Αρχή Πιστοποίησης Ελληνικού Δημοσίου

Κανονισμός Πιστοποίησης

Όπως τροποποιήθηκε και ισχύει

[ΦΕΚ 799 Β/09-06-2010 - ΦΕΚ 3320 Β/27-12-2013]

Τελευταία Ενημέρωση: 14 Απριλίου 2015

Περιεχόμενα

1. Εισαγωγή

Το έγγραφο αυτό αποτελεί τον Κανονισμό Πιστοποίησης της ΑΡΧΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ του ΕΛΛΗΝΙΚΟΥ ΔΗΜΟΣΙΟΥ - ΑΠΕΔ (Πρωτεύουσας Αρχής Πιστοποίησης), σύμφωνα με τις διατάξεις των παραγράφων 1, 2 και 3 του άρθρου 20 του Ν. 3448/2006 (ΦΕΚ 57/Α), με την οποία καθορίζονται οι όροι και οι προϋποθέσεις για την παροχή των υπηρεσιών πιστοποίησης από την ΑΠΕΔ ως Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ) και τις Υποκείμενες Αρχές Πιστοποίησης (ΥπΑΠ), καθώς και για την εν γένει παροχή υπηρεσιών πιστοποίησης του Ελληνικού Δημοσίου, μέσω της Υποδομής Δημοσίου Κλειδιού της ΑΠΕΔ, η οποία αναλύεται στα επιμέρους κεφάλαια του παρόντος.

Καθορίζει τις πολιτικές πιστοποιητικών της ΑΠΕΔ (Ενότητα Α), καθώς και τη Δήλωση Πρακτικής των Υποκείμενων Αρχών Πιστοποίησης της ΑΠΕΔ (Ενότητα Β) η οποία εξειδικεύει τους όρους και τις προϋποθέσεις για την παροχή υπηρεσιών πιστοποίησης σύμφωνα με την πολιτική πιστοποιητικών της ΑΠΕΔ και με τις διατάξεις της παραγράφου 2 του Άρθρου 20 του Νόμου 3448/2006 (ΦΕΚ 57/Α).

Τα ψηφιακά πιστοποιητικά τελικών χρηστών που είχαν εκδοθεί βάσει της υπ' αριθμ. 2512 οικ./2006 (ΦΕΚ 165Β/10.11.2006) κοινής απόφασης του Υπουργού Εσωτερικών, Δημόσιας Διοίκησης και Αποκέντρωσης και του Υπουργού Μεταφορών και Επικοινωνιών «Κύρωση Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου», συνεχίζουν να ισχύουν μέχρι την ημερομηνία λήξης τους με βάση την Πολιτική Πιστοποίησης όπως αυτή καθορίστηκε με τις διατάξεις της με υπ' αριθμ. 2512 οικ./2006 ΚΥΑ.

- Ο Κανονισμός Πιστοποίησης κυρώθηκε με την Υπουργική Απόφαση αριθμ. ΥΑΠ/Φ.60/38/232 που δημοσιεύθηκε στο ΦΕΚ 799Β/9.6.2010 και **τέθηκε σε ισχύ από την 9η Ιουνίου 2010.**
- Τροποποιήθηκε με την ΚΥΑ με αριθμ. ΥΑΠ/Φ.60/3431 που δημοσιεύθηκε στο ΦΕΚ 3320Β/27.12.2013.

Στην συνέχεια παρουσιάζεται ο **Κανονισμός Πιστοποίησης όπως τροποποιήθηκε και ισχύει.**

2. Κανονισμός Πιστοποίησης της ΑΡΧΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΕΛΛΗΝΙΚΟΥ ΔΗΜΟΣΙΟΥ (ΑΠΕΔ)

Η παρούσα πράξη αποτελεί τον Κανονισμό Πιστοποίησης (ΚΠ) της ΑΡΧΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ του ΕΛΛΗΝΙΚΟΥ ΔΗΜΟΣΙΟΥ - ΑΠΕΔ (Πρωτεύουσας Αρχής Πιστοποίησης), σύμφωνα με τις διατάξεις των παραγράφων 1, 2 και 3 του άρθρου 20 του Ν. 3448/2006 (ΦΕΚ 57/Α), με την οποία καθορίζονται οι όροι και οι προϋποθέσεις για την παροχή των υπηρεσιών πιστοποίησης από την ΑΠΕΔ ως Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ) και τις Υποκείμενες Αρχές Πιστοποίησης (ΥπΑΠ), καθώς και για την εν γένει παροχή υπηρεσιών πιστοποίησης του Ελληνικού Δημοσίου, μέσω της Υποδομής Δημοσίου Κλειδιού της ΑΠΕΔ, η οποία αναλύεται στα επιμέρους κεφάλαια του παρόντος.

Ως εκ τούτου, με την παρούσα καθορίζονται οι πολιτικές πιστοποιητικών της ΑΠΕΔ (Ενότητα Α), καθώς και η Δήλωση Πρακτικής των Υποκείμενων Αρχών Πιστοποίησης της ΑΠΕΔ (Ενότητα Β) η οποία εξειδικεύει τους όρους και τις προϋποθέσεις για την παροχή υπηρεσιών πιστοποίησης σύμφωνα με την πολιτική πιστοποιητικών της ΑΠΕΔ και με τις διατάξεις της παραγράφου 2 του Άρθρου 20 του Νόμου 3448/2006 (ΦΕΚ 57/Α).

Πέραν των διατάξεων της παρούσας πράξης οι παραπάνω πολιτικές πιστοποιητικών εξειδικεύονται και με τις εκάστοτε Δηλώσεις Πρακτικής άλλων υπαγόμενων στην ΑΠΕΔ ΥπΑΠ, οι οποίες εκδίδουν ψηφιακά πιστοποιητικά, καθώς και στις Δηλώσεις Πρακτικής των τρίτων φορέων - Παροχών Υπηρεσιών Πιστοποίησης. Σημειώνεται ότι στο παρόν κείμενο ο όρος ΥπΑΠ αναφέρεται στις Αρχές Πιστοποίησης που έχουν ως Πρωτεύουσα Αρχή Πιστοποίησης την ΑΠΕΔ, ενώ όπου χρησιμοποιείται ο όρος εκδότριες ΑΠ περικλείει τόσο τις ΥπΑΠ, όσο και τους τρίτους φορείς - Παρόχους Υπηρεσιών Πιστοποίησης, οι οποίοι εφαρμόζουν μία ή περισσότερες από τις πολιτικές πιστοποιητικών της ΑΠΕΔ σύμφωνα με τις ως άνω διατάξεις.

Α. Πολιτική Πιστοποιητικών της ΑΠΕΔ

1. Εισαγωγή

Στην παρούσα Πολιτική Πιστοποιητικών (ΠΠ) καθορίζονται οι πολιτικές πιστοποιητικών της ΑΠΕΔ, οι όροι και οι προϋποθέσεις για την ανάθεση και υποστήριξη ή παροχή υπηρεσιών πιστοποίησης σε φορείς - Παρόχους Υπηρεσιών Πιστοποίησης οι οποίοι υποχρεούνται να εφαρμόζουν το παρόν νομικό, τεχνικό και λειτουργικό πλαίσιο παροχής υπηρεσιών πιστοποίησης σύμφωνα με τις διατάξεις της παραγράφων 2 και 5 του Άρθρου 20 του Νόμου 3448/2006 (ΦΕΚ 57/Α).
Σε κάθε περίπτωση, η ΑΠΕΔ μεριμνά και λαμβάνει τα αναγκαία μέτρα για την εφαρμογή του της παρούσας ΠΠ στους τομείς ευθύνης της, όπως αυτή περιγράφεται στον παρόν κείμενο.

1.1 Περίληψη

Η παρούσα ΠΠ καθορίζει τους όρους, τις προϋποθέσεις για την έγκριση, έκδοση, χειρισμό, χρήση, ανάκληση και ανανέωση των ψηφιακών πιστοποιητικών και την παροχή των σχετικών υπηρεσιών πιστοποίησης από τις εκδότριες ΑΠ. Ειδικότερα, η παρούσα ΠΠ θέτει το πλαίσιο για:

- Τις υποχρεώσεις των εκδοτριών Αρχών Πιστοποίησης (Certification Authorities), των Αρχών Εγγραφής (Registration Authorities), των Τελικών Χρηστών και των Τρίτων Συμμετεχόντων.
- Τα θέματα που αφορούν στους Όρους Χρήσης Πιστοποιητικών (ΟΧΠ) Τελικού Χρήστη και τους Όρους Τρίτων Συμμετεχόντων (ΟΤΣ).
- Τις μεθόδους που χρησιμοποιούνται για την επιβεβαίωση της ταυτότητας των Τελικών Χρηστών.
- Τις λειτουργικές διαδικασίες ως προς τις υπηρεσίες κύκλου ζωής Πιστοποιητικού: υποβολή αιτήματος για έκδοση, αποδοχή, ανάκληση και ανανέωση Πιστοποιητικού.
- Το περιεχόμενο των Πιστοποιητικών, των Καταλόγων Ανακληθέντων Πιστοποιητικών (ΚΑΠ), και των Πιστοποιητικών της υπηρεσίας δικτυακού ελέγχου κατάστασης πιστοποιητικών σε πραγματικό χρόνο (Online Certificate Status Protocol - OCSP), όταν διατίθεται.
- Τις λειτουργικές διαδικασίες ασφάλειας ως προς την καταγραφή στοιχείων ελέγχου, την τήρηση αρχείων και την αποκατάσταση καταστροφών.
- Τους κανονισμούς φυσικής ασφάλειας, ασφάλειας προσωπικού, διαχείρισης κλειδιών και λογικής ασφάλειας.
- Τη διαχείριση της ΠΠ, συμπεριλαμβανομένων των μεθόδων τροποποίησης της.

- Τις τεχνικές προδιαγραφές και εξειδικεύσεις των Δηλώσεων Πρακτικής των Υποκείμενων Αρχών Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου.

Ο Πίνακας 1 περιλαμβάνει τον κατάλογο των προς δημοσίευση εγγράφων της ΑΠΕΔ, καθώς και των τοποθεσιών δημοσίευσης των. Τα έγγραφα που δε διατίθενται προς δημοσίευση αποτελούν εμπιστευτικό υλικό της ΑΠΕΔ.

Πίνακας 1: Διαθέσιμα Έγγραφα Κανονισμών

Έγγραφα	Κατάσταση	Τοποθεσία Δημοσίευσης για το Κοινό
Πολιτική Πιστοποιητικών της ΑΠΕΔ	Δημόσιο	Χώρος Αποθήκευσης της ΑΠΕΔ, σύμφωνα με την §2.2 της ΠΠ
Όροι Χρήσης Πιστοποιητικών (ΟΧΠ) Τελικών Χρηστών και Όροι Τρίτου Συμμετέχοντα (ΟΤΣ)	Δημόσιο	Χώρος Αποθήκευσης της ΑΠΕΔ, σύμφωνα με την §2.2 της ΠΠ

1.2 Όνομα και Ταυτότητα Εγγράφου

Η ΑΠΕΔ έχει προσαρμόσει την παρούσα ΠΠ στο πρότυπο Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (Πλαίσιο Πολιτικής Πιστοποιητικού Υποδομής Δημόσιου Κλειδιού και Κανονισμών Πιστοποίησης X.509 για το Διαδίκτυο), γνωστό και ως RFC 3647, της Ομάδας Δράσης για την Διαδικτυακή Μηχανική (Internet Engineering Task Force), φορέας ο οποίος είναι υπεύθυνος για τον καθορισμό προτύπων στο Διαδίκτυο, για να διευκολύνει την απεικόνιση της εφαρμοζόμενης πολιτικής πιστοποιητικού. Μικρές αποκλίσεις από την δομή του RFC 3647 σε επιμέρους λεπτομέρειες, είναι απαραίτητες εξαιτίας της εφαρμογής του λειτουργικού μοντέλου της ΑΠΕΔ στο δημόσιο τομέα. Η ΑΠΕΔ, εξάλλου, διατηρεί το δικαίωμα να προβαίνει στις απαραίτητες ενέργειες στο πλαίσιο της παρούσας ΠΠ, όπου αυτό κρίνεται σκόπιμο, με σκοπό τη βελτίωση της ποιότητας των παρεχόμενων υπηρεσιών της.

1.2.1 Πολιτικές Πιστοποιητικών

1.2.1.1 Πολιτική Πιστοποιητικού 1 (ΠΠ 1)

Η Πολιτική Πιστοποιητικού 1 (ΠΠ 1) αναφέρεται σε Αναγνωρισμένα Πιστοποιητικά τελικών χρηστών.

Τα πιστοποιητικά που εκδίδονται βάσει της ΠΠ 1 χρησιμοποιούνται για ψηφιακή υπογραφή (προηγμένη ηλεκτρονική υπογραφή) ηλεκτρονικών μηνυμάτων και εγγράφων ή/και για αυθεντικοποίηση χρήστη. Ήτοι, τα Πιστοποιητικά που εκδίδονται βάσει της ΠΠ 1 είναι κατάλληλα για να υποστηρίξουν προηγμένη ηλεκτρονική υπογραφή, σύμφωνα με τις διατάξεις της παράγ. 1 του άρθρου 3 του ΠΔ150/2001 (ΦΕΚ 125/Α), η οποία βασίζεται σε Αναγνωρισμένο Πιστοποιητικό και δημιουργείται σε Ασφαλή Διάταξη Δημιουργίας Υπογραφής (ΑΔΔΥ), οπότε και επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο.

Η ΠΠ 1 αντιστοιχεί στην δημόσια πολιτική πιστοποιητικών "QCP + SSCD" όπως περιγράφεται στο πρότυπο ETSI 101 456 του European Telecommunications Standards Institute - ETSI (εφεξής αναφερόμενο ως έγγραφο Πολιτικής ETSI 101 456) αναφορικά με τις Απαιτήσεις Πολιτικής για Αρχές Πιστοποίησης που εκδίδουν Αναγνωρισμένα Πιστοποιητικά. Τα Πιστοποιητικά που εκδίδονται με βάση την ΠΠ 1 πιστοποιούν την αντιστοιχία του φυσικού προσώπου (Τελικού Χρήστη) με τα στοιχεία που αναφέρονται στο έγγραφο ταυτοποίησης του.

