοποιητικών και η βάση δεδομένων με την κατάσταση των πιστοποιητικών.

4.10.2 Διαθεσιμότητα υπηρεσίας

Η on-line αποθήκη συντηρείται με στόχο την αδιάλειπτη διαθεσιμότητά της.

4.10.3 Προαιρετικά χαρακτηριστικά

Δεν ορίζονται.

4.11 Λήξη συνδρομής

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

4.12 Συνοδεία ιδιωτικού κλειδιού (key escrow) και επαναφορά κλειδιού

4.12.1 Διαδικασίες και πρακτικές συνοδείας και επαναφοράς κλειδιού

Δεν ορίζεται.

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

Δεν ορίζεται.

5 ΔΙΟΙΚΗΤΙΚΟΙ, ΤΕΧΝΙΚΟΙ, ΚΑΙ ΛΕΙΤΟΥΡΓΙΚΟΙ ΕΛΕΓΧΟΙ

5.1 Φυσικοί έλεγχοι

5.1.1 Θέση και κατασκευή

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. βρίσκεται στις εγκαταστάσεις του Υπολογιστικού Κέντρου του Τμήματος Φυσικής Α.Π.Θ. που στεγάζεται στο Κτίριο 22d της Σχολής Θετικών Επιστημών του Αριστοτέλειου Πανεπιστήμιου Θεσσαλονίκης.

5.1.2 Φυσική πρόσβαση

Η πρόσβαση στην ΑΠ του Τμήματος Φυσικής Α.Π.Θ. περιορίζεται σε εξουσιοδοτημένο προσωπικό μόνο.

5.1.3 Ηλεκτρική παροχή και κλιματισμός

Ο υπογράφων τα πιστοποιητικά Η/Υ (signing machine) και ο εξυπηρετητής παγκόσμιου δικτυακού ιστού (web server) της ΑΠ του Τμήματος Φυσικής Α.Π.Θ. προστατεύονται από μονάδα αδιάλειπτης ηλεκτρικής παροχής (UPS) και εφεδρικό ηλεκτροπαραγωγό ζεύγος. Η θερμοκρασία περιβάλλοντος στους χώρους που περιέχουν εξοπλισμό σχετιζόμενο με την ΑΠ, διατηρείται σε κατάλληλο επίπεδα με χρήση κλιματιστικών μονάδων.

5.1.4 Έκθεση σε νερό

Δεν αναμένονται πλημμύρες, λόγω της θέσης της ΑΠ του Τμήματος Φυσικής Α.Π.Θ. .

5.1.5 Πρόληψη και προστασία από πυρκαγιά

Οι εγκαταστάσεις της ΑΠ του Τμήματος Φυσικής Α.Π.Θ. υπόκεινται στην ελληνική νομοθεσία σχετικά με την πρόληψη και την προστασία πυρκαγιάς στα δημόσια κτήρια.

5.1.6 Μέσα αποθήκευσης

1. Το ιδιωτικό κλειδί της ΑΠ του Τμήματος Φυσικής Α.Π.Θ. διατηρείται σε διάφορα μεταφερόμενα μέσα αποθήκευσης πάντα σε κρυπτογραφημένη μορφή προστατευμένο με κωδικό (pass phrase) που γνωρίζει αποκλειστικά εξουσιοδοτημένο προσωπικό

2. Αντίγραφα ασφαλείας της σχετιζόμενης πληροφορίας με την ΑΠ διατηρούνται σε μαγνητικές ταινίες (magnetic tape cartridges), εύκαμπτους μαγνητικούς δίσκους (floppy disks) και οπτικούς δίσκους (CD-ROMs).

5.1.7 Διάθεση αποβλήτων

Απόβλητα που περιέχουν εμπιστευτική πληροφορία, όπως παλαιοί εύκαμπτοι μαγνητικοί δίσκοι (floppy disks) καταστρέφονται πριν απορριφθούν.

5.1.8 Τήρηση αντιγράφων ασφαλείας εκτός εγκαταστάσεων

Για λόγους ασφαλείας κρυπτογραφημένο αντίγραφο του ιδιωτικού κλειδιού της αρχής πιστοποίησης διατηρείται σε πυρίμαχο χρηματοκιβώτιο εκτός των εγκαταστάσεων του ΥΚ του Τμήματος Φυσικής.

5.2 Έλεγχοι διαδικασιών

5.2.1 Εμπιστευτικοί ρόλοι

Όλοι οι υπάλληλοι, ανάδοχοι και σύμβουλοι της ΑΠ του Τμήματος Φυσικής (αποκαλούμενοι «προσωπικό») οι οποίοι έχουν πρόσβαση ή έλεγχο στις κρυπτογραφικές διαδικασίες που μπορούν να έχουν επιπτώσεις στις λειτουργίες έκδοσης, χρήσης, αναστολής η ανάκλησης πιστοποιητικών της ΑΠ, συμπεριλαμβανομένης της πρόσβασης σε περιορισμένες λειτουργίες του μηχανισμού αποθήκευσης της ΑΠ, για τον σκοπό του παρόντος κειμένου πολιτικής, θα θεωρείται ότι υπηρετούν σε εμπιστευτικό ρόλο. Το προσωπικό αυτό περιλαμβάνει, αλλά δεν περιορίζεται σε διαχειριστές και μηχανικούς συστημάτων, χειριστές, και προσωπικό που επιτηρεί τις διαδικασίες

5.2.2 Αριθμός ατόμων που απαιτούνται ανά εργασία

Δεν ορίζεται.

5.2.3 Εξακρίβωση ταυτότητας για κάθε ρόλο

Δεν ορίζεται.

5.2.4 Ρόλοι που απαιτούν διαχωρισμό καθηκόντων

Δεν ορίζεται.

5.3 Έλεγχος ασφαλείας προσωπικού

5.3.1 Προσόντα, εμπειρία και ειδικές εξουσιοδοτήσεις που πρέπει το προσωπικό να διαθέτει

Το προσωπικό που χειρίζεται ρόλους των Αρχών Πιστοποίησης και των Αρχών Καταχώρισης πρέπει να διαθέτει εμπειρία σε θέματα ψηφιακών πιστοποιητικών και σε θέματα υποδομής δημοσίου κλειδιού. Επίσης, πρέπει να διαθέτει προϋπηρεσία σε διαχείριση ευαίσθητων προσωπικών δεδομένων και γενικά απόρρητων πληροφοριών.

5.3.2 Διαδικασίες ελέγχου παρελθόντος για το προσωπικό των ΑΠ και το λοιπό προσωπικό

Ακολουθείται η κείμενη νομοθεσία και το πλαίσιο που ισχύει για το προσωπικό του ΑΠΘ.

5.3.3 Απαιτήσεις εκπαίδευσης

Παρέχεται εσωτερική εκπαίδευση στους χειριστές της ΑΠ και της ΑΚ του Τμήματος Φυσικής Α.Π.Θ.

5.3.4 Διαδικασίες και συχνότητα επανεκπαιδεύσεων

Δεν ορίζεται

5.3.5 Εναλλαγή και σειρά αλλαγής ρόλων

Δεν ορίζεται

5.3.6 Κύρωσης που επιβάλλονται για μη εξουσιοδοτημένες ενέργειες

Ακολουθούνται όλες οι νόμιμες διαδικασίες που προβλέπονται για συγκεκριμένα αδικήματα και ο εσωτερικός κανονισμός λειτουργίας του ΑΠΘ.

5.3.7 Έλεγχος σε προσωπικό ανεξάρτητων εργολάβων που εργάζονται εκτός του ΑΠΘ και εμπλέκονται με την ΥΔΚ του Τμήματος Φυσικής ΑΠΘ

Δεν ορίζεται

5.3.8 Παρεχόμενη τεκμηρίωση στο προσωπικό

Τεκμηρίωση σχετική με όλες τις λειτουργικές διαδικασίες της ΑΠ παρέχεται στο προσωπικό κατά τη διάρκεια της αρχικής εκπαίδευσης.

5.4 Διαδικασία καταγραφής συναλλαγών- συμβάντων

5.4.1 Τύποι συναλλαγών - συμβάντων που καταγράφονται

- Κλεισίματα (shutdown) και εκκινήσεις (boot) συστημάτων
- Διαδραστικές συνδέσεις σε Συστήματα (Interactive system logins)
- αιτήσεις πιστοποιητικών
- διαδικασίες επαλήθευσης ταυτότητας
- έκδοση πιστοποιητικών
- αιτήσεις ανάκλησης πιστοποιητικών
- έκδοση λίστας ανακληθέντων πιστοποιητικών (CRL)

5.4.2 Συχνότητα αρχειοθέτησης των επεξεργασμένων συναλλαγών - συμβάντων

Το σύστημα αρχειοθετεί όλες τις συναλλαγές καθημερινά.

5.4.3 Διάστημα τήρησης του αρχείου συναλλαγών - συμβάντων

Τα αρχεία συναλλαγών-συμβάντων τηρούνται για χρονικό διάστημα δύο (2) ετών, ώστε να είναι διαθέσιμα για ενδεχόμενο νόμιμο έλεγχο. Το διάστημα αυτό δύναται να τροποποιηθεί ανάλογα με τις εξελίξεις σχετικής νομοθεσίας.

5.4.4 Προστασία του αρχείου συναλλαγών - συμβάντων

Δεν επιτρέπεται η πρόσβαση στο αρχείο συναλλαγών παρά μόνο για ανάγνωση και προσθήκη από εξουσιοδοτημένα συστήματα και εξουσιοδοτημένο προσωπικό. Δεν επιτρέπονται διαγραφές εγγραφών του αρχείου.

5.4.4.1 Πρόσβαση

Πρόσβαση στο αρχείο των συναλλαγών επιτρέπεται μόνο για ανάγνωση από συγκεκριμένες εφαρμογές της ΑΠ και ΑΚ καθώς και σε εξουσιοδοτημένο προσωπικό.

5.4.4.2 Προστασία κατά των μεταβολών αρχείων συναλλαγών

Εφαρμόζεται πολιτική πρόσβασης η οποία δεν επιτρέπει τις μεταβολές παρά μόνο στους διαχειριστές του λειτουργικού συστήματος της ΑΠ και ΑΚ.

5.4.4.3 Προστασία κατά των διαγραφών αρχείων συναλλαγών

Εφαρμόζεται πολιτική πρόσβασης η οποία δεν επιτρέπει τις διαγραφές παρά μόνο στους διαχειριστές του λειτουργικού συστήματος της ΑΠ και ΑΚ.

5.4.5 Διαδικασίες αντιγράφων ασφαλείας αρχείων συμβάντων

Τηρείται αντίγραφο ασφαλείας του αρχείου συναλλαγών-συμβάντων.

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

Δεν ορίζεται.

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

Δεν ορίζεται.

5.4.8 Αξιολογήσεις ευπάθειας του συστήματος καταγραφής συναλλαγών-συμβάντων

Δεν ορίζεται.

5.5 Αρχειοθέτηση εγγραφών

5.5.1 Τύποι εγγραφών που αρχειοθετούνται

Τα ακόλουθα δεδομένα και αρχεία αρχειοθετούνται από την ΑΠ του Τμήματος Φυσικής Α.Π.Θ.:

1. όλα τα στοιχεία εφαρμογής πιστοποιητικών, συμπεριλαμβανομένων πιστοποίησης και ανάκλησης
2. όλα τα πιστοποιητικά και οι λίστες ανακληθέντων πιστοποιητικών ή τα παραγόμενα στοιχεία κατάστασης των πιστοποιητικών
3. τα login/logout/reboot του Η/Υ που εκδίδει τα πιστοποιητικά.

5.5.2 Διάστημα διατήρησης του αρχείου εγγραφών

Τα αρχεία εγγραφών τηρούνται για χρονικό διάστημα δύο (2) ετών, ώστε να είναι διαθέσιμα για ενδεχόμενο νόμιμο έλεγχο. Το διάστημα αυτό δύναται να τροποποιηθεί ανάλογα με τις εξελίξεις σχετικής νομοθεσίας.