Η ταυτοποίηση των Τελικών Χρηστών προϋποθέτει τη φυσική παρουσία τους ενώπιον αρμόδιων στελεχών σύμφωνα με τα προβλεπόμενα στην παρούσα πράξη, οι οποίοι ελέγχουν τα έγγραφα που τεκμηριώνουν την ταυτότητα του Τελικού Χρήστη (§3.2.3).

Τα Αναγνωρισμένα Πιστοποιητικά Τελικών Χρηστών αναφέρονται αποκλειστικά και μόνο σε φυσικά πρόσωπα. Σε κάθε περίπτωση το Αναγνωρισμένο Πιστοποιητικό συνδέεται κατ` αποκλειστικότητα με ένα φυσικό πρόσωπο το οποίο και φέρει την αποκλειστική ευθύνη για αυτό το πιστοποιητικό.

1.2.1.2 Πολιτική Πιστοποιητικού 2 (ΠΠ 2)

Η Πολιτική Πιστοποιητικού 2 (ΠΠ 2) αναφέρεται σε Πιστοποιητικά Τελικών Χρηστών που χρησιμοποιούνται για κρυπτογράφηση ηλεκτρονικών μηνυμάτων ή εγγράφων.

Τα Πιστοποιητικά αυτά, μπορούν είτε να αποθηκεύονται σε ΑΔΔΥ είτε όχι. Για τα Πιστοποιητικά που ακολουθούν την ΠΠ 2 παρέχονται σε ορισμένες περιπτώσεις, οι οποίες εξειδικεύονται στην εκάστοτε Δήλωση Πρακτικής της εκδότριας Αρχής Πιστοποίησης, υπηρεσίες αρχειοθέτησης του ιδιωτικού κλειδιού του Τελικού Χρήστη, και συνεπώς η δυνατότητα ανάκτησης των ιδιωτικών κλειδιών των Τελικών Χρηστών.

1.2.1.3 Πολιτική Πιστοποιητικού 3 (ΠΠ 3)

Η Πολιτική Πιστοποιητικού 3 (ΠΠ 3) αναφέρεται σε Αναγνωρισμένα Πιστοποιητικά Τελικών Χρηστών.

Τα Πιστοποιητικά που εκδίδονται βάσει της ΠΠ 3 χρησιμοποιούνται για ψηφιακή υπογραφή (προηγμένη ηλεκτρονική υπογραφή) ηλεκτρονικών μηνυμάτων και εγγράφων ή/και για αυθεντικό ποίηση χρήστη. Ήτοι, τα Πιστοποιητικά που εκδίδονται βάσει της ΠΠ 3 είναι κατάλληλα για να υποστηρίξουν προηγμένη ηλεκτρονική υπογραφή, σύμφωνα με τις διατάξεις της παράγ. 2 του άρθρου 3 του ΠΔ 150/2001 (ΦΕΚ 125/Α`), η οποία βασίζεται σε Αναγνωρισμένο Πιστοποιητικό και δε δημιουργείται σε ΑΔΔΥ. Η ΠΠ 3 αντιστοιχεί στην δημόσια πολιτική πιστοποιητικών "QCP public" όπως περιγράφεται στο "έγγραφο Πολιτικής ETS1101 456" του European Telecommunications Standards Institute - ETSI (εφεξής αναφερόμενο ως έγγραφο Πολιτικής ETS1101 456) αναφορικά με τις Απαιτήσεις Πολιτικής για Αρχές Πιστοποίησης που εκδίδουν Αναγνωρισμένα Πιστοποιητικά.
Τα Πιστοποιητικά που εκδίδονται με βάση την ΠΠ 3 πιστοποιούν την αντιστοιχία του φυσικού προσώπου (Τελικού Χρήστη) με τα στοιχεία που αναφέρονται στο έγγραφο ταυτοποίησης του.
Η ταυτοποίηση των τελικών χρηστών προϋποθέτει τη φυσική παρουσία τους ενώπιον αρμόδιων στελεχών σύμφωνα με τα προβλεπόμενα στην παρούσα πράξη, οι οποίοι ελέγχουν τα έγγραφα που τεκμηριώνουν την ταυτότητα του Τελικού Χρήστη (§3.2.3).
Τα Αναγνωρισμένα Πιστοποιητικά Τελικών Χρηστών αναφέρονται αποκλειστικά και μόνο σε φυσικά πρόσωπα. Σε κάθε περίπτωση το Αναγνωρισμένο Πιστοποιητικό συνδέεται κατ` αποκλειστικότητα με ένα φυσικό πρόσωπο το οποίο και φέρει την αποκλειστική ευθύνη για αυτό το πιστοποιητικό.

1.2.1.4 Πολιτική Πιστοποιητικού 4 (ΠΠ 4)
Η Πολιτική Πιστοποιητικού 4 (ΠΠ 4) αναφέρεται σε Αναγνωρισμένα Πιστοποιητικά Τελικών Χρηστών. Τα Πιστοποιητικά που εκδίδονται βάσει της ΠΠ 4 χρησιμοποιούνται για αυθεντικοποίηση χρήστη από φορείς που απαιτούν την ύπαρξη τομεακών αναγνωριστικών στο πιστοποιητικό και μπορούν είτε να αποθηκεύονται σε ΑΔΔΥ είτε όχι.
Η ταυτοποίηση των τελικών χρηστών προϋποθέτει τη φυσική παρουσία τους ενώπιον αρμόδιων στελεχών σύμφωνα με τα προβλεπόμενα στην παρούσα πράξη, οι οποίοι ελέγχουν τα έγγραφα που τεκμηριώνουν την ταυτότητα του Τελικού Χρήστη (§3.2.3) καθώς και τα έγγραφα - αποδεικτικά από τα οποία να προκύπτει η απόδοση του τομεακού αναγνωριστικού στον τελικό χρήστη.

1.2.1.5 Πολιτική Πιστοποιητικού 5 (ΠΠ 5)
Για την Πολιτική Πιστοποιητικού 5 (ΠΠ 5) ισχύουν όλα τα προβλεπόμενα της ΠΠ1, με την μόνη διαφορά, ότι το Αναγνωρισμένο Πιστοποιητικό εκδίδεται σε φυσικό πρόσωπο (Τελικός Χρήστης) που φέρει την ιδιότητα του νόμιμου εκπροσώπου νομικού προσώπου ή άλλο νομίμως εξουσιοδοτημένο πρόσωπο του νομικού προσώπου.
Η ταυτοποίηση των Τελικών Χρηστών προϋποθέτει τη φυσική παρουσία τους ενώπιον αρμόδιων στελεχών σύμφωνα με τα προβλεπόμενα στην παρούσα πράξη, οι οποίοι ελέγχουν τα έγγραφα που τεκμηριώνουν την ταυτότητα του Τελικού Χρήστη και τη σχέση του με το φορέα (§3.2.2 - §3.2.3).

1.2.1.6 Πολιτική Πιστοποιητικού 6 (ΠΠ 6)
Για την Πολιτική Πιστοποιητικού 6 (ΠΠ 6) ισχύουν όλα τα προβλεπόμενα της ΠΠ 2, με την μόνη διαφορά, ότι το Πιστοποιητικό εκδίδεται σε φυσικό πρόσωπο (Τελικός Χρήστης) που φέρει την ιδιότητα του νόμιμου εκπροσώπου νομικού προσώπου ή άλλο νομίμως εξουσιοδοτημένο πρόσωπο του νομικού προσώπου.
Η ταυτοποίηση των Τελικών Χρηστών προϋποθέτει τη φυσική παρουσία τους ενώπιον αρμόδιων στελεχών σύμφωνα με τα προβλεπόμενα στην παρούσα πράξη, οι οποίοι ελέγχουν τα έγγραφα που τεκμηριώνουν την ταυτότητα του Τελικού Χρήστη και τη σχέση του με το φορέα (§3.2.2 - §3.2.3).

1.2.1.7 Πολιτική Πιστοποιητικού 7 (ΠΠ 7)
Η Πολιτική Πιστοποίησης 7 (ΠΠ 7) αναφέρεται σε Πιστοποιητικά Φορέων του δημοσίου τομέα ή ανεξάρτητων διοικητικών αρχών ή ΝΠΙΔ, τα οποία χρησιμοποιούνται για ψηφιακή υπογραφή (προηγμένη ηλεκτρονική υπογραφή) και κρυπτογράφηση ηλεκτρονικών μηνυμάτων και εγγράφων που εκδίδονται από τους εν λόγω Φορείς.
Για τα Πιστοποιητικά αυτά «Τελικό Χρήστη» αποτελεί ο ίδιος ο Φορέας, στο όνομα του οποίου εκδίδεται το Πιστοποιητικό, ενώ ο εκάστοτε νόμιμος εκπρόσωπος του Φορέα, ή ο νόμιμος εκπρόσωπος του εποπτεύοντος Φορέα, ή άλλο νομίμως εξουσιοδοτημένο για αυτό το σκοπό φυσικό πρόσωπο (εφεξής «Εκπρόσωπος του Φορέα») είναι υπεύθυνος για τη διαχείριση του ως άνω Πιστοποιητικού ως «αιτών» το πιστοποιητικό (Subscriber). Τα Πιστοποιητικά αυτά δύνανται να δημιουργούνται ή/ και να αποθηκεύονται σε ΑΔΔΥ ή σε άλλη Ασφαλή Κρυπτογραφική Μονάδα. Η όποια αναφορά σε «Εκπρόσωπο Φορέα» σε αυτό το έγγραφο, αφορά τη συγκεκριμένη Πολιτική Πιστοποίησης και μόνο.

**** Η παρ. 1.2.1.7 τροποποιήθηκε ως άνω, με την ΚΥΑ με αριθμ. ΥΑΠ/Φ.60/3431 (ΦΕΚ Β 3320/27.12.2013) παρ.2.*

1.2.2 Κριτήρια ένταξης ΥπΑΠ στην παρούσα Υποδομή Δημοσίου Κλειδιού

Ως ΥπΑΠ στην παρούσα Υποδομή Δημοσίου Κλειδιού - ΥΔΚ, σύμφωνα με τις διατάξεις του παρόντος, εντάσσονται οι φορείς του δημόσιου τομέα οι οποίοι παρέχουν υπηρεσίες πιστοποίησης σύμφωνα με το άρθρο 20 του Νόμου 3448/2006 (ΦΕΚ 57/Α`) και ασκούν αρμοδιότητες για τη διεκπεραίωση των οποίων απαιτείται πιστοποίηση.
Στην παρούσα ΥΔΚ μπορούν να ενταχθούν και φορείς σύμφωνα με τις διατάξεις της παραγράφου 5 του άρθρου 20 του Νόμου 3448/2006 (ΦΕΚ 57/Α`).
Για την ένταξη ενός φορέα στην ΥΔΚ της ΑΠΕΔ, απαιτείται η αποδεδειγμένη συμμόρφωση του με όλα τα προβλεπόμενα στην παρούσα ΠΠ και η πρότερη έγκριση της ΑΠΕΔ. Ο φορέας που επιθυμεί να ενταχθεί στην παρούσα ΥΔΚ είτε αποδέχεται πλήρως τη Δήλωση Πρακτικής των Υποκείμενων Αρχών Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου είτε υποβάλει προς έλεγχο και έγκριση από την ΑΠΕΔ προτάσεις διαφοροποιήσεων της πρακτικής του, σύμφωνα με την ενότητα §1.5.3 του παρόντος.

1.2.3 Κριτήρια συμμόρφωσης Τρίτων Φορέων - Παροχών Υπηρεσιών Πιστοποίησης με τις Πολιτικές Πιστοποιητικών της ΑΠΕΔ

Προκειμένου ένας Τρίτος Φορέας - Πάροχος Υπηρεσιών Πιστοποίησης να χρησιμοποιήσει μία ή περισσότερες από τις πολιτικές πιστοποιητικών της ΑΠΕΔ, και να συμπεριλάβει τη συγκεκριμένη τιμή προσδιοριστή αντικειμένου (βλ. κατωτέρω ενότητα §1.2.5 της ΠΠ), απαιτείται η αποδεδειγμένη συμμόρφωση του με τα προβλεπόμενα στην παρούσα ΠΠ και η πρότερη έγκριση της ΑΠΕΔ. Ειδικότερα, εφαρμόζονται εν προκειμένω οι διατάξεις της παραγράφου 5, εδάφιο β` του άρθρου 20 του Νόμου 3448/2006.

1.2.4 Προσφερόμενες Υπηρεσίες της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ)

Η ΑΠΕΔ παρέχει υπηρεσίες πιστοποίησης σε Φορείς του δημόσιου τομέα που εντάσσονται στην παρούσα Υποδομή Δημοσίου Κλειδιού, σύμφωνα με την ενότητα §1.2.2 και §1.2.3 της ΠΠ ανωτέρω.

1.2.5 Τιμές Προσδιοριστή Αντικειμένου

Τα Πιστοποιητικά που εκδίδονται σύμφωνα με τις πολιτικές πιστοποιητικών της ΑΠΕΔ περιλαμβάνουν τιμές προσδιοριστή αντικειμένου (Object Identifier) που αντιστοιχούν στην εκάστοτε πολιτική πιστοποιητικού που ακολουθείται. Η τιμή προσδιοριστή αντικειμένου για την:

- ΠΠ 1 είναι: 1.2.300.0.110001.1.7.1.1.1
- ΠΠ 2 είναι: 1.2.300.0.110001.1.7.1.1.2
- ΠΠ 3 είναι: 1.2.300.0.110001.1.7.1.1.3
- ΠΠ 4 είναι: 1.2.300.0.110001.1.7.1.1.4
- ΠΠ 5 είναι: 1.2.300.0.110001.1.7.1.1.5
- ΠΠ 6 είναι: 1.2.300.0.110001.1.7.1.1.6
- ΠΠ 7 είναι: 1.2.300.0.110001.1.7.1.1.7

1.3 Συμμετέχοντες στην Υποδομή Δημοσίου Κλειδιού

Η παρούσα ΠΠ διέπει τις υπηρεσίες Υποδομής Δημοσίου Κλειδιού που παρέχονται σύμφωνα με τις διατάξεις του άρθρου 20 του Ν. 3448/2006 (ΦΕΚ 57/Α`).