5.5.3 Προστασία του αρχείου εγγραφών

Δεν επιτρέπεται η πρόσβαση στο αρχείο εγγραφών παρά μόνο για ανάγνωση από εξουσιοδοτημένα συστήματα και εξουσιοδοτημένο προσωπικό. Δεν επιτρέπονται διαγραφές ή μεταβολές εγγραφών του αρχείου.

5.5.3.1 Πρόσβαση

Πρόσβαση στο αρχείο των εγγραφών επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.

5.5.3.2 Προστασία κατά των μεταβολών αρχείων εγγραφών

Εφαρμόζεται πολιτική πρόσβασης η οποία δεν επιτρέπει τις μεταβολές.

5.5.3.3 Προστασία κατά των διαγραφών αρχείων εγγραφών

Εφαρμόζεται πολιτική πρόσβασης η οποία δεν επιτρέπει τις διαγραφές.

5.5.3.4 Προστασία κατά της φθοράς των μέσων αποθήκευσης

Δεν ορίζεται.

5.5.3.5 Προστασία κατά της μελλοντικής έλλειψης διαθεσιμότητας συσκευών ανάγνωσης των παλαιών μέσων αποθήκευσης

Δεν ορίζεται.

5.5.4 Διαδικασίες αντιγράφων ασφαλείας αρχείων εγγραφών

Τηρείται αντίγραφο ασφαλείας των αρχείων εγγραφών.

5.5.5 Απαίτηση χρονοσήμανσης-χρονοσφραγίδας αρχείων εγγραφών

Στην παρούσα φάση δεν απαιτείται χρονοσήμανση-χρονοσφράγιση των αρχείων εγγραφών.

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

Δεν ορίζεται.

5.5.7 Διαδικασίες για ανάκτηση και επαλήθευση των στοιχείων των αρχείων εγγραφών

Δεν ορίζεται.

5.6 Ριζική μεταβολή κλειδιού

Το ιδιωτικό κλειδί της ΑΠ αλλάζει περιοδικά. Από τότε και στο εξής μόνο το νέο κλειδί χρησιμοποιείται για υπογραφή πιστοποιητικών. Η περίοδος επικάλυψης του παλαιού και του νέου κλειδιού μπορεί να διαρκέσει το πολύ για ένα (1) χρόνο. Για την συγκεκριμένη περίοδο επικάλυψης, το παλαιό εν ισχύ πιστοποιητικό θα είναι διαθέσιμο για τον έλεγχο παλαιών υπογραφών, και το μυστικό κλειδί για να υπογράφονται οι κατάλογοι ανακληθέντων πιστοποιητικών (CRLs).

5.7 Αποκατάσταση από παραβίαση ασφάλειας και καταστροφή

5.7.1 Διαδικασίες χειρισμού περιστατικών και παραβιάσεων

Τα αρχεία καταγραφής ελέγχονται περιοδικά για ανίχνευση παραβίασης ασφάλειας συστημάτων ή υποσυστημάτων. Σε περίπτωση που ανιχνευθεί κάποια ανωμαλία ή υπάρχει υποψία παραβίασης,

διακόπτεται η παροχή της υπηρεσίας και γίνεται ενδελεχής έλεγχος όλων των συστημάτων.

5.7.2 Διαδικασίες αντιμετώπισης σε περίπτωση παραβίασης-καταστροφής ή υποψίας παραβίασης-καταστροφής υπολογιστικών συστημάτων, λογισμικού, δεδομένων

Σε περίπτωση παραβίασης ή καταστροφής ή υποψίας παραβίασης του ιδιωτικού κλειδιού η ΑΠ οφείλει να διακόψει τη λειτουργία και να διενεργήσει ενδελεχή έλεγχο όλων των εμπλεκόμενων μονάδων και συστημάτων. Σε περίπτωση που διαπιστωθεί παραβίαση ή καταστροφή τότε η ΑΠ του Τμήματος Φυσικής οφείλει:

1. να ειδοποιήσει τους συνδρομητές, τις αρχές εγγραφής και τις σχετιζόμενες Αρχές Πιστοποίησης όπως την Κεντρική Αρχή Πιστοποίησης του ΑΠΘ προκειμένου να ανακαλέσει το Πιστοποιητικό της ΑΠ του Τμήματος Φυσικής ΑΠΘ.
2. να προχωρήσει στην ανάκληση όλων των ενεργών πιστοποιητικών
3. να σταματήσει την έκδοση και διανομή πιστοποιητικών και λιστών ανακληθέντων πιστοποιητικών (CRLs)
4. να ειδοποιήσει τις σχετικές επαφές ασφάλειας

5.7.3 Διαδικασίες αντιμετώπισης σε περίπτωση απώλειας ιδιωτικών κλειδιών

Σε περίπτωση απώλειας ιδιωτικών κλειδιών τελικών πιστοποιητικών, γίνεται ανάκλησή τους από την υπηρεσία πιστοποίησης και έκδοση νέων χωρίς την διακοπή της υπηρεσίας.

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

Το υπολογιστικό κέντρο του Τμήματος Φυσικής καταβάλει την μέγιστη δυνατή προσπάθεια ώστε να είναι σε θέση να επαναφέρει σε λειτουργία τη ΑΠ σε περίπτωση καταστροφής της από φυσικές ή άλλες καταστροφές, χρησιμοποιώντας το αντίγραφο του ιδιωτικού κλειδιού και όλων των απαραίτητων αρχείων που είναι αποθηκευμένα εκτός του κτηρίου όπου στεγάζεται.

5.8 Λήξη ΑΠ ή ΑΚ

Κατά τη λήξη η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. οφείλει :

1. να ειδοποιήσει τους συνδρομητές, τις αρχές εγγραφής και τις σχετιζόμενες Αρχές Πιστοποίησης
2. να σταματήσει την έκδοση και διανομή πιστοποιητικών και λιστών ανακληθέντων πιστοποιητικών (CRLs)
3. να ειδοποιήσει τις σχετικές επαφές ασφάλειας.
4. να δηλώσει όσο το δυνατόν ευρύτερα το τέλος της υπηρεσίας.