1.3.1 Αρχές Πιστοποίησης

Η Πρωτεύουσα Αρχή Πιστοποίησης είναι αρμόδια για την πιστοποίηση, τον καθορισμό των κατευθύνσεων και το συντονισμό των άλλων δημοσίων υπηρεσιών ή φορέων του δημόσιου τομέα (Υποκείμενες Αρχές Πιστοποίησης), οι οποίοι διαχειρίζονται ψηφιακά πιστοποιητικά και εντάσσονται στην παρούσα Υποδομή Δημοσίου Κλειδιού ή ακολουθούν μία ή περισσότερες εκ των πολιτικών πιστοποίησης της ΑΠΕΔ, κατά τα οριζόμενα στην παράγραφο 2 του άρθρου 20 του Ν 3448/2006 (ΦΕΚ 57/ Α`), και εγγράφονται στο μητρώο Παροχών Υπηρεσιών Πιστοποίησης της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ), σύμφωνα με το άρθρο 10 του υπ` αριθ. 248/71/2002 Κανονισμού Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής (ΦΕΚ 603/Β`).
Ως εκ τούτου:

1. Η ΑΠΕΔ η οποία ενεργεί ως Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ), πιστοποιεί τις Υποκείμενες Αρχές Πιστοποίησης με την έκδοση αντίστοιχων Πιστοποιητικών.
2. Οι Υποκείμενες Αρχές Πιστοποίησης (ΥπΑΠ), εφόσον ενταχθούν στην Υποδομή Δημοσίου Κλειδιού, βάσει των διατάξεων του παρόντος και πιστοποιηθούν από την ΑΠΕΔ, σύμφωνα με τα παραπάνω, διαχειρίζονται τα Πιστοποιητικά Τελικών Χρηστών σύμφωνα με τις πολιτικές πιστοποιητικών του παρόντος και ορίζουν μια ή περισσότερες οργανικές μονάδες οι οποίες, αφού γνωστοποιηθούν στην ΑΠΕΔ, θα ασκήσουν τις

αρμοδιότητες των "Αρχών Εγγραφής" και των "Εντεταλμένων Γραφείων" (ΠΠ §1.3.2 και ΠΠ §1.3.2.1). Ειδικότερα, οι ΥπΑΠ, αναλαμβάνουν τη διαχείριση του κύκλου ζωής των ψηφιακών Πιστοποιητικών Τελικών Χρηστών (έκδοση - ανάκληση -ανανέωση - ανάκτηση κλπ.), σύμφωνα με τα προβλεπόμενα στην παρούσα ΠΠ, όπως αυτή εξειδικεύεται στην εκάστοτε Δήλωση Πρακτικής της ΥπΑΠ. Επίσης, οι ΥπΑΠ μπορούν να ασκήσουν και αρμοδιότητες της Αρχής Εγγραφής και των Εντεταλμένων Γραφείων όπως αυτές ορίζονται στις ενότητες §1.3.2 και §1.3.2.1.

3. Οι τρίτοι φορείς - Πάροχοι Υπηρεσιών Πιστοποίησης, που δεν έχουν πιστοποιηθεί από την ΑΠΕΔ, εκδίδουν και διαχειρίζονται Πιστοποιητικά Τελικών Χρηστών - Ιδιωτών και Νομικών Προσώπων Ιδιωτικού Δικαίου (ΝΠΙΔ), σύμφωνα με μία ή περισσότερες εκ των πολιτικών πιστοποιητικών που περιγράφονται στην παρούσα ΠΠ και εξειδικεύονται στην Δήλωση Πρακτικής τους, εφόσον έχουν εγκριθεί προηγουμένως από την ΑΠΕΔ.

1.3.2 Αρχές Εγγραφής

Οι Αρχές Εγγραφής (ΑΕ) προκειμένου για τη χορήγηση των ψηφιακών Πιστοποιητικών σύμφωνα με τις διατάξεις του παρόντος, είναι αρμόδιες για τον έλεγχο των αιτημάτων και των εγγραφών των Τελικών Χρηστών, και για την επιβεβαίωση των στοιχείων της ταυτότητας των Τελικών Χρηστών. Επιπλέον, οι ΑΕ ελέγχουν και εισηγούνται την ανάκληση, ανάκτηση ή ανανέωση Πιστοποιητικών, ή άλλες υποστηριζόμενες λειτουργίες του κύκλου ζωής πιστοποιητικών (π.χ. αναστολή).

1.3.2.1 Εντεταλμένα Γραφεία

Σε κάθε Αρχή Εγγραφή απευθύνεται ένας αριθμός Εντεταλμένων Γραφείων τα στελέχη των οποίων είναι αρμόδια για την επιβεβαίωση - επαλήθευση των στοιχείων ταυτότητας των Τελικών Χρηστών καθώς και την παραλαβή των αιτημάτων για έκδοση, ανανέωση, ανάκληση και ανάκτηση Πιστοποιητικών ή άλλες υποστηριζόμενες λειτουργίες του κύκλου ζωής Πιστοποιητικών Τελικών Χρηστών (π.χ. αναστολή) και αναφέρονται στην προϊσταμένη Αρχή (ή Αρχές) Εγγραφής.

1.3.3 Τελικοί Χρήστες

Ως Τελικοί Χρήστες νοούνται τα φυσικά πρόσωπα, κάτοχοι Πιστοποιητικών σύμφωνα με τις διατάξεις του παρόντος. Ειδικά για τα πιστοποιητικά που εκδίδονται σύμφωνα με την ΠΠ 1, ΠΠ 3 και ΠΠ 5 οι Τελικοί Χρήστες θα πρέπει να έχουν δικαιοπρακτική ικανότητα.

Για Πιστοποιητικά που εκδίδονται σύμφωνα με την ΠΠ 7 ως Τελικός Χρήστης νοείται ο φορέας του δημοσίου τομέα, στο όνομα του οποίου εκδίδεται το Πιστοποιητικό.

1.3.4 Τρίτοι Συμμετέχοντες

Ως Τρίτοι Συμμετέχοντες νοούνται τα φυσικά ή νομικά πρόσωπα που ενεργούν βάσει εμπιστοσύνης σε κάποιο Πιστοποιητικό που έχει εκδοθεί σύμφωνα με τις διατάξεις του παρόντος. Ο Τρίτος Συμμετέχοντας μπορεί να είναι, ή και να μην είναι, Τελικός Χρήστης εντός της ΥΔΚ της ΑΠΕΔ.

1.4 Εφαρμογή των Πιστοποιητικών

1.4.1 Εγκεκριμένες Χρήσεις Πιστοποιητικών

Οι προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε Πιστοποιητικά που ακολουθούν την ΠΠ 1 ή την ΠΠ 5 και έχουν δημιουργηθεί από ασφαλή διάταξη δημιουργίας υπογραφής επέχουν θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο όπως αναφέρεται στην κείμενη εθνική νομοθεσία (ΠΔ150/2001). Τα Πιστοποιητικά που ακολουθούν την ΠΠ 1 ή την ΠΠ 5, αποτελούν Πιστοποιητικά ηλεκτρονικής υπογραφής ή/και Πιστοποιητικά αυθεντικοποίησης (ανάλογα με την τιμή που ορίζεται στα πεδία KeyUsage και Extended Key Usage που περιλαμβάνουν, σύμφωνα με την ενότητα §7.1.2.1).

Το ζεύγος κλειδιών που περιλαμβάνεται στα Πιστοποιητικά που ακολουθούν την ΠΠ 2 ή την ΠΠ 6 χρησιμοποιούνται για κρυπτογράφηση δεδομένων και εγγράφων.

Οι προηγμένες ηλεκτρονικές υπογραφές που βασίζονται σε Πιστοποιητικά που ακολουθούν την ΠΠ 3 και δεν έχουν δημιουργηθεί από ασφαλή διάταξη δημιουργίας υπογραφής, ανταποκρίνονται στην παράγραφο 2 του άρθρου 3 του ΠΔ 150/2001, η οποία προβλέπει ότι η ισχύς της ηλεκτρονικής υπογραφής ή το παραδεκτό της ως αποδεικτικού στοιχείου δεν αποκλείεται από μόνο το λόγο ότι δε συντρέχουν οι προϋποθέσεις της παραγράφου 1 του ίδιου άρθρου. Επομένως η ΠΠ 3 σκοπό έχει να διευκολύνει εφαρμογές για προηγμένες ηλεκτρονικές υπογραφές όπου το επίπεδο ισχύος που παρέχεται από το άρθρο 3 παράγραφος 2 του ΠΔ 150/2001 είναι κατάλληλο και επαρκές. Δηλαδή τα Αναγνωρισμένα Πιστοποιητικά που εκδίδονται σύμφωνα με την ΠΠ 3 υποστηρίζουν τη χρήση ψηφιακών

υπογραφών των οποίων δεν θα αμφισβητηθεί η νομική αποτελεσματικότητα απλά και μόνο επειδή δε συνδυάζονται με τη χρήση ΑΔΔΥ.
Τα Πιστοποιητικά που ακολουθούν την ΠΠ 3, αποτελούν Πιστοποιητικά Ηλεκτρονικής Υπογραφής ή/ και Πιστοποιητικά Αυθεντικοποίησης (ανάλογα με την τιμή που ορίζεται στα πεδία KeyUsage και Extended Key Usage που περιλαμβάνουν, σύμφωνα με την ενότητα §7.1.2.1).
Τα Πιστοποιητικά που ακολουθούν την ΠΠ 4 χρησιμοποιούνται αποκλειστικά και μόνο για την αυθεντικοποίηση του Τελικού Χρήστη, όπου η χρήση τομεακών αναγνωριστικών κρίνεται απαραίτητη, και όχι για ηλεκτρονική υπογραφή.
Τα Πιστοποιητικά που ακολουθούν την ΠΠ 7 χρησιμοποιούνται για την ψηφιακή υπογραφή μηνυμάτων και εγγράφων που εκδίδονται από τον Φορέα του δημόσιου τομέα, στο όνομα του οποίου έχει εκδοθεί το Πιστοποιητικό, καθώς και για την κρυπτογράφηση μηνυμάτων και εγγράφων που αποστέλλονται προς τον εν λόγω φορέα.
Τα Πιστοποιητικά Τελικών Χρηστών που εκδίδονται για φυσικά πρόσωπα είναι αυστηρώς προσωπικά και χρησιμοποιούνται στα πλαίσια που προβλέπονται από τις Δηλώσεις Πρακτικής των εκδοτριών ΑΠ.
Οι εφαρμογές στις οποίες μπορούν να χρησιμοποιηθούν τα Πιστοποιητικά Τελικών Χρηστών που θα παρασχεθούν βάσει της Υποδομής Δημοσίου Κλειδιού του παρόντος και με την χρήση προηγμένης ηλεκτρονικής υπογραφής, όπου απαιτείται, δύνανται να είναι αποκλειστικά μία ή περισσότερες από τις εξής:

- Έλεγχος πρόσβασης
- Ασφαλής προσδιορισμός ηλεκτρονικής ταυτότητας
- Προσδιορισμός του Υπευθύνου για κάθε σχετική ηλεκτρονική επικοινωνία / συναλλαγή
- Υπογραφή και κρυπτογράφηση ηλεκτρονικών αρχείων (π.χ. αρχεία Adobe Acrobat)
- Ασφαλής χρήση ηλεκτρονικού ταχυδρομείου / μηνυμάτων (υπογραφή και κρυπτογράφηση)

1.4.1.1 Μελλοντικές χρήσεις πιστοποιητικών τελικών χρηστών
Ενδεχόμενες μελλοντικές χρήσεις Πιστοποιητικών Τελικών Χρηστών θα προσδιοριστούν κατόπιν αποφάσεως της ΑΠΕΔ.

1.4.1.2 Περιορισμοί στη χρήση των πιστοποιητικών
Τα πιστοποιητικά που είναι σύμφωνα με τις ΠΠ 1, ΠΠ 3 και ΠΠ 5, έχουν περιορισμούς στη χρήση τους όπως ορίζεται στην §1.4.1 του παρόντος. Σε κάθε περίπτωση οι διατάξεις του παρόντος δε θίγουν διατάξεις που αναφορικά με τη σύναψη και την ισχύ συμβάσεων ή εν γένει νομικών υποχρεώσεων, επιβάλλουν τη χρήση ορισμένου τύπου, ούτε διατάξεις για την αποδεικτική ή άλλη χρήση εγγράφων ή διατάξεις με τις οποίες απαγορεύεται να διακινούνται και να καθίστανται γνωστά έγγραφα ορισμένων κατηγοριών και δεδομένα προσωπικού χαρακτήρα, σύμφωνα και με τις διατάξεις της παρ. 2 του άρθρου 1 του Π.Δ. 150/2001 (ΦΕΚ 25/Α`).

1.4.2 Μη εγκεκριμένες εφαρμογές
Τα Πιστοποιητικά δεν έχουν σχεδιαστεί, δεν αποσκοπούν και δεν είναι εγκεκριμένα να χρησιμοποιηθούν σε περιπτώσεις όπου απαιτείται τήρηση στοιχείων υψηλής διαβάθμισης ή συνθηκών υψηλής ασφάλειας (όπως για παράδειγμα, εθνική άμυνα και ασφάλεια). Εξάλλου, απαγορεύεται η χρήση των Πιστοποιητικών για σκοπούς άλλους από εκείνους για τους οποίους αυστηρά εκδόθηκαν.

1.5 Διαχείριση Πολιτικής
1.5.1 Οργανισμός που διαχειρίζεται το έγγραφο
Την παρούσα ΠΠ εκδίδει και τροποποιεί η ΑΠΕΔ, ως Πρωτεύουσα Αρχή Πιστοποίησης σύμφωνα με τις διατάξεις της παραγράφου 2 του άρθρου 20 του Ν.3448/2006 (ΦΕΚ 57/Α). Τυχόν αιτήματα για διευκρινίσεις επί των κεφαλαίων του παρόντος θα απευθύνονται προς την ΑΠΕΔ.