Τα αρχεία καταγραφής των ΑΚ και ΑΠ τηρούνται για χρονικό διάστημα δύο (2) ετών, ώστε να είναι διαθέσιμα για ενδεχόμενο νόμιμο έλεγχο. Το διάστημα αυτό δύναται να τροποποιηθεί ανάλογα με τις εξελίξεις σχετικής νομοθεσίας

6 ΤΕΧΝΙΚΟΙ ΕΛΕΓΧΟΙ ΑΣΦΑΛΕΙΑΣ

6.1 Παραγωγή και εγκατάσταση ζεύγους Κλειδιών

6.1.1 Παραγωγή ζεύγους κλειδιών

Τα ζεύγη κλειδιών των Αρχών Πιστοποίησης, και των διαχειριστών των Αρχών Καταχώρησης πρέπει να παράγονται κατά τέτοιο τρόπο ώστε το ιδιωτικό κλειδί να μην είναι γνωστό σε κανένα άλλο εκτός από τον ιδιοκτήτη του ζεύγους.

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν παράγει ιδιωτικά κλειδιά για τους συνδρομητές της.

6.1.2 Παράδοση ιδιωτικού κλειδιού στον συνδρομητή

Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. δεν παράγει ιδιωτικά κλειδιά για τους συνδρομητές της.

6.1.3 Παράδοση δημοσίου κλειδιού στον εκδότη του πιστοποιητικού

Το δημόσιο κλειδί του συνδρομητή πρέπει να μεταφέρεται στην ΑΠ του Τμήματος Φυσικής Α.Π.Θ. κατά τρόπο πού να διασφαλίζει ότι δεν έχει μεταβληθεί.

6.1.4 Παράδοση του δημόσιου κλειδιού της ΑΠ σε υποστηριζόμενα μέρη

Το πιστοποιητικό της ΑΠ μπορεί να μεταφορτώνετε από τον δικτυακό τόπο της ΑΠ του Τμήματος Φυσικής Α.Π.Θ. και από το δικτυακό τόπο της Υποδομής Δημοσίου Κλειδιού του ΑΠΘ.

6.1.5 Μεγέθη κλειδιών

1. Το ελάχιστο μέγεθος κλειδιού πιστοποιητικού φυσικού προσώπου, υπηρεσίας ή εξυπηρετητή είναι 1024 bits.
2. Το ελάχιστο μήκος του ιδιωτικού κλειδιού της ΑΠ του Τμήματος Φυσικής Α.Π.Θ. είναι 2048 bits.

6.1.6 Παράμετροι παραγωγής κλειδιών

Δεν ορίζεται.

6.1.7 Σκοποί χρήσης κλειδιού (σύμφωνα με το πεδίο «χρήση κλειδιού» του X.509v3)

Πιστοποιητικό ΑΠ : Το πιστοποιητικό της ΑΠ μπορεί να χρησιμοποιείται για υπογραφή πιστοποιητικών (keyCertSign) και υπογραφή ΛΑΠ (cRLSign)

Πιστοποιητικά Φυσικών Προσώπων : Τα πιστοποιητικά φυσικών προσώπων μπορούν να χρησιμοποιούνται για επικύρωση δεδομένων (dataEncipherment), καθιέρωση συνόδου (keyEncipherment), ακεραιότητα μηνυμάτων (digitalSignature) και μη απόρριψης ηλεκτρονικών πράξεων (nonRepudiation)

Πιστοποιητικά συσκευών και υπηρεσιών : Τα πιστοποιητικά συσκευών και υπηρεσιών μπορούν να χρησιμοποιούνται για επικύρωση δεδομένων (dataEncipherment), καθιέρωση συνόδου (keyEncipherment) και ακεραιότητα μηνυμάτων (digitalSignature).

6.2 Προστασία ιδιωτικών κλειδιών

6.2.1 Προδιαγραφές για κρυπτογραφικές μονάδες

Δεν ορίζεται.

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

Δεν ορίζεται.

6.2.3 Συνοδεία ιδιωτικού κλειδιού (key escrow)

Δεν ορίζεται.

6.2.4 Αντίγραφα ασφαλείας ιδιωτικού κλειδιού

Το ιδιωτικό κλειδί της ΑΠ του Τμήματος Φυσικής Α.Π.Θ. διατηρείται κρυπτογραφημένο σε αποθηκευτικά μέσα όπως περιγράφεται στην παράγραφο 5.1.6 . Όλα τα μέσα φυλάσσονται σε ασφαλή μέρη όπου η πρόσβαση περιορίζεται μόνο σε εξουσιοδοτημένο προσωπικό.

6.2.5 Αρχειοθέτηση αντιγράφων ασφαλείας ιδιωτικού κλειδιού

Το αντίγραφο ασφαλείας του ιδιωτικού κλειδιού της Αρχής Πιστοποίησης αρχειοθετείται και φυλάσσεται με ασφαλείς μεθόδους και σε ασφαλή χώρο. Η πρόσβαση στο αρχειοθετημένο αντίγραφο ασφαλείας επιτρέπεται μόνο σε εξουσιοδοτημένο προσωπικό.

Η Αρχή Πιστοποίησης του Τμήματος φυσικής δεν αρχειοθετεί τα ιδιωτικά κλειδιά των συνδρομητών.

6.2.6 Μεταφορά ιδιωτικού κλειδιού στο ή από το κρυπτογραφικό μηχανισμό

Δεν ορίζεται

6.2.7 Αποθήκευση ιδιωτικού κλειδιού σε κρυπτογραφικό μηχανισμό

Δεν ορίζεται

6.2.8 Μέθοδος ενεργοποίησης ιδιωτικού κλειδιού

Το ιδιωτικό κλειδί της ΑΠ βρίσκεται κρυπτογραφημένο στον Η/Υ που χρησιμοποιείται στις διαδικασίες υπογραφής της ΑΠ. Για την όποια χρήση του ιδιωτικού κλαδιού πρέπει πρώτα να αποκρυπτογραφηθεί. Η διαδικασία αποκρυπτογράφησης του ιδιωτικού κλειδιού με σκοπό τη πραγματοποίηση κρυπτογραφικών διαδικασιών θα αποκαλείτε στο εξής ενεργοποίηση ιδιωτικού κλειδιού.