1.5.2 Στοιχεία επικοινωνίας
Τα στοιχεία επικοινωνίας για την Αρχή Πιστοποίησης του Ελληνικού Δημοσίου δημοσιεύονται στις παρακάτω ιστοσελίδες:

- http://www.yap.gov.gr
- http://www.ermis.gov.gr
- http://www.syzefxis.gov.gr

1.5.3 Έγκριση Καταλληλότητας Δήλωσης Πρακτικής για την Πολιτική Πιστοποιητικών

Η ΑΠΕΔ εξετάζει και εγκρίνει τις Δηλώσεις Πρακτικής των εκδοτριών ΑΠ αναφορικά με την καταλληλότητα και συμμόρφωση τους σε τεχνικά, διαδικαστικά και συναφή ζητήματα, με τις απαιτήσεις του παρόντος. Τροποποιήσεις στις εγκεκριμένες Δηλώσεις Πρακτικής απαιτούν επίσης την προηγούμενη έγκριση της ΑΠΕΔ.
Τροποποιήσεις επί του παρόντος απαιτούν την εκ νέου συμμόρφωση των εκδοτριών ΑΠ, σε χρονικό διάστημα που θα ορίζει η ΑΠΕΔ, και έγκριση από την ΑΠΕΔ των εκάστοτε Δηλώσεων Πρακτικής.

1.5.3.1 Διαδικασίες Έγκρισης Δήλωσης Πρακτικής

Η ΑΠΕΔ λαμβάνει τα αναγκαία μέτρα, διαθέτει τον κατάλληλο μηχανισμό και τα μέσα για την επεξεργασία και έλεγχο συμμόρφωσης των Δηλώσεων Πρακτικής των εκδοτριών ΑΠ, και των ενδεχόμενων τροποποιήσεων τους με την παρούσα ΠΠ.

1.6 Ορισμοί και ακρωνύμια

Στο Παράρτημα Α παρατίθεται Πίνακας Ορισμών και Ακρωνυμίων.

2. Δημοσίευση και Χώρος Αποθήκευσης

2.1 Χώροι Αποθήκευσης

Η ΑΠΕΔ διασφαλίζει τη λειτουργία ηλεκτρονικού χώρου αποθήκευσης για την Πρωτεύουσα Αρχή Πιστοποίησης (ΑΠΕΔ). Οι εκδότριες ΑΠ διασφαλίζουν επίσης ένα δημοσίως προσβάσιμο ηλεκτρονικό χώρο αποθήκευσης για τις υπηρεσίες ΥΔΚ που προσφέρουν.

2.2 Δημοσίευση Πληροφοριών

Τόσο η ΑΠΕΔ όσο και οι εκδότριες ΑΠ διασφαλίζουν ένα δημοσίως προσβάσιμο χώρο αποθήκευσης που βρίσκεται σε δικτυακό κόμβο, ο οποίος επιτρέπει στους Τρίτους Συμμετέχοντες να ελέγχουν την κατάσταση των Πιστοποιητικών μέσω της έκδοσης Καταλόγων Ανακληθέντων Πιστοποιητικών (ΚΑΠ-CRL).
Η ΑΠΕΔ εκδίδει Καταλόγους Ανακληθέντων Πιστοποιητικών για τις ΥπΑΠ, ενώ η κάθε εκδότρια ΑΠ εκδίδει Καταλόγους Ανακληθέντων Πιστοποιητικών για τα Πιστοποιητικά τελικών χρηστών που έχει εκδώσει.
Με την ανάκληση ενός Πιστοποιητικού ΥπΑΠ η ΑΠΕΔ δημοσιεύει αναγγελία της ανάκλησης αυτής στο χώρο αποθήκευσης τους. Με την ανάκληση ενός Πιστοποιητικού Τελικού Χρήστη, οι εκδότριες ΑΠ δημοσιεύουν άμεσα την ανάκληση αυτή σύμφωνα με τους προβλεπόμενους στην παρούσα ΠΠ μηχανισμούς (§4.9.6 και §4.9.8). Για το σκοπό αυτό οι εκδότριες ΑΠ δύναται να παρέχουν και υπηρεσίες δικτυακού ελέγχου κατάστασης πιστοποιητικών σε πραγματικό χρόνο (Online Certificate Status Protocol - OCSP).
Η ΑΠΕΔ δημοσιεύει την παρούσα ΠΠ στο χώρο αποθήκευσης που βρίσκεται στο δικτυακό της κόμβο.
Η κάθε εκδότρια ΑΠ δημοσιεύει στο χώρο αποθήκευσης που βρίσκεται στον δικτυακό της κόμβο την παρούσα ΠΠ, τη Δήλωση Πρακτικής της, τους Όρους Χρήσης Πιστοποιητικού (ΟΧΠ) και τους Όρους Τρίτου Συμμετέχοντα (ΟΤΣ).
Τέλος, οι εκδότριες ΑΠ δημοσιεύουν τα Πιστοποιητικά Τελικών Χρηστών που εγκρίνουν, εφόσον:

- είναι αναγκαίο για το σκοπό της χρήσης των Πιστοποιητικών, και
- δεν τίθεται σχετικός περιορισμός από την ισχύουσα νομοθεσία περί προστασίας δεδομένων προσωπικού χαρακτήρα.

Στην περίπτωση που συντρέχουν οι ως άνω προϋποθέσεις, οι εκδότριες ΑΠ παρέχουν στους Τρίτους Συμμετέχοντες πληροφορίες σχετικά με την τοποθεσία δημοσίευσης και τον τρόπο αναζήτησης των Πιστοποιητικών Τελικών Χρηστών που εκδίδουν.

2.2.1 Δημοσίευση της ΠΠ

Η παρούσα ΠΠ δημοσιεύεται σε ηλεκτρονική μορφή στο Χώρο Αποθήκευσης της ΑΠΕΔ στη διεύθυνση http:// www.yap.gov.gr όπου βρίσκεται διαθέσιμη σε μορφή εγγράφου Adobe Acrobat® pdf ή/και Microsoft Word® ή HTML. Η ΑΠΕΔ επίσης
διαθέτει την ΠΠ σε μορφή Adobe Acrobat® pdf ή Microsoft Word ®στις διευθύνσεις http:// www.ermis.gov.gr και http://www.syzefxis.gov.gr.

2.2.2 Στοιχεία που δεν δημοσιεύονται στην ΠΠ

Τα έγγραφα ασφαλείας που θεωρούνται εμπιστευτικά από την ΑΠΕΔ δεν αποκαλύπτονται σε τρίτους.

2.3 Χρόνος ή Συχνότητα Δημοσίευσης

Η ΑΠΕΔ ανακοινώνει τις τροποποιήσεις της ΠΠ, μέσα σε εύλογο χρονικό διάστημα στο τμήμα του Χώρου Αποθήκευσης της που προορίζεται για Ενημερώσεις και Ανακοινώσεις επί των Πολιτικών, στις διευθύνσεις που αναφέρονται στην ενότητα §2.2.1.

Τα Πιστοποιητικά Τελικών Χρηστών δημοσιεύονται κατά την έκδοση. Πληροφορίες αναφορικά με την κατάσταση Πιστοποιητικών δημοσιεύονται σύμφωνα με τις §4.9.6 και §4.9.8 της ΠΠ.

2.4 Έλεγχοι Πρόσβασης σε Χώρους Αποθήκευσης

Η ΑΠΕΔ διασφαλίζει την εφαρμογή και υλοποίηση λογικών και φυσικών μέτρων ασφαλείας προκειμένου να αποτραπεί η προσθήκη, διαγραφή ή τροποποίηση των καταχωρήσεων στο χώρο αποθήκευσης από μη εξουσιοδοτημένα πρόσωπα. Το αυτό αποτελεί υποχρέωση για τις εκδότριες ΑΠ αναφορικά με το χώρο αποθήκευσης τους.

Η ΑΠΕΔ και οι εκδότριες ΑΠ, δεν χρησιμοποιούν τεχνικά μέσα για τον περιορισμό πρόσβασης στην παρούσα ΠΠ και τις δικές τους Δηλώσεις Πρακτικής, Πιστοποιητικά, και πληροφορίες κατάστασης Πιστοποιητικών ή τους ΚΑΠ, κ.α.

Ωστόσο, οι εκδότριες ΑΠ, δύναται να απαιτούν από τους τρίτους την προηγούμενη αποδοχή των Όρων Τρίτου Συμμετέχοντα, ως προϋπόθεση της χρήσης Πιστοποιητικών, πληροφοριών κατάστασης Πιστοποιητικών ή ΚΑΠ.

3. Αναγνώριση και Ταυτοποίηση

3.1 Ονοματοδοσία

Τα ονόματα που εμφανίζονται στα Πιστοποιητικά, τα οποία συμμορφώνονται με μία ή περισσότερες από τις πολιτικές πιστοποιητικών της ΑΠΕΔ, επαληθεύονται.

3.1.1 Τύποι Ονομάτων

Τα Πιστοποιητικά που εκδίδει η ΑΠΕΔ για την πιστοποίηση των ΥπΑΠ, περιλαμβάνουν Διακριτικά Ονόματα X.501 στα πεδία Εκδότη και Υποκειμένου. Τα Διακριτικά Ονόματα των ΥπΑΠ της ΑΠΕΔ αποτελούνται από τα στοιχεία που προσδιορίζονται παρακάτω στον Πίνακα 2.

Πίνακας 2: Χαρακτηριστικά Διακριτικού Ονόματος ΥπΑΠ

Χαρακτηριστικό	Τιμή
Country (C) - Χώρα=	"GR"
Organizational Unit (OU) – Οργανική Μονάδα =	Τα Πιστοποιητικά των ΥπΑΠ της ΑΠΕΔ δύναται να περιέχουν ένα ή περισσότερα OU. Το περιεχόμενο αυτών μπορεί να σχετίζεται με τη χρήση των Πιστοποιητικών αυτών (π.χ. “CA for Public Bodies” εάν η ΑΠ εκδίδει πιστοποιητικά μόνο για φορείς).
Common Name (CN) – Κοινό Όνομα =	Το χαρακτηριστικό αυτό περιλαμβάνει το Κοινό Όνομα της ΥπΑΠ (CA name).

Τα Πιστοποιητικά Τελικού Χρήστη που εκδίδονται σύμφωνα με τις πολιτικές πιστοποίησης που ορίζονται στην παρούσα ΠΠ περιλαμβάνουν διακριτικό όνομα X.501 στο πεδίο ονόματος Υποκειμένου και αποτελούνται από τα στοιχεία που προσδιορίζονται στον Πίνακα 3. Οι τιμές που περιλαμβάνουν τα επιμέρους πεδία εξειδικεύονται στην εκάστοτε Δήλωση Πρακτικής της Αρχής Πιστοποίησης, όπου αυτό κρίνεται απαραίτητο.

Πίνακας 3: Χαρακτηριστικά Διακριτικού Ονόματος σε Πιστοποιητικά Τελικού Χρήστη

Χαρακτηριστικό	Τιμή
Country (C) - Χώρα=	"GR"
Organization (0) - Οργανισμός =	Το πεδίο αυτό δύναται να περιλαμβάνει πρόσθετες πληροφορίες αναφορικά με τον φορέα ή οργανισμό στον οποίο υπάγεται ο Τελικός Χρήστης. Για Πιστοποιητικά Τελικών Χρηστών που εκδίδονται βάσει της ΠΠ 5 και ΠΠ 6 το πεδίο αυτό περιέχει στοιχεία αναφορικά με το νομικό πρόσωπο το οποίο ο κάτοχος του Πιστοποιητικού εκπροσωπεί (§7.1.4). Για Πιστοποιητικά που εκδίδονται βάσει της ΠΠ 7 το πεδίο αυτό περιλαμβάνει την επίσημη ονομασία του φορέα στον οποίο υπάγεται η Υπηρεσία του Δημοσίου, Ν.Π.Δ.Δ., ή Ο.Τ.Α. για την οποία εκδίδεται το Πιστοποιητικό.
Organizational Unit (OU) – Οργανική Μονάδα =	Τα Πιστοποιητικά Τελικού Χρήστη δύναται να περιέχουν ένα ή περισσότερα OU. Το περιεχόμενο αυτών μπορεί να περιέχει πρόσθετες πληροφορίες αναφορικά με τον φορέα

	στον οποίο υπάγεται ο Τελικός Χρήστης ή άλλες πληροφορίες κατά τη διακριτική ευχέρεια της εκδότριας ΑΠ. Για Πιστοποιητικά Τελικών Χρηστών που εκδίδονται βάσει της ΠΠ 5 και ΠΠ 6 το πεδίο αυτό περιέχει πρόσθετα στοιχεία αναφορικά με το νομικό πρόσωπο το οποίο ο κάτοχος του Πιστοποιητικού εκπροσωπεί (§7.1.4). Για Πιστοποιητικά που εκδίδονται βάσει της ΠΠ 7 το πεδίο αυτό περιλαμβάνει πρόσθετες πληροφορίες αναφορικά με το φορέα στον οποίο υπάγεται ο κάτοχος ή την Υπηρεσία του Δημοσίου, Ν.Π.Δ.Δ., ή Ο.Τ.Α. για την οποία εκδίδεται το Πιστοποιητικό. Στα Πιστοποιητικά φυσικών προσώπων (ΠΠ 1 – ΠΠ 6) σε ξεχωριστό πεδίο OU αναγράφεται το ονοματεπώνυμο του φυσικού προσώπου με ελληνικούς χαρακτήρες, όπου αυτό έχει εφαρμογή, και με τη μορφή «Όνομα Επίθετο».
Common Name (CN)– Κοινό Όνομα =	Το χαρακτηριστικό αυτό περιλαμβάνει το Ονοματεπώνυμο του Τελικού Χρήστη με λατινικούς χαρακτήρες και με τη μορφή «Όνομα Επώνυμο», όπως αναγράφεται στο επίσημο έγγραφο που προσκομίζεται κατά τη διαδικασία της εγγραφής, σύμφωνα με την ενότητα §3.2.3 της ΠΠ. Η διατύπωση των ονομάτων των φυσικών προσώπων με λατινικούς χαρακτήρες γίνεται με τη χρήση του προτύπου ΕΛΟΤ 743 (εκτός και αν αυτό αναγράφεται με διαφορετικό τρόπο στο προσκομισθέν κατά την εγγραφή δικαιολογητικό – §3.2.3). Για Πιστοποιητικά που εκδίδονται βάσει της ΠΠ 7 το πεδίο αυτό περιλαμβάνει την επίσημη Αγγλική ονομασία του Φορέα του δημόσιου τομέα για τον οποίον εκδίδεται το Πιστοποιητικό.
Surname (SN) – Επώνυμο =	Τα χαρακτηριστικό αυτό περιλαμβάνει το επώνυμο (ένα ή περισσότερα) του Τελικού Χρήστη με λατινικούς χαρακτήρες (με χρήση του προτύπου ΕΛΟΤ 743, εκτός και αν αναγράφεται με διαφορετικό τρόπο στο προσκομισθέν κατά την εγγραφή δικαιολογητικό). Για Πιστοποιητικά που εκδίδονται βάσει της ΠΠ 7 το πεδίο αυτό δε χρησιμοποιείται
Given name (G) – Όνομα =	Το χαρακτηριστικό αυτό περιλαμβάνει το όνομα (ή ονόματα) του Τελικού Χρήστη με λατινικούς χαρακτήρες (με χρήση του προτύπου ΕΛΟΤ 743, εκτός και αν αναγράφεται με διαφορετικό τρόπο στο προσκομισθέν κατά την εγγραφή δικαιολογητικό). Για Πιστοποιητικά που εκδίδονται βάσει της ΠΠ 7 το πεδίο αυτό δε χρησιμοποιείται
Serial Number – Σειριακός Αριθμός =	Το χαρακτηριστικό αυτό περιλαμβάνει τον Κωδικό Διαχείρισης Πιστοποιητικού του Τελικού Χρήστη. Για Πιστοποιητικά που εκδίδονται βάσει της ΠΠ 7 το πεδίο αυτό δε χρησιμοποιείται.

3.1.2 Ανάγκη Κατανόησης των Ονομάτων

Τα ονόματα που περιλαμβάνονται στα Πιστοποιητικά Τελικού Χρήστη βρίσκονται σε μορφή απλή και κατανοητή ώστε να επιτρέπουν τον προσδιορισμό της ταυτότητας του φυσικού προσώπου που αποτελεί το Υποκείμενο του Πιστοποιητικού.

3.1.3 Ανωνυμία ή ψευδωνυμία τελικού χρήστη

Κατά τη διαδικασία εγγραφής διασφαλίζεται η τήρηση των διατάξεων της κείμενης νομοθεσίας για την προστασία των προσωπικών δεδομένων.

Όταν απαιτείται από την νομοθεσία ή ζητείται από ένα φορέα ο οποίος πρόκειται να είναι και ο Τρίτος Συμμετέχοντας η προστασία της ταυτότητας του Τελικού Χρήστη, ένα Πιστοποιητικό δύναται να εκδίδεται με ψευδώνυμο, υποδεικνύοντας ότι η ταυτότητα του Τελικού Χρήστη έχει επαληθευτεί αλλά προστατεύεται.

Οι εκδότριες ΑΠ που εκδίδουν Πιστοποιητικά με χρήση ψευδωνύμου περιγράφουν στη Δήλωση Πρακτικής τους τις προϋποθέσεις παροχής και χρήσης της συγκεκριμένης δυνατότητας.

3.1.4 Μοναδικότητα των Ονομάτων

Οι εκδότριες ΑΠ της ΑΠΕΔ διασφαλίζουν ότι τα διακριτικά ονόματα Υποκειμένου είναι μοναδικά μέσω αυτοματοποιημένων διαδικασιών κατά τη διαδικασία εγγραφής των Τελικών Χρηστών.

Στις περιπτώσεις συνωνυμίας τελικών χρηστών, οι εκδότριες ΑΠ διασφαλίζουν τη μοναδικότητα του ονόματος μέσω των διαδικασιών ελέγχου της συνωνυμίας και επίλυσης διαφορών, που περιγράφονται στην εφαρμοστέα Δήλωση Πρακτικής τους.

3.1.5 Αναγνώριση και Αυθεντικοποίηση

Σε κάθε περίπτωση, οι Τελικοί Χρήστες δεν πρέπει να χρησιμοποιούν ονόματα στις Αιτήσεις τους που παραβιάζουν δικαιώματα πνευματικής ιδιοκτησίας τρίτων.

3.2 Αρχική Εγγραφή

3.2.1 Μέθοδος Απόδειξης της Κατοχής Ιδιωτικού Κλειδιού

Οι εκδότριες ΑΠ επαληθεύουν ότι ο ενδιαφερόμενος Τελικός Χρήστης κατέχει το ιδιωτικό κλειδί υπογραφής μέσω της χρήσης ψηφιακά υπογεγραμμένου αιτήματος πιστοποιητικού σύμφωνα με το PKCS #10 (Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού), άλλη ισοδύναμη κρυπτογραφικά μορφή ή άλλη μέθοδο εγκεκριμένη από την ΑΠΕΔ.

3.2.2 Μέθοδος Απόδειξης της Ταυτότητας Οργανισμού

3.2.2.1 Μέθοδος Απόδειξης της Ταυτότητας Νομικού Προσώπου (ΠΠ 5 και ΠΠ 6)

Για όλα τα Πιστοποιητικά που ακολουθούν την ΠΠ 5 και ΠΠ 6, οι Αρχές Εγγραφής των εκδοτριών Αρχών Πιστοποίησης, πέρα των αναφερομένων στην ενότητα §3.2.3 κατωτέρω, επιβεβαιώνουν ότι:

- Ο Τελικός Χρήστης είναι ο νόμιμος εκπρόσωπος του νομικού προσώπου που έχει δηλώσει στην Αίτηση για Πιστοποιητικά.
- Το νομικό πρόσωπο υφίσταται και λειτουργεί νόμιμα.
- Ο Τελικός Χρήστης έχει εξουσιοδοτηθεί από το νομικό πρόσωπο να προμηθευτεί ψηφιακά Πιστοποιητικά.
- Ο Αριθμός Φορολογικού Μητρώου (ΑΦΜ) του νομικού προσώπου, που ο Τελικός Χρήστης έχει δηλώσει στην Αίτηση για Πιστοποιητικά, είναι ορθός και αληθής.

Τα απαιτούμενα δικαιολογητικά που υποβάλλονται από τον Τελικό Χρήστη είναι, πέρα από τα αναφερόμενα στην ενότητα §3.2.3, τα κάτωθι:

- Νομιμοποιητικά έγγραφα (ή επικυρωμένα αντίγραφα αυτών) από τα οποία να προκύπτει η απόδοση Αριθμού Φορολογικού Μητρώου (ΑΦΜ) του νομικού προσώπου που εκπροσωπεί ο Τελικός Χρήστης ή τελευταία Βεβαίωση Μεταβολής Στοιχείων Νομικού Προσώπου.
- Νομιμοποιητικά έγγραφα (ή επικυρωμένα αντίγραφα αυτών) του νομικού προσώπου για λογαριασμό του οποίου ο Τελικός Χρήστης θα ενεργεί ως νόμιμος εκπρόσωπος στις συναλλαγές του, από τα οποία να προκύπτει ρητά ότι ο Τελικός Χρήστης έχει εξουσιοδοτηθεί, ώστε να ενεργεί με το Πιστοποιητικό του για λογαριασμό του συγκεκριμένου νομικού προσώπου.
- Άλλα απαραίτητα έγγραφα που περιγράφονται στη Δήλωση Πρακτικής της εκδότριας ΑΠ.

3.2.2.2 Μέθοδος Απόδειξης της Ταυτότητας Φορέα του Δημοσίου Τομέα (ΠΠ 7)

Για όλα τα Πιστοποιητικά που ακολουθούν την ΠΠ 7, οι Αρχές Εγγραφής των εκδοτριών Αρχών Πιστοποίησης, επιβεβαιώνουν κατ` ελάχιστον ότι:

- Ο φορέας υφίσταται και λειτουργεί νόμιμα.
- Το φυσικό πρόσωπο που αιτείται την έκδοση του Πιστοποιητικού, είναι Εκπρόσωπος του Φορέα κατά τη στιγμή που υποβάλλεται η Αίτηση.

Σε κάθε περίπτωση, ο Φορέας υποχρεούται να ενημερώσει την Αρχή Εγγραφής για τις όποιες αλλαγές υφίστανται αναφορικά με την νόμιμη εκπροσώπηση του και την ανάθεση αρμοδιοτήτων σε νέο Εκπρόσωπο του Φορέα.

3.2.3 Μέθοδος Απόδειξης της Ταυτότητας Φυσικού Προσώπου

3.2.3.1 Πιστοποιητικά Φυσικών Προσώπων

Για όλα τα Πιστοποιητικά φυσικών προσώπων, η αρμόδια Αρχή Εγγραφής ή/και εκδότρια Αρχή Πιστοποίησης, επιβεβαιώνουν ότι:

- Ο Τελικός Χρήστης ή ο νόμιμος Εκπρόσωπος είναι το πρόσωπο που προσδιορίζεται στην Ηλεκτρονική Εγγραφή ή Αίτηση για Πιστοποιητικά.
- Ο Τελικός Χρήστης διαθέτει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που αναγράφεται στο Πιστοποιητικό σύμφωνα με την §3.2.1 της ΠΠ.
- Οι πληροφορίες που περιλαμβάνονται στο Πιστοποιητικό είναι ακριβείς.
- Η πιστοποίηση της ταυτότητας του Τελικού Χρήστη ή νόμιμου Εκπροσώπου γίνεται με την προσωπική (φυσική) επαφή του με στέλεχος του Εντεταλμένου Γραφείου, ή όπου αυτό κρίνεται απαραίτητο, με στέλεχος της Αρχής Εγγραφής, ή της Εκδότριας ΑΠ, όπου ελέγχεται η ταυτότητα του από το δελτίο αστυνομικής του ταυτότητας ή άλλο επίσημο έγγραφο - παραστατικό της ταυτότητας του προσώπου που φέρει επικυρωμένη φωτογραφία.

Τα απαιτούμενα δικαιολογητικά που υποβάλλονται από τον Τελικό Χρήστη είναι:

- Επικυρωμένο φωτοαντίγραφο του αστυνομικού δελτίου ταυτότητας ή άλλου επίσημου εγγράφου - αποδεικτικού της ταυτότητας του φυσικού προσώπου.
- Άλλα απαραίτητα έγγραφα που περιγράφονται στη Δήλωση Πρακτικής της εκδότριας ΑΠ.
- Πρόσθετα έγγραφα - αποδεικτικά από τα οποία να προκύπτει η απόδοση του τομεακού αναγνωριστικού στον τελικό χρήστη, όταν αυτά απαιτείται να συμπεριληφθούν σε πιστοποιητικό που εκδίδεται σύμφωνα με την ΠΠ 4.
- Πρόσθετα έγγραφα τα οποία να τεκμηριώνουν την προσθήκη στοιχείων στα πεδία Organization (O) και Organization Unit (OU) του Διακριτικού Ονόματος του Υποκειμένου, όπου αυτό απαιτείται.

3.2.3.2 Πιστοποιητικά Φορέων

Για τα Πιστοποιητικά Φορέων (ΠΠ 7), η αρμόδια Αρχή Εγγραφής ή/και εκδότρια Αρχή Πιστοποίησης, επιβεβαιώνουν ότι:

- Ο Εκπρόσωπος του Φορέα είναι το πρόσωπο που προσδιορίζεται στην Ηλεκτρονική Εγγραφή ή Αίτηση για Πιστοποιητικά.
- Ο Τελικός Χρήστης διαθέτει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που αναγράφεται στο Πιστοποιητικό σύμφωνα με την §3.2.1 της ΠΠ.
- Οι πληροφορίες που περιλαμβάνονται στο Πιστοποιητικό είναι ακριβείς.
- Η πιστοποίηση της ταυτότητας του προσώπου που υποβάλλει την αίτηση γίνεται με την προσωπική (φυσική) επαφή του με στέλεχος του Εντεταλμένου Γραφείου, ή όπου αυτό κρίνεται απαραίτητο, με στέλεχος της Αρχής Εγγραφής, ή της Εκδότριας ΑΠ, όπου ελέγχεται η ταυτότητα του από το δελτίο αστυνομικής του ταυτότητας ή άλλο επίσημο έγγραφο - παραστατικό της ταυτότητας του προσώπου που φέρει επικυρωμένη φωτογραφία.

Τα απαιτούμενα δικαιολογητικά που υποβάλλονται από τον Εκπρόσωπο του Φορέα είναι:

- Επικυρωμένο φωτοαντίγραφο του αστυνομικού δελτίου ταυτότητας ή άλλου επίσημου εγγράφου - αποδεικτικού της ταυτότητας του φυσικού προσώπου.
- Νομιμοποιητικά έγγραφα από τα οποία να προκύπτει ότι το φυσικό πρόσωπο αποτελεί το νόμιμο εκπρόσωπο του φορέα, ή νόμιμο εκπρόσωπο του εποπτεύοντος φορέα, ή άλλο νομίμως εξουσιοδοτημένο για το σκοπό αυτό πρόσωπο.
- Εξουσιοδότηση από τον νόμιμο εκπρόσωπο του φορέα, ή το νόμιμο εκπρόσωπο του εποπτεύοντος φορέα, όπου έχει εφαρμογή.
- Άλλα απαραίτητα έγγραφα που περιγράφονται στη Δήλωση Πρακτικής της εκδότριας ΑΠ.

3.2.4 Πληροφορίες Τελικού Χρήστη που Δεν Επαληθεύονται

Τα πιστοποιητικά των Τελικών Χρηστών δε περιλαμβάνουν πληροφορίες που δεν επαληθεύονται.

3.2.5 Επαλήθευση Δικαιωμάτων

Για τα Πιστοποιητικά που ακολουθούν την ΠΠ 5, ΠΠ 6 οι Αρχές Εγγραφής των εκδοτριών ΑΠ επαληθεύουν (§3.2.2)ότι ο Τελικός Χρήστης έχει εξουσιοδοτηθεί και δικαιούται να αιτηθεί Πιστοποιητικά προκειμένου να ενεργεί για λογαριασμό του νομικού προσώπου που δηλώνει στην Αίτηση για Πιστοποιητικό.