Το ιδιωτικό κλειδί της ΑΠ του Τμήματος Φυσικής Α.Π.Θ, ενεργοποιείται με τη χρήση κωδικού ασφαλείας (pass phrase) που γνωρίζει εξουσιοδοτημένο προσωπικό. Βλέπε παράγραφο 6.4.1 .

6.2.9 Μέθοδος απενεργοποίησης ιδιωτικού κλειδιού

Δεν ορίζεται

6.2.10 Μέθοδος καταστροφής ιδιωτικού κλειδιού

Δεν ορίζεται

6.2.11 Αξιολόγηση κρυπτογραφικών συστημάτων

Δεν ορίζεται

6.3 Άλλα θέματα διαχείρισης ζεύγους κλειδιών

6.3.1 Αρχειοθέτηση δημοσίων κλειδιών

Δεν ορίζεται

6.3.2 Περίοδοι χρήσης πιστοποιητικών και ζευγών κλειδιών

Όλα τα πιστοποιητικά που διανέμονται στους συνδρομητές από την ΑΠ του Τμήματος Φυσικής Α.Π.Θ. έχουν μέγιστο χρόνο ζωής ένα (1) έτος.

Ο χρόνος ζωής του πιστοποιητικού της ΑΠ του Τμήματος Φυσικής Α.Π.Θ. είναι τεσσάρων (4) ετών.

6.4 Δεδομένα ενεργοποίησης

6.4.1 Παραγωγή και εγκατάσταση δεδομένων ενεργοποίησης

Ο κωδικός με τον οποίο ενεργοποιείται το ιδιωτικό κλειδί της ΑΠ του Τμήματος Φυσικής Α.Π.Θ. παράγεται στον Η/Υ που χρησιμοποιείται στις διαδικασίες υπογραφής της ΑΠ και πρέπει να έχει τουλάχιστον δώδεκα (12) χαρακτήρες μήκος.

6.4.2 Προστασία δεδομένων ενεργοποίησης

- Ο συνδρομητής είναι υπεύθυνος για την προστασία των δεδομένων ενεργοποίησης του ιδιωτικού του κλειδιού.
- Η ΑΠ του Τμήματος Φυσικής Α.Π.Θ. χρησιμοποιεί κωδικό για να ενεργοποιήσει το ιδιωτικό της κλειδί, που είναι γνωστό μόνο στους εξουσιοδοτημένους χειριστές της. Αντίγραφο του κωδικού σε γραπτή μορφή τοποθετημένο σε σφραγισμένο φάκελο κρατείται σε ασφαλές μέρος, στο οποίο η πρόσβαση περιορίζεται στον διευθυντή και τους εξουσιοδοτημένους χειριστές της ΑΠ. Τα παλαιότερα στοιχεία ενεργοποίησης καταστρέφονται σύμφωνα με τις παρούσες βέλτιστες πρακτικές.

6.4.3 Άλλα θέματα σχετικά με τα δεδομένα ενεργοποίησης

Δεν ορίζεται

6.5 Έλεγχοι ασφαλείας υπολογιστών

6.5.1 Ειδικές τεχνικές απαιτήσεις ασφάλειας υπολογιστών

1. Τα λειτουργικά συστήματα των Η/Υ των ΑΠ/ΑΚ διατηρούνται σε υψηλό επίπεδο ασφάλειας με την εφαρμογή όλων των σχετικών οδηγιών ασφάλειας
2. Συνεχής παρακολούθηση διενεργείται για την ανίχνευση μη εξουσιοδοτημένων αλλαγών στο λογισμικό
3. Η διαμόρφωση των Η/Υ της ΑΠ περιορίζεται στα απολύτως απαραίτητα
4. Ο Η/Υ που υπογράφει κρατείται κλειστός στο χρόνο που δεν χρησιμοποιείται

6.5.2 Βαθμολόγηση ασφάλειας υπολογιστών

Δεν ορίζεται

6.6 Έλεγχοι ασφάλειας κύκλου ζωής

6.6.1 Έλεγχοι ανάπτυξης συστημάτων

Δεν ορίζεται

6.6.2 Έλεγχοι διαχείρισης ασφάλειας

Δεν ορίζεται

6.6.3 Βαθμολόγηση ασφάλειας κύκλου ζωής

Δεν ορίζεται

6.7 Έλεγχοι ασφάλειας δικτύου

1. Ο Η/Υ που υπογράφει κρατείται εκτός δικτύου.
2. Οι υπόλοιποι Η/Υ των Αρχών Καταχώρησης, Αποθήκης προστατεύονται από firewall.
3. Προκειμένου να ανιχνεύονται κακόβουλες δικτυακές δραστηριότητες εκτελείται παθητική παρακολούθηση.

6.8 Χρονοσφραγίδες - Χρονοσήμανση

Δεν ορίζεται

7 ΣΧΗΜΑ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ, ΛΑΠ ΚΑΙ OCSP

7.1 Σχήμα Πιστοποιητικού

7.1.1 Αριθμοί εκδόσεων

Όλα τα πιστοποιητικά που παραπέμπουν σ΄ αυτό το κείμενο πολιτικής θα εκδίδονται στη μορφή που ορίζεται στο πρότυπο X.509v3.

7.1.2 Επεκτάσεις πιστοποιητικού

- Πιστοποιητικό Χρήστη (Φυσικού προσώπου), Εξυπηρετητή και Υπηρεσίας**:**

  1. Basic Constraints (critical): Not a CA.
  2. Key Usage (critical): Ψηφιακή Υπογραφή, μη-αποκήρυξη, υπολογισμοί κλειδιών, υπολογισμοί δεδομένων.
  3. Subject key identifier
  4. Authority key identifier
  5. Subject alternative name
  6. Issuer alternative name
  7. CRL distribution points
  8. Certificate policies
  9. Netscape cert type

7.1.3 Αναγνωριστικά αντικειμένων αλγορίθμων

Δεν ορίζεται.

7.1.4 Σχήμα ονομάτων

Εκδότης:

C=GR
O=Aristotle University of Thessaloniki,
OU=School of Physics,
OU=Certification Authorities,
CN=PhysNet Server CA v2

Υποκείμενο:

C=GR
O=Aristotle University of Thessaloniki,
OU= School of Physics,
OU=*[Hosts|Services|People],*
CN=*SUBJECT NAME*
emailAdress=*E-MAIL ADDRESS OF SUBJECT OR SUBJECTS RESPONSIBLE PERSON*

7.1.5 Περιορισμοί ονομάτων

Περιορισμοί ιδιοτήτων υποκειμένου :

Country:
Πρέπει να είναι "GR"

OrganizationName:
Πρέπει να είναι "Aristotle University of Thessaloniki"

OrganizationalUnitName:
Πρέπει να είναι η "School of Physics"

OrganizationalUnitName:

Πρέπει να είναι ένα από τα "People" , "Hosts" ή "Services".

commonName:
Κύριο όνομα και Επώνυμο του αντικειμένου όταν πρόκειται για πιστοποιητικό χρήστη – φυσικού πρόσωπου , DNS FQDN για πιστοποιητικό εξυπηρετητή ή υπηρεσίας.

SubjectAltName: Η ηλεκτρονική διεύθυνση αλληλογραφίας εντός του Α.Π.Θ του αντικειμένου, όταν πρόκειται για πιστοποιητικό χρήστη, DNS FQDN για πιστοποιητικό εξυπηρετητή ή υπηρεσίας.

7.1.6 Αναγνωριστικό πολιτικής πιστοποίησης

Το αναγνωριστικό της πολιτικής πιστοποίησης, OID (Object Identifier) : 1.3.6.1.4.1.13089.2.1.2.0, με την οποία συμμορφώνεται η «Πολιτική Πιστοποίησης και Δήλωση Διαδικασιών Πιστοποίησης της Υποδομής Δημοσίου Κλειδιού του Τμήματος Φυσικής του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης, έκδοση 2.0» περιλαμβάνεται στα πιστοποιητικά.

7.1.7 Χρήση επέκτασης περιορισμού πολιτικής

Δεν ορίζεται.

7.1.8 Σύνταξη και σημασιολογία του χαρακτηρισμού πολιτικής

Δεν ορίζεται.

7.1.9 Επεξεργασία σημασιολογίας για την κρίσιμη επέκταση πολιτικής πιστοποίησης

Δεν ορίζεται.

7.2 Σχήμα ΛΑΠ

7.2.1 Αριθμοί εκδόσεων

Όλες οι ΛΑΠ θα εκδίδονται σε μορφή X.509 version 2.

7.2.2 ΛΑΠ και επεκτάσεις των εγγραφών της ΛΑΠ

Δεν ορίζεται.

7.3 Σχήμα OCSP

7.3.1 Αριθμοί εκδόσεων

Δεν ορίζεται.

7.3.2 Επεκτάσεις OCSP

Δεν ορίζεται.

8 ΈΛΕΓΧΟΙ ΣΥΜΜΟΡΦΩΣΗΣ ΚΑΙ ΑΛΛΕΣ ΑΞΙΟΛΟΓΗΣΕΙΣ

8.1 Συχνότητα ή συνθήκες αξιολόγησης

Δεν απαιτείται εξωτερικός έλεγχος συμμόρφωσης παρά μόνο αυτοεξέταση της συμμόρφωσης της ΥΔΚ προς την ΠΠ/ΔΔΠ.

Έλεγχος συμμόρφωσης μπορεί να διεξαχθεί από τους ενδιαφερόμενους για συνεργασία με την Υπηρεσία, μετά από άδεια του φορέα που λειτουργεί την Υπηρεσία και εφόσον ο ενδιαφερόμενος καλύψει όλα τα έξοδα του ελέγχου.

8.2 Ταυτότητα και προσόντα αξιολογητή

Δεν ορίζεται.

8.3 Σχέση αξιολογητή με την αξιολογούμενη οντότητα

Δεν ορίζεται.

8.4 Θέματα που καλύπτει η αξιολόγηση

Δεν ορίζεται.

8.5 Μέτρα που λαμβάνονται σε περίπτωση ανεπάρκειας

Δεν ορίζεται.

8.6 Επικοινωνία αποτελεσμάτων

Δεν ορίζεται.

9 ΑΛΛΑ ΔΙΟΙΚΗΤΙΚΑ ΚΑΙ ΝΟΜΙΚΑ ΖΗΤΗΜΑΤΑ

9.1 Αμοιβές

9.1.1 Αμοιβές έκδοσης ή ανανέωσης πιστοποιητικού

Καμία αμοιβή δεν χρεώνεται.

9.1.2 Αμοιβή για τη πρόσβαση σε εκδοθέντα πιστοποιητικά

Καμία αμοιβή δεν χρεώνεται.

9.1.3 Αμοιβή για πρόσβαση στις λίστες ανάκλησης πιστοποιητικών

Καμία αμοιβή δεν χρεώνεται.

9.1.4 Αμοιβή για λοιπές υπηρεσίες

Καμία αμοιβή δεν χρεώνεται.

9.1.5 Πολιτική επιστροφής χρημάτων

Καμία αμοιβή δεν χρεώνεται συνεπώς δεν προβλέπεται πολιτική επιστροφής χρημάτων.

9.2 Οικονομικές ευθύνες

9.2.1 Ασφαλιστική κάλυψη

Η ΑΠ του Τμήματος Φυσικής δεν αναλαμβάνει καμία οικονομική ευθύνη για καταστροφές ή φθορές που μπορεί προκληθούν από τη λειτουργία της.