Για τα Πιστοποιητικά που ακολουθούν την ΠΠ 7, η αρμόδια Αρχή Εγγραφής ή η εκδότρια Αρχή Πιστοποίησης, επαληθεύουν ότι το φυσικό πρόσωπο που αιτείται το Πιστοποιητικό είναι, τη στιγμή υποβολής της Αίτησης, ο νόμιμος εκπρόσωπος του φορέα, ή νόμιμος εκπρόσωπος του εποπτευόμενου φορέα, ή φυσικό πρόσωπο που έχει εξουσιοδοτηθεί για αυτό το σκοπό, και στο όνομα του οποίου θα επαληθευτεί το Πιστοποιητικό.

3.2.6 Κριτήρια Διαλειτουργικότητας

Η ΑΠΕΔ μπορεί να παρέχει υπηρεσίες διαλειτουργικότητας οι οποίες προσφέρουν σε Αρχές Πιστοποίησης εκτός της Υποδομής της ΑΠΕΔ, τη δυνατότητα να διασφαλίζουν διαλειτουργικότητα με την ΥΔΚ της ΑΠΕΔ, πιστοποιώντας μονόπλευρα την συγκεκριμένη ΑΠ. Οι ΑΠ που διαθέτουν αυτές τις δυνατότητες διαλειτουργικότητας θα συμμορφώνονται προς την παρούσα ΠΠ και κάθε επιπλέον πολιτική που προστίθεται σε αυτή όταν απαιτείται.

Η ΑΠΕΔ θα επιτρέπει τη διαλειτουργικότητα μεταξύ αυτής και Αρχών Πιστοποίησης εκτός της δικής της ΥΔΚ, σε περιπτώσεις κατά τις οποίες η ενδιαφερόμενη Αρχή Πιστοποίησης πληροί τις ακόλουθες ελάχιστες προϋποθέσεις:

- Συνάπτει σύμβαση με την ΑΠΕΔ.
- Λειτουργεί σύμφωνα με Δήλωση Πρακτικής η οποία πληροί τις απαιτήσεις της παρούσας Πολιτικής Πιστοποιητικών ως προς τις πολιτικές πιστοποιητικών που πρόκειται να εκδίδει.

- Υποβάλλεται σε αξιολόγηση συμμόρφωσης προτού της επιτραπεί η διαλειτουργικότητα.
- Υποβάλλεται σε ετήσια αξιολόγηση συμμόρφωσης για να διασφαλιστεί ότι εξακολουθεί να πληροί τις προϋποθέσεις διαλειτουργικότητας.

3.3 Ταυτοποίηση και Αυθεντικό ποίηση για Επαναδημιουργία Κλειδιών

3.3.1 Ταυτοποίηση και Αυθεντικοποίηση για Τακτική Επαναδημιουργία Κλειδιών

Για τα Πιστοποιητικά τελικού χρήστη, τα οποία δεν έχουν ανακληθεί και είναι σε ισχύ, είναι δυνατή η ανανέωση τους με ταυτόχρονη επαναδημιουργία κλειδιών, σύμφωνα με τις καταγεγραμμένες διαδικασίες στις Δηλώσεις Πρακτικής των εκδοτριών ΑΠ, οι οποίες επιβεβαιώνουν ότι ο χρήστης που αιτείται την επαναδημιουργία κλειδιών είναι πράγματι το Υποκείμενο του Πιστοποιητικού ή εξουσιοδοτημένο προς το σκοπό αυτό πρόσωπο.

3.3.2 Ταυτοποίηση και Αυθεντικοποίηση για Επαναδημιουργία Κλειδιών Μετά την Ανάκληση

Η Επαναδημιουργία Κλειδιών μετά την ανάκληση δεν είναι δυνατή εφόσον:

- Η ανάκληση συνέβη επειδή τα Πιστοποιητικά εκδόθηκαν προς πρόσωπο διαφορετικό από αυτό το οποίο κατονομάζεται ως το Υποκείμενο του Πιστοποιητικού.
- Τα Πιστοποιητικά εκδόθηκαν χωρίς τη συγκατάθεση του προσώπου το οποίο κατονομάζεται ως Υποκείμενο τους, ή του εξουσιοδοτημένου για αυτό το σκοπό φυσικού προσώπου.
- Το πρόσωπο το οποίο εγκρίνει την Ηλεκτρονική Εγγραφή ή Αίτηση του Τελικού Χρήστη για Πιστοποιητικά ανακαλύπτει ή έχει λόγο να πιστεύει ότι ορισμένα ουσιώδη στοιχεία στην Ηλεκτρονική Εγγραφή η Αίτηση για Πιστοποιητικά είναι ψευδή.

Υπό τους ανωτέρω όρους, τα Πιστοποιητικά Τελικού Χρήστη, τα οποία έχουν ανακληθεί ή έχουν λήξει, είναι δυνατόν να αντικατασταθούν (να ξαναδημιουργηθούν τα ζεύγη κλειδιών), σύμφωνα με τις §3.4, §3.2.3 της ΠΠ και όπου εφαρμόζεται της §3.2.2 και §3.2.2.2.

3.4 Ταυτοποίηση και Αυθεντικοποίηση για Αίτηση Ανάκλησης

Για την ανάκληση Πιστοποιητικών Τελικών Χρηστών ακολουθούνται καταγεγραμμένες, στις Δηλώσεις Πρακτικής των εκδοτριών ΑΠ διαδικασίες, οι οποίες επιβεβαιώνουν ότι ο χρήστης που αιτείται την ανάκληση είναι πράγματι το υποκείμενο του Πιστοποιητικού ή εξουσιοδοτημένο προς το σκοπό αυτό πρόσωπο.

4. Λειτουργικές Απαιτήσεις Κύκλου Ζωής Πιστοποιητικών

4.1 Αίτηση για Έκδοση Πιστοποιητικού

4.1.1 Ποιος Μπορεί να Υποβάλλει Αίτηση για Έκδοση Πιστοποιητικού

Για την έκδοση Πιστοποιητικού Τελικού Χρήστη, το πρόσωπο που μπορεί να υποβάλει αίτηση Πιστοποιητικού είναι το φυσικό πρόσωπο που αποτελείτο Υποκείμενο του Πιστοποιητικού.

Όταν πρόκειται για Πιστοποιητικά Τελικού Χρήστη που εκδίδονται για λογαριασμό νομικών προσώπων (ΠΠ 5 και ΠΠ 6), το πρόσωπο που μπορεί να υποβάλει αίτηση Πιστοποιητικού είναι το φυσικό πρόσωπο που φέρει την ιδιότητα του νόμιμου εκπροσώπου του νομικού προσώπου ή άλλο νομίμως εξουσιοδοτημένο πρόσωπο του νομικού προσώπου.

Για την έκδοση Πιστοποιητικού Φορέα (ΠΠ 7) το φυσικό πρόσωπο που μπορεί να υποβάλλει Αίτηση Πιστοποιητικού φέρει την ιδιότητα του νόμιμου Εκπροσώπου του Φορέα κατά τη συγκεκριμένη χρονική στιγμή, ή νόμιμου εκπροσώπου του εποπτεύοντος φορέα, ή άλλου νομίμως εξουσιοδοτημένου για το σκοπό αυτό προσώπου.

Για την έκδοση Πιστοποιητικού Αρχής Εγγραφής, το πρόσωπο που μπορεί να υποβάλει αίτηση Πιστοποιητικού είναι κάθε εξουσιοδοτημένος εκπρόσωπος της Αρχής Εγγραφής.

Για την έκδοση Πιστοποιητικού Αρχής Πιστοποίησης, το πρόσωπο που μπορεί να υποβάλει αίτηση Πιστοποιητικού είναι κάθε εξουσιοδοτημένος εκπρόσωπος της Αρχής Πιστοποίησης.

4.1.2 Διαδικασίες για τη χορήγηση Πιστοποιητικού

4.1.2.1 Διαδικασίες για τη χορήγηση Πιστοποιητικού Τελικού Χρήστη

Για τη χορήγηση Πιστοποιητικών Τελικού Χρήστη, όλοι οι Τελικοί Χρήστες υποβάλλονται σε διαδικασία εγγραφής και επαλήθευσης της ταυτότητας, η οποία περιγράφεται στις Δηλώσεις Πρακτικής των εκδοτριών ΑΠ, και η οποία τουλάχιστον συνίσταται σε:

- Φυσική παρουσία του ίδιου του Τελικού Χρήστη, ή του Εκπροσώπου του Φορέα στην περίπτωση της ΠΠ 7, σε αρμόδιο Εντεταλμένο Γραφείο ή, όπου αυτό κρίνεται απαραίτητο, σε εκπροσώπους της Αρχής Εγγραφής ή της Εκδότριας ΑΠ.
- Γραπτή ή ηλεκτρονική αποδοχή των Όρων Χρήσης Πιστοποιητικού (ΟΧΠ).
- Δημιουργία ή υποβολή αιτήματος για δημιουργία ζεύγους κλειδιών σύμφωνα με την §6.1 της ΠΠ.
- Αποστολή του δημόσιου κλειδιού από τον Τελικό Χρήστη, στην εκδότρια ΑΠ, σύμφωνα με την §6.1.3 της ΠΠ.
- Ο Τελικός Χρήστης αποδεικνύει στην εκδότρια ΑΠ σύμφωνα με την §3.2.1 της ΠΠ ότι έχει στην κατοχή του το ιδιωτικό κλειδί υπογραφής που αντιστοιχεί στο δημόσιο κλειδί που απέστειλε στην εκδότρια ΑΠ.

Τα αρχεία που διατηρούνται σύμφωνα με την §5.5.1 της ΠΠ περιλαμβάνουν τις πληροφορίες που χρησιμοποιούνται για να ταυτοποιήσουν τον Τελικό Χρήστη, ή τον Εκπρόσωπο του Φορέα στην περίπτωση της ΠΠ 7 (συμπεριλαμβανομένου οιουδήποτε στοιχείου που χρησιμοποιείται για την ταυτοποίηση), καθώς και ένα αρχείο των Όρων Χρήσης Πιστοποιητικού (ΟΧΠ) είτε σε χαρτί είτε σε ηλεκτρονική μορφή.

Στην περίπτωση μιας αίτησης για ανανέωση ή επανέκδοση:

- οποιεσδήποτε αλλαγές στους ΟΧΠ μετά από την προηγούμενη εγγραφή ή επανεγγραφή είναι σύμφωνες με την §2.2 της ΠΠ και
- τα αρχεία που διατηρούνται σύμφωνα με την §5.5.1 της ΠΠ επίσης περιλαμβάνουν τη συγκατάθεση του Τελικού Χρήστη, ή του Εκπροσώπου του Φορέα στην περίπτωση της ΠΠ7, για τις παραπάνω αλλαγές.

4.2 Επεξεργασία Αίτησης Έκδοσης Πιστοποιητικού

4.2.1 Έκδοση Πιστοποιητικού Τελικού Χρήστη

Με την υποβολή των απαραίτητων νομιμοποιητικών εγγράφων, εξουσιοδοτημένος υπάλληλος του Εντεταλμένου Γραφείου ή, όπου αυτό κρίνεται απαραίτητο, της Αρχής Εγγραφής ή της Εκδότριας ΑΠ, επιβεβαιώνει τα στοιχεία ταυτοποίησης σύμφωνα με την §3.2.2 και §3.2.3 της ΠΠ. Με την επιτυχή τέλεση όλων των απαιτούμενων διαδικασιών ταυτοποίησης η ΑΠ θα προχωρήσει στην έκδοση των σχετικών Πιστοποιητικών. Εφόσον η ταυτοποίηση δεν είναι επιτυχής, αντίστοιχα θα την απορρίψει.
Τα Πιστοποιητικά Τελικού Χρήστη δημιουργούνται και εκδίδονται μετά την έγκριση από την ΑΠ της Αίτησης που υποβάλλεται από τον Τελικό Χρήστη ή τον Εκπρόσωπο του Φορέα στην περίπτωση της ΠΠ 7. Η εκδότρια ΑΠ δημιουργεί και εκδίδει Πιστοποιητικά προς τον ενδιαφερόμενο Τελικό Χρήστη βάσει των στοιχείων που ο ίδιος έχει υποβάλλει και εφόσον έχει εγκρίνει την Αίτηση για Πιστοποιητικά.
Οι διαδικασίες της παραγράφου αυτής ισχύουν επίσης και για την έκδοση πιστοποιητικών μετά από υποβολή αιτήματος επαναδημιουργίας κλειδιών σύμφωνα με την §3.3.

4.2.2 Έκδοση Πιστοποιητικού ΥπΑΠ

Η ΑΠΕΔ ως Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ) πιστοποιεί Υποκείμενες Αρχές Πιστοποίησης και υπογράφει τα αντίστοιχα Πιστοποιητικά ΥπΑΠ σύμφωνα με τα προβλεπόμενα στις διατάξεις του άρθρου 20 του Ν.3448/2006 και την §1.2.2 της ΠΠ.

4.2.3 Χρόνος Επεξεργασίας Αιτήσεων

Οι ΑΠ και οι ΑΕ ξεκινούν την επεξεργασία των αιτήσεων για Πιστοποιητικό μέσα σε εύλογο χρονικό διάστημα από την παραλαβή τους. Δεν υπάρχει συγκεκριμένη πρόβλεψη σχετικά με το χρόνο ολοκλήρωσης της επεξεργασίας των αιτήσεων, εκτός εάν δηλώνεται κάτι διαφορετικό στη σχετικούς ΟΧΠ ή στη Δήλωση Πρακτικής της εκδότριας ΑΠ. Οι αιτήσεις για Πιστοποιητικό παραμένουν εν ενεργεία μέχρι την απόρριψη τους.

4.3 Έκδοση Πιστοποιητικού

4.3.1 Ενέργειες της εκδότριας ΑΠ κατά τη Διάρκεια Έκδοσης Πιστοποιητικού Τελικού Χρήστη

Το Πιστοποιητικό δημιουργείται και εκδίδεται μετά τη διαβίβαση αιτήματος έκδοσης πιστοποιητικού από την ΑΕ και τη σχετική έγκριση από την εκδότρια ΑΠ. Η εκδότρια ΑΠ δημιουργεί και εκδίδει Πιστοποιητικό προς τον Τελικό Χρήστη βάσει των στοιχείων της Αίτησης για Πιστοποιητικό και εφόσον έχει εγκρίνει την Αίτηση αυτή.

4.3.2 Ενημέρωση του Τελικού Χρήστη για την Έκδοση Πιστοποιητικού

Οι εκδότριες ΑΠ που εκδίδουν Πιστοποιητικά σε Τελικούς Χρήστες κοινοποιούν, είτε απευθείας είτε μέσω μιας ΑΕ, στους Τελικούς Χρήστες τη δημιουργία αυτών των Πιστοποιητικών και τους τρόπους πρόσβασης στα Πιστοποιητικά, ειδοποιώντας τους ότι τα Πιστοποιητικά είναι διαθέσιμα και ενημερώνοντας τους σχετικά με τους τρόπους με τους οποίους θα τα παραλάβουν.

Τα Πιστοποιητικά καθίστανται διαθέσιμα στους Τελικούς Χρήστες, είτε επιτρέποντας τους να τα "φορτώσουν" από κάποιον δικτυακό τόπο ή μέσω μηνύματος το οποίο αποστέλλεται στον Τελικό Χρήστη και το οποίο εμπεριέχει αυτό το Πιστοποιητικό.

4.4 Αποδοχή Πιστοποιητικού

4.4.1 Ενέργειες που Αποτελούν Αποδοχή Πιστοποιητικού

Η χρήση του Πιστοποιητικού ή η μη απόρριψη του Πιστοποιητικού ή του περιεχομένου του από τον Τελικό Χρήστη μέσα σε εύλογο χρονικό διάστημα, συνιστούν την αποδοχή του Πιστοποιητικού από τον Τελικό Χρήστη.

4.4.2 Δημοσίευση Πιστοποιητικού από την Αρχή Πιστοποίησης

Η ΑΠΕΔ δημοσιεύει το Πιστοποιητικό της καθώς και τα Πιστοποιητικά ΥπΑΠ που εκδίδει σύμφωνα με τον ακόλουθο Πίνακα 4.

Πίνακας 4: Απαιτήσεις Δημοσίευσης

Μορφή Πιστοποιητικού	Απαιτήσεις Δημοσίευσης
Πιστοποιητικό ΑΠΕΔ	Διαθέσιμα στους Τρίτους Συμμετέχοντες, διαδικτυακά μέσω του χώρου αποθήκευσής της ΑΠΕΔ καθώς και ως μέρος της Αλυσίδας Πιστοποιητικού η οποία ενσωματώνεται στο Πιστοποιητικό Τελικού Χρήστη μέσω των λειτουργιών αναζήτησης που περιγράφονται παρακάτω.
Πιστοποιητικά ΥπΑΠ	Διαθέσιμα στους Τρίτους Συμμετέχοντες, διαδικτυακά μέσω των χώρων αποθήκευσής της ΑΠΕΔ και των εκδοτριών ΑΠ, καθώς και ως μέρος της Αλυσίδας Πιστοποιητικού η οποία ενσωματώνεται στο Πιστοποιητικό Τελικού Χρήστη μέσω των λειτουργιών αναζήτησης που περιγράφονται παρακάτω.

Οι εκδότριες ΑΠ δημοσιεύουν Πιστοποιητικά τα οποία εκδίδουν σε χώρο πληροφοριών προσβάσιμο από το κοινό. Επίσης τα Πιστοποιητικά Τελικού Χρήστη είναι διαθέσιμα μέσω αναζήτησης στον εξυπηρετητή (server) του καταλόγου LDAP της εκδότριας ΑΠ.

4.4.2.1 Αποτύπωμα Πιστοποιητικού ΑΠΕΔ

Τα αποτυπώματα των πιστοποιητικών της ΑΠΕΔ είναι:

- Πιστοποιητικό υπογεγραμμένο με ShalRSA, και με αλγόριθμο αποτύπωσης τον sha1:"31 53 41 d3 dO 05 d3 41 37 a7 42 eb 83 d3 02 5e 58 e8 33 b6"
- Πιστοποιητικό υπογεγραμμένο με Sha256RSA, και με αλγόριθμο αποτύπωσης τον sha1:"d1 40 88 fa 00 2c 8b 13 00 15 86 19 96 6a 10 38 91 3a a8f2"

Το αναγνωριστικό κλειδιού της ΑΠΕΔ είναι:"32 49 40 49 88 16 1d 6a ab c4 24 29 c8 27 c4 49 fb 4f 61 0b".

4.4.3 Ενημέρωση Έκδοσης Πιστοποιητικού από την Αρχή Πιστοποίησης προς Άλλες Οντότητες

Οι εκδότριες ΑΠ δύνανται να ενημερώνουν τις ΑΕ σχετικά με την έκδοση των Πιστοποιητικών που οι εκδότριες ΑΠ έχουν εγκρίνει.

4.5 Ζεύγος κλειδιών και Χρήση Πιστοποιητικών

4.5.1 Χρήση Ιδιωτικού Κλειδιού και Πιστοποιητικού από Τελικό Χρήστη

Η χρήση του Ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί που περιλαμβάνεται στο Πιστοποιητικό θα επιτρέπεται μόνο εφόσον ο Τελικός Χρήστης έχει συμφωνήσει με τους ΟΧΠ και έχει αποδεχθεί το Πιστοποιητικό. Το Πιστοποιητικό θα χρησιμοποιείται σύμφωνα με τους ΟΧΠ, τους όρους της παρούσας ΠΠ και της εφαρμοστέας Δήλωσης Πρακτικής της εκδότριας ΑΠ. Επιπλέον, η χρήση του Πιστοποιητικού θα πρέπει να συμμορφώνεται με τις επεκτάσεις τομέα Χρήσης Κλειδιού (KeyUsage) του Πιστοποιητικού.

Οι Τελικοί Χρήστες θα προστατεύουν τα ιδιωτικά κλειδιά τους από μη εξουσιοδοτημένη χρήση και θα διακόπτουν τη χρήση τους μετά τη λήξη ή την ανάκληση του Πιστοποιητικού.

4.5.2 Χρήση Δημοσίου Κλειδιού και Πιστοποιητικού από Τρίτο Συμμετέχοντα

Οι Τρίτοι Συμμετέχοντες αποδέχονται τους εφαρμόσιμους Όρους Τρίτου Συμμετέχοντα ως προϋπόθεση για να εμπιστευθούν το Πιστοποιητικό. Η εξάρτηση από Πιστοποιητικό πρέπει να είναι εύλογη σύμφωνα με τις περιστάσεις.

Πριν από οποιαδήποτε ενέργεια, η οποία θα έχει ως αποτέλεσμα να εμπιστευτούν κάποιο Πιστοποιητικό, οι Τρίτοι Συμμετέχοντες θα αξιολογούν ανεξάρτητα και με δική τους ευθύνη:

- Την καταλληλότητα της χρήσης του Πιστοποιητικού για τον δεδομένο σκοπό, ότι η χρήση του Πιστοποιητικού δεν αντίκειται στην ΠΠ και ότι το Πιστοποιητικό χρησιμοποιείται σύμφωνα με τις επεκτάσεις του πεδίου Χρήσης Κλειδιού (KeyUsage) του Πιστοποιητικού.
- Την κατάσταση του Πιστοποιητικού και όλων των ΑΠ στην αλυσίδα έκδοσης του Πιστοποιητικού. Εάν κάποιο από τα Πιστοποιητικά της Αλυσίδας Πιστοποιητικών έχει ανακληθεί, ο Τρίτος Συμμετέχοντας φέρει αποκλειστικά την ευθύνη διερεύνησης του κατά πόσον είναι εύλογο να βασιστεί σε μια ψηφιακή υπογραφή που πραγματοποιήθηκε από έναν Τελικό Χρήστη πριν την ανάκληση του Πιστοποιητικού της Αλυσίδας Πιστοποιητικών. Σε αυτή την περίπτωση, η ευθύνη της εμπιστοσύνης στο Πιστοποιητικό βαρύνει αποκλειστικά τον Τρίτο Συμμετέχοντα.

Εφόσον η χρήση του Πιστοποιητικού είναι η κατάλληλη, οι Τρίτοι Συμμετέχοντες θα πρέπει να χρησιμοποιούν το κατάλληλο λογισμικό ή/και εξοπλισμό για να εμπιστευθούν κάποιο Πιστοποιητικό και να επιτύχουν επαλήθευση της ψηφιακής υπογραφής ή να εκτελέσουν άλλες κρυπτογραφικές εφαρμογές.

Η ΑΠΕΔ και οι εκδότριες ΑΠ δε φέρουν ευθύνη για την αξιολόγηση της καταλληλότητας χρήσης των Πιστοποιητικών.

4.6 Ανανέωση Πιστοποιητικού

4.6.1 Συνθήκες για Ανανέωση Πιστοποιητικού

Η ανανέωση Πιστοποιητικού αποτελεί την έκδοση ενός νέου Πιστοποιητικού προς το Υποκείμενο του Πιστοποιητικού χωρίς αλλαγή του δημόσιου κλειδιού ή οποιουδήποτε άλλου στοιχείου του Πιστοποιητικού. Η ανανέωση Πιστοποιητικού υποστηρίζεται για τα Πιστοποιητικά ΥπΑΠ, σύμφωνα με τον Πίνακα 5 που ακολουθεί, και ο οποίος περιγράφει τις απαιτήσεις της ΑΠΕΔ για ανανέωση των Πιστοποιητικών που εκδίδει για τις ΥπΑΠ.

Πίνακας 5: Απαιτήσεις Ανανέωσης

Μορφή Πιστοποιητικού	Απαιτήσεις Ανανέωσης
Πιστοποιητικά Τελικού Χρήστη	Τα Πιστοποιητικά Τελικού Χρήστη δεν ανανεώνονται. Για τα Πιστοποιητικά αυτά υποστηρίζεται μόνο η δυνατότητα επαναδημιουργίας κλειδιών.
Πιστοποιητικά ΥπΑΠ	Παρέχεται η δυνατότητα της ανανέωσης Πιστοποιητικών χωρίς την υποχρέωση επαναδημιουργίας του ζεύγους κλειδιών, εφόσον ο αθροιστικός πιστοποιημένος χρόνος ζωής του ζεύγους κλειδιών της ΥπΑΠ δεν υπερβαίνει το εκάστοτε ανώτερο όριο διάρκειας ισχύος ζεύγους κλειδιών ΥπΑΠ όπως καθορίζεται στην §6.3.2 της ΠΠ.

4.6.2 Ποιος Μπορεί να Αιτηθεί Ανανέωση

Ανανέωση των Πιστοποιητικών ΥπΑΠ μπορεί να αιτηθεί ο νόμιμος εκπρόσωπος της ΥπΑΠ.

4.6.3 Επεξεργασία Αίτησης Ανανέωσης Πιστοποιητικού

Οι διαδικασίες ανανέωσης Πιστοποιητικού αποσκοπούν στην επιβεβαίωση ότι η οντότητα που επιδιώκει την ανανέωση ενός Πιστοποιητικού είναι στην πραγματικότητα το Υποκείμενο του Πιστοποιητικού (ή εξουσιοδοτημένος εκπρόσωπος αυτού). Για την ανανέωση του Πιστοποιητικού ΥπΑΠ διενεργείται Τελετή Δημιουργίας Κλειδιών, σύμφωνα με την §6.1.1 της ΠΠ.

4.6.4 Δημοσίευση και Ενημέρωση Χρήστη για την Έκδοση Νέου Πιστοποιητικού

Η ΑΠΕΔ καθιστά διαθέσιμα τα ανανεωμένα Πιστοποιητικά των ΥπΑΠ στους Τελικούς Χρήστες και τους Τρίτους Συμμετέχοντες από το χώρο αποθήκευσης της.

Τα Πιστοποιητικά ΑΠ της ΑΠΕΔ μπορούν επίσης να "φορτωθούν" από Κατάλογο Lightweight Directory Access Protocol (LDAP).

Οι εκδότριες ΑΠ καθιστούν διαθέσιμη την πλήρη αλυσίδα Πιστοποιητικών ΑΠ στον Τελικό Χρήστη κατά την έκδοση ενός Πιστοποιητικού.

4.7 Επαναδημιουργία Κλειδιών Πιστοποιητικού

4.7.1 Συνθήκες Επαναδημιουργίας Κλειδιών Πιστοποιητικού

Το Υποκείμενο του Πιστοποιητικού πριν από τη λήξη τους είναι απαραίτητο να αποκτήσει ένα νέο ζεύγος κλειδιών ώστε να διασφαλίσει τη συνέχεια της χρήσης τους. Για αυτό οι εκδότριες ΑΠ απαιτούν από τον Τελικό Χρήστη να δημιουργήσει ένα νέο ζεύγος κλειδιών υπογραφής το οποίο θα αντικαταστήσει το ζεύγος κλειδιών υπογραφής που λήγει (τεχνικά ορίζεται ως "επαναδημιουργία κλειδιών"). Το ίδιο ισχύει και για τα Πιστοποιητικά των ΑΠ. Ο Πίνακας 6 κατωτέρω περιγράφει τις απαιτήσεις της ΑΠΕΔ για τακτική επαναδημιουργία κλειδιών.

Πίνακας 6: Απαιτήσεις Επαναδημιουργίας Κλειδιών

Μορφή Πιστοποιητικού	Απαιτήσεις Ανανέωσης
Πιστοποιητικά Τελικού Χρήστη	Ουσιαστικός όρος για την αποδοχή της ανανέωσης ενός Πιστοποιητικού Τελικού Χρήστη είναι ο έλεγχος των πληροφοριών που διενεργείται από την εκδότρια ΑΠ για να επιβεβαιωθεί ότι η ταυτότητα του Τελικού Χρήστη είναι ακόμα έγκυρη. Αυτή η διαδικασία γίνεται με σκοπό να επιβεβαιωθεί ότι το πρόσωπο που επιδιώκει να ανανεώσει ένα Πιστοποιητικό Τελικού Χρήστη είναι στην πραγματικότητα ο Τελικός Χρήστης του Πιστοποιητικού ή ο Εκπρόσωπος του Φορέα για την περίπτωση της ΠΠ 7, όπως αναφέρεται στην §3.2.2, §3.2.2.2 και §3.2.3 της ΠΠ.
Πιστοποιητικά ΥπΑΠ και ΑΠΕΔ	Η επαναδημιουργία κλειδιών ΑΠ γίνεται κάτω από αυστηρά μέτρα ελέγχου, σε ειδικές Τελετές Δημιουργίας Κλειδιών σύμφωνα με την §6.1.1 της Πολιτικής Πιστοποιητικών.