9.2.2 Άλλα περιουσιακά ζητήματα

Η ΑΠ του Τμήματος Φυσικής δεν αναλαμβάνει καμία οικονομική ευθύνη για καταστροφές ή φθορές που μπορεί προκληθούν από τη λειτουργία της.

9.2.3 Ασφαλιστική ή εγγυητική κάλυψη τελικών οντοτήτων

Δεν ορίζεται.

9.3 Εμπιστευτικότητα πληροφοριών εμπορικού χαρακτήρα

Η ΥΔΚ του Τμήματος Φυσικής ΑΠΘ δεν διαχειρίζεται πληροφορίες εμπορικού χαρακτήρα.

9.3.1 Πεδίο εμπιστευτικής πληροφορίας

Δεν ορίζεται.

9.3.2 Πληροφορία που δεν εντάσσεται στο πεδίο της εμπιστευτικής πληροφορίας

Δεν ορίζεται.

9.3.3 Ευθύνη προστασίας εμπιστευτικής πληροφορίας

Δεν εφαρμόζεται.

9.4 Εμπιστευτικότητα πληροφοριών προσωπικού χαρακτήρα

Η ΑΠ του Τμήματος Φυσικής δεν συλλέγει απόρρητα ή ευαίσθητα προσωπικά δεδομένα των συνδρομητών.

9.4.1 Σχέδιο εμπιστευτικότητας

Δεν ορίζεται.

9.4.2 Πληροφορίες που χαρακτηρίζονται εμπιστευτικές

Η ΑΠ του Τμήματος Φυσικής δεν συλλέγει εμπιστευτική ή απόρρητη πληροφορία προσωπικού χαρακτήρα.

9.4.3 Πληροφορίες οι οποίες δεν χαρακτηρίζονται ως προσωπικές ή απόρρητες

Η ΑΠ του Τμήματος Φυσικής συλλέγει τις ακόλουθες πληροφορίες που δεν χαρακτηρίζονται ως ευαίσθητα προσωπικά δεδομένα:

1. την ηλεκτρονική διεύθυνση του χρήστη
2. το ονοματεπώνυμο του χρήστη
3. το ψηφιακό πιστοποιητικό του χρήστη.

9.4.4 Ευθύνη προστασίας προσωπικών δεδομένων

Η ΑΠ του Τμήματος Φυσικής συμμορφώνεται με την ισχύουσα νομοθεσία περί προστασίας Προσωπικών Δεδομένων.

Η ΑΠ του Τμήματος Φυσικής δεν συλλέγει δεδομένα που χαρακτηρίζονται εμπιστευτικά ή απόρρητα προσωπικού χαρακτήρα.

9.4.5 Διάθεση πληροφοριών σε αρχές επιβολής του νόμου

Η ΑΠ του Τμήματος Φυσικής δεν συλλέγει εμπιστευτική ή απόρρητη πληροφορία προσωπικού χαρακτήρα.

Οι μη εμπιστευτικές πληροφορίες που τηρεί η Υπηρεσία είναι διαθέσιμες στις δικαστικές αρχές, μετά από έγγραφη αίτησή τους. Για τη διάθεση στις δικαστικές αρχές εμπιστευτικών πληροφοριών ή προσωπικών δεδομένων των εγγραφόμενων, θα γίνεται αίτηση σύμφωνα με την ισχύουσα νομοθεσία και μέσω της Πρυτανείας του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης. Ιδιωτικά κλειδιά που χρησιμοποιούνται από την Υπηρεσία για την υπογραφή πιστοποιητικών, δεν δημοσιοποιούνται σε τρίτους σε καμία περίπτωση, εκτός αν ο νόμος το απαιτεί ρητά.

9.4.6 Πληροφορίες που μπορούν να διατεθούν για την αναζήτηση

οντοτήτων

Η ΑΠ του Τμήματος Φυσικής δεν συλλέγει εμπιστευτική ή απόρρητη πληροφορία προσωπικού χαρακτήρα.

Οι μη εμπιστευτικές πληροφορίες που τηρεί η Υπηρεσία είναι διαθέσιμες για την αναζήτηση οντοτήτων, μετά από αίτηση.

9.4.7 Όροι για τη διάθεση πληροφοριών μετά από αίτημα του ιδιοκτήτη τους

Οι πληροφορίες που τηρεί η ΑΠ είναι διαθέσιμες στον ιδιοκτήτη τους, μετά από αίτησή του.

9.4.8 Άλλες περιπτώσεις στις οποίες διατίθενται εμπιστευτικές πληροφορίες

Η ΑΠ του Τμήματος Φυσικής δεν συλλέγει εμπιστευτική ή απόρρητη πληροφορία προσωπικού χαρακτήρα.

9.5 Δικαιώματα πνευματικής ιδιοκτησίας

Η ΥΔΚ του Τμήματος Φυσικής ΑΠΘ δεν έχει δικαιώματα πνευματικής ιδιοκτησίας στα εκδιδόμενα πιστοποιητικά.

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

9.6 Αντιπροσωπεύσεις και εξουσιοδοτήσεις

9.6.1 Αντιπροσωπεύσεις και εξουσιοδοτήσεις της ΑΠ

Δεν ορίζεται.

9.6.2 Αντιπροσωπεύσεις και εξουσιοδοτήσεις της ΑΚ

Δεν ορίζεται.

9.6.3 Αντιπροσωπεύσεις και εξουσιοδοτήσεις των συνδρομητών

Δεν ορίζεται.

9.6.4 Αντιπροσωπεύσεις και εξουσιοδοτήσεις των υποστηριζόμενων μερών

Δεν ορίζεται.

9.6.5 Αντιπροσωπεύσεις και εξουσιοδοτήσεις άλλων συμμετεχόντων

Δεν ορίζεται.

9.7 Αποκηρύξεις και εγγυήσεις

Δεν ορίζεται.