4.7.2 Ποιος Μπορεί να Αιτηθεί Πιστοποίηση Νέου Κλειδιού

Πιστοποίηση νέου κλειδιού μπορεί να αιτηθεί μόνο ο ίδιος ο Τελικός Χρήστης ή ο Εκπρόσωπος του Φορέα στην περίπτωση της ΠΠ 7.

4.7.3 Επεξεργασία Αιτημάτων Επαναδημιουργίας Κλειδιών Πιστοποιητικού

Οι διαδικασίες επαναδημιουργίας κλειδιών Πιστοποιητικού αποσκοπούν στην επιβεβαίωση ότι το πρόσωπο που επιδιώκει την επαναδημιουργία κλειδιών ενός Πιστοποιητικού Τελικού Χρήστη είναι στην πραγματικότητα το Υποκείμενο του Πιστοποιητικού ή ο Εκπρόσωπος του Φορέα στην περίπτωση της ΠΠ 7.

4.7.4 Ενημέρωση Χρήστη για την Έκδοση Νέου Πιστοποιητικού.

Η κοινοποίηση έκδοσης Πιστοποιητικού με επαναδημιουργημένα κλειδιά στον Τελικό Χρήστη ή στον Εκπρόσωπο του Φορέα στην περίπτωση της ΠΠ 7, πραγματοποιείται σύμφωνα με τα προβλεπόμενα στην §4.3.2 της ΠΠ.

4.7.5 Ενέργειες που Αποτελούν Αποδοχή Πιστοποιητικού με Νέο Κλειδί

Οι ενέργειες Αποδοχής Πιστοποιητικού με επαναδημιουργημένα κλειδιά περιγράφονται στην §4.4.1 της ΠΠ.

4.7.6 Δημοσίευση του Νέου Πιστοποιητικού από την Αρχή Πιστοποίησης

Οι εκδότριες ΑΠ δημοσιεύουν τα Πιστοποιητικά με επαναδημιουργημένα κλειδιά σε χώρο πληροφοριών προσβάσιμο από το κοινό, σύμφωνα με την §4.4.2 της ΠΠ.

4.7.7 Ενημέρωση Άλλων Οντοτήτων της Έκδοσης Πιστοποιητικού από την Αρχή Πιστοποίησης

Οι εκδότριες ΑΠ δύνανται να ενημερώνουν τις ΑΕ σχετικά με την έκδοση των Πιστοποιητικών που οι τελευταίες έχουν εγκρίνει.

4.8 Μετατροπή Πιστοποιητικού

Δεν προβλέπεται η δυνατότητα Μετατροπής Πιστοποιητικού. Όταν ένα ή περισσότερα από τα στοιχεία του Πιστοποιητικού μεταβάλλονται, τότε εκδίδεται νέο Πιστοποιητικό, σύμφωνα με τις διαδικασίες αρχικής εγγραφής που περιγράφονται στην §4.1 της ΠΠ.

4.9 Αναστολή και Ανάκληση Πιστοποιητικού

4.9.1 Συνθήκες Ανάκλησης

4.9.1.1 Συνθήκες για Ανάκληση Πιστοποιητικών Τελικού Χρήστη

Ένα Πιστοποιητικό Τελικού Χρήστη ανακαλείται εφόσον:

1. Η ΑΠΕΔ ή η εκδότρια ΑΠ ή ένας Τελικός Χρήστης έχουν σοβαρές υπόνοιες ότι έχει υπάρξει Έκθεση σε Κίνδυνο του ιδιωτικού κλειδιού ενός Τελικού Χρήστη.
2. Η ΑΠΕΔ ή η εκδότρια ΑΠ έχει σοβαρές υπόνοιες ότι ο Τελικός Χρήστης έχει παραβεί ουσιωδώς μια σημαντική υποχρέωση ή εγγύηση σύμφωνα με τους ισχύοντες ΟΧΠ.
3. Υπάρχει απώλεια της ΑΔΔΥ ή των μυστικών αριθμών PIN-PUK από τον Τελικό Χρήστη.
4. Αδυναμία χρήσης ενός ή και όλων των Πιστοποιητικών του Τελικού Χρήστη για τεχνικούς λόγους.
5. Οι ΟΧΠ έχουν τροποποιηθεί και δεν έχουν γίνει αποδεκτοί από τον Τελικό Χρήστη.
6. Η ΑΠΕΔ ή η εκδότρια ΑΠ έχει λόγο να πιστεύει ότι το Πιστοποιητικό έχει εκδοθεί με τρόπο που δεν είναι ουσιαστικά σύμφωνος με τις διαδικασίες που απαιτούνται από την εφαρμοστέα Δήλωση Πρακτικής, ότι το Πιστοποιητικό εκδόθηκε προς πρόσωπο διαφορετικό από αυτό που κατονομάζεται ως το Υποκείμενο του Πιστοποιητικού ή χωρίς την έγκριση του προσώπου που κατονομάζεται ως το Υποκείμενο του Πιστοποιητικού αυτού.
7. Η ΑΠΕΔ ή η εκδότρια ΑΠ έχει λόγο να πιστεύει ότι κάποιο ουσιαστικό στοιχείο της Ηλεκτρονικής Αίτησης ή εγγραφής για Πιστοποιητικά είναι ψευδές.
8. Η ΑΠΕΔ ή η εκδότρια ΑΠ αποφαίνεται ότι δεν ικανοποιείται ή υπάρχει
1. απόκλιση από μια βασική προϋπόθεση για την Έκδοση Πιστοποιητικού.
9. Οι πληροφορίες που περιλαμβάνονται στο Πιστοποιητικό είναι ανακριβείς ή έχουν μεταβληθεί.
10. Ο Τελικός Χρήστης (ή εξουσιοδοτημένος εκπρόσωπος αυτού) έχει ζητήσει ανάκληση του Πιστοποιητικού σύμφωνα με την §4.9.3 της ΠΠ.
11. Για οποιαδήποτε άλλο λόγο αναφέρεται στη Δήλωση Πρακτικής της εκδότριας ΑΠ, και δεν αντιβαίνει στα οριζόμενα στην παρούσα ΠΠ.
12. Για όλους τους λόγους που αναφέρονται στην Απόφαση της ΕΕΤΤ υπ` αριθ, 248/71 "Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής", άρθρο 5 (ΦΕΚ 603/ Β`/16.05.2002).

Η ΑΠΕΔ ή η εκδότρια ΑΠ δύναται να ανακαλέσει ένα Πιστοποιητικό Υπεύθυνου ΑΕ εφόσον η απόφαση βάσει της οποίας του έχουν εκχωρηθεί αυτές οι αρμοδιότητες έχει τροποποιηθεί.
Οι ΟΧΠ των εκδοτριών ΑΠ απαιτούν από τους Τελικούς Χρήστες να ενημερώσουν άμεσα την εκδότρια ΑΠ εάν γνωρίζουν ή έχουν υπόνοιες για την έκθεση σε κίνδυνο του ιδιωτικού τους κλειδιού σύμφωνα με τις διαδικασίες της §4.9.3 της ΠΠ.
Για πιστοποιητικά που έχουν εκδοθεί σύμφωνα με την ΠΠ 7 η μεταβίβαση αρμοδιοτήτων σε νέο Εκπρόσωπο του Φορέα είναι δυνατή χωρίς την ανάκληση του πιστοποιητικού του φορέα.

4.9.1.2 Συνθήκες Ανάκλησης Πιστοποιητικών που εκδίδει η ΑΠΕΔ

Η ΑΠΕΔ ανακαλεί πιστοποιητικά που εκδίδει για τις ΥπΑΠ, εφόσον:

- Ανακαλύψει ή έχει λόγο να πιστεύει ότι έχει υπάρξει έκθεση σε κίνδυνο του ιδιωτικού κλειδιού ΥπΑΠ.
- Ανακαλύψει ή έχει λόγο να πιστεύει ότι το Πιστοποιητικό ΥπΑΠ έχει εκδοθεί με τρόπο που δεν είναι ουσιαστικά σύμφωνος με τις διαδικασίες που απαιτούνται από την παρούσα ΠΠ, ότι το Πιστοποιητικό ΥπΑΠ εκδόθηκε για Φορέα άλλον από αυτόν που κατονομάζεται ως το Υποκείμενο του πιστοποιητικού ΥπΑΠ ή χωρίς την έγκριση αυτού.
- Διαπιστώσει ότι δεν τηρούνται οι όροι της παρούσας ΠΠ ή υπάρχει παραίτηση από μια ουσιώδη προϋπόθεση για την Έκδοση Πιστοποιητικού ΥπΑΠ.
- Η ΑΠΕΔ παύσει να λειτουργεί ως ΑΠ.

4.9.2 Ποιος Μπορεί να Ζητήσει Ανάκληση

4.9.2.1 Ποιος Μπορεί να Ζητήσει Ανάκληση Πιστοποιητικού Τελικού Χρήστη

Η ΑΠΕΔ ή η εκδότρια ΑΠ δύναται να ζητήσει την ανάκληση οιουδήποτε Πιστοποιητικού Τελικού Χρήστη που έχει εκδώσει σύμφωνα με την §4.9.1.1 της ΠΠ.
Οι Τελικοί Χρήστες (ή εξουσιοδοτημένοι εκπρόσωποι αυτών) δύνανται να ζητήσουν ανάκληση των δικών τους Πιστοποιητικών.

4.9.2.2 Ποιος Μπορεί να Ζητήσει Ανάκληση Πιστοποιητικού ΥπΑΠ

Η ΑΠΕΔ ή η ΥπΑΠ έχει δικαίωμα να ζητήσει την ανάκληση πιστοποιητικού ΥπΑΠ που έχει εκδοθεί για την τελευταία, σύμφωνα με τις διατάξεις του άρθρου 20 του Ν. 3448/2006.

4.9.3 Διαδικασία για Υποβολή Αιτήματος Ανάκλησης Πιστοποιητικού

Ένας Τελικός Χρήστης που επιθυμεί ανάκληση του Πιστοποιητικού του πρέπει να υποβάλλει αίτημα ανάκλησης, σύμφωνα με τις καταγεγραμμένες διαδικασίες που περιγράφονται στη Δήλωση Πρακτικής της εκδότριας ΑΠ. Οι διαδικασίες αυτές επιβεβαιώνουν ότι το πρόσωπο που αιτείται την ανάκληση του Πιστοποιητικού είναι εξουσιοδοτημένο προς το σκοπό αυτό, σύμφωνα με την ενότητα §4.9.2 ανωτέρω. Το αίτημα αυτό διαβιβάζεται στην υπεύθυνη ΑΕ που έχει ελέγξει την Ηλεκτρονική Εγγραφή ή Αίτηση του Τελικού Χρήστη για Πιστοποιητικά και η οποία είναι αρμόδια να το ανακαλέσει άμεσα.

Οι εκδότριες ΑΠ παρέχουν σε κάθε περίπτωση και τη δυνατότητα τηλεφωνικού αιτήματος ανάκλησης Πιστοποιητικών από τους Τελικούς Χρήστες. Ο σχετικός αριθμός τηλεφώνου ανάκλησης, περιλαμβάνεται στην εκάστοτε Δήλωση Πρακτικής της εκδότριας ΑΠ, στους εφαρμοστέους ΟΧΠ καθώς και στον δικτυακό τόπο της εκδότριας ΑΠ.

4.9.4 Χρονικό Διάστημα Μέσα στο Οποίο η ΑΠ θα Πρέπει να Επεξεργαστεί το Αίτημα Ανάκλησης

Οι αρμόδιες ΑΠ πραγματοποιούν όλες τις εύλογες ενέργειες για την έγκαιρη επεξεργασία των αιτημάτων ανάκλησης.

Συγκεκριμένα οι αιτήσεις ανάκλησης Αναγνωρισμένων Πιστοποιητικών, τυγχάνουν άμεσης επεξεργασίας από τις ΑΕ.

Αμέσως μετά την ανάκληση του Πιστοποιητικού, η εκδότρια ΑΠ ενημερώνει τον Τελικό Χρήστη για το γεγονός αυτό, μέσω μηνύματος ηλεκτρονικού ταχυδρομείου ή τηλεφωνικά. Η εκδότρια ΑΠ τηρεί σχετικά αρχεία που αποδεικνύουν ότι έχει πραγματοποιηθεί η σχετική ενημέρωση.

4.9.5 Απαιτήσεις Ελέγχου Ανάκλησης για Τρίτους Συμμετέχοντες

Οι Τρίτοι Συμμετέχοντες θα πρέπει να ελέγχουν την κατάσταση των Πιστοποιητικών στα οποία επιθυμούν να βασιστούν, χρησιμοποιώντας κάποιον από τους μηχανισμούς ελέγχου κατάστασης πιστοποιητικών που παρέχονται από την εκδότρια ΑΠ.

Για την περίπτωση του Καταλόγου Ανακληθέντων Πιστοποιητικών, ο Τρίτος Συμμετέχων θα πρέπει να ελέγξει την κατάσταση Πιστοποιητικού στο οποίο επιθυμεί να βασιστεί ανατρέχοντας στον πιο πρόσφατο Κατάλογο Ανακληθέντων Πιστοποιητικών (ΚΑΠ) που δημοσιεύτηκε από την ΑΠΕΔ ή την εκδότρια ΑΠ που εξέδωσε το Πιστοποιητικό.

Για την ΑΠΕΔ, οι ΚΑΠ παρατίθενται στο χώρο αποθήκευσης της στη διεύθυνση: http://www.yap.gov.gr, καθώς και στις διευθύνσεις: http://www.ermis.gov.gr και http:// www.syzefxis