9.8 Περιορισμοί ευθυνών

Η Υποδομή Δημοσίου Κλειδιού του Τμήματος Φυσικής ΑΠΘ δεν ευθύνεται για προβλήματα ή ζημιές που μπορεί να προκύψουν από την ανυπαίτια πλημμελή λειτουργία της ή από την κακή χρήση των

πιστοποιητικών που εκδίδει. Η χρήση της ΥΔΚ του Τμήματος Φυσικής ΑΠΘ και των υπηρεσιών Πιστοποίησης προϋποθέτει την ανεπιφύλακτη παραδοχή εκ μέρους του χρήστη ότι η ΥΔΚ του Τμήματος Φυσικής ΑΠΘ δεν ευθύνεται για ζημία ή βλάβη, δεν αναλαμβάνει, ούτε μπορούν να τις αποδοθούν οικονομικές, αστικές ή άλλου είδους ευθύνες, παρά μόνο σε περιπτώσεις που αποδεικνύεται δόλος ή αμέλεια της.

9.9 Αποζημιώσεις

Η Υποδομή Δημοσίου Κλειδιού του Τμήματος Φυσικής ΑΠΘ και οι υπηρεσίες Πιστοποίησης δεν αναλαμβάνουν ούτε μπορούν να τους αποδοθούν οικονομικές, αστικές ή άλλου είδους ευθύνες, παρά μόνο σε περιπτώσεις που αποδεικνύεται δόλος ή αμέλεια τους. Επίσης χρησιμοποιείται αποκλειστικά για Ακαδημαϊκούς και Ερευνητικούς σκοπούς και απαγορεύεται ρητά η εμπορική εκμετάλλευσή της. Συνεπώς, η ΥΔΚ απαλλάσσεται από κάθε ζημία, που δε συνδέεται αιτιωδώς με τη χρήση των υπηρεσιών πιστοποίησης για τους παραπάνω σκοπούς.

9.10 Χρονική περίοδος ισχύος και λήξη.

9.10.1 Χρονική Περίοδος ισχύος

Δεν ορίζεται.

9.10.2 Λήξη ισχύος

Δεν ορίζεται.

9.10.3 Επιπτώσεις και κατάλοιπα λήξης

Δεν ορίζεται.

9.11 Ατομικές ειδοποιήσεις και επικοινωνία μεταξύ των αποτελούμενων μερών

Δεν ορίζεται.

9.12 Τροποποιήσεις

9.12.1 Διαδικασία τροποποιήσεων

Συντακτικές ή άλλες αλλαγές οι οποίες δεν επιφέρουν αλλοίωση στα άρθρα της παρούσης μπορούν να γίνουν χωρίς καμία άλλη ενέργεια.

Οποιεσδήποτε αλλαγές επιφέρουν αλλοίωση στο περιεχόμενο της παρούσης συνοδεύονται υποχρεωτικά από μεταβολή της έκδοσης του αριθμού αναγνώρισης του εγγράφου (OID) και ταυτόχρονη δημοσίευση του κειμένου στην ιστοσελίδα της ΥΔΚ του Τμήματος Φυσικής Α.Π.Θ. (http://pki.physics.auth.gr)

9.12.2 Μηχανισμοί ενημέρωσης και περίοδος ενημέρωσης

Η τρέχουσα ενεργή καθώς και όλες οι προηγούμενες εκδόσεις ΠΠ/ΔΔΠ δημοσιεύονται στη στην ιστοσελίδα της ΥΔΚ του Τμήματος Φυσικής Α.Π.Θ. (http://pki.physics.auth.gr)

9.12.3 Συνθήκες κάτω από τις οποίες το OID πρέπει να αλλάζει

Σε περίπτωση σημαντικών αλλαγών που επιφέρουν αλλοίωση στο περιεχόμενο της παρούσης πρέπει

να αλλάζει το αναγνωριστικό όνομα του εγγράφου (OID).

9.13 Διαδικασίες επίλυσης αντιδικιών

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

9.14 Ισχύουσα νομοθεσία

Η λειτουργία της ΥΔΚ του Τμήματος Φυσικής ΑΠΘ καθώς και η ερμηνεία της Πολιτικής Πιστοποίησης/Δήλωσης Διαδικασιών Πιστοποίησης υπόκεινται κύρια στα Ακαδημαϊκά ήθη και στην Ελληνική Νομοθεσία. Ιδιαίτερα όσο αφορά το Προεδρικό Διάταγμα 150/2001 «Προσαρμογή στην οδηγία 99/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές», τα πιστοποιητικά που εκδίδονται μέσω της ΥΔΚ του Τμήματος Φυσικής ΑΠΘ ΔΕΝ θεωρούνται γενικά ως «Αναγνωρισμένα Πιστοποιητικά». Βασικές προϋποθέσεις για την αναγνώριση του πιστοποιητικού και της παραγόμενης ψηφιακής υπογραφής ως ισότιμης με τη χειρόγραφη, είναι α) η χρήση «ασφαλούς διάταξης δημιουργίας υπογραφής» στην πλευρά του πελάτη (π.χ. έξυπνη κάρτα όπου δημιουργείται, αποθηκεύεται και χρησιμοποιείται αποκλειστικά το ιδιωτικό κλειδί του πελάτη) και β) η έγκριση του εκάστοτε αρμόδιου οργάνου (π.χ. σύγκλητος).

9.15 Συμμόρφωση με την κείμενη νομοθεσία

Η ΥΔΚ του Τμήματος Φυσικής ΑΠΘ συμμορφώνεται πλήρως με την κείμενη Ελληνική νομοθεσία.

9.16 Διάφορες παροχές

9.16.1 Συνολική σύμβαση

Δεν ορίζεται.

9.16.2 Ανάθεση

Δεν ορίζεται.

9.16.3 Διαιρετότητα

Δεν ορίζεται.

9.16.4 Εφαρμογή (αμοιβές πληρεξουσίων και παραίτηση εκ των δικαιωμάτων)

Δεν ορίζεται.

9.16.5 Ανωτέρα βία

Δεν ορίζεται.

9.17 Άλλες παροχές

Δεν ορίζεται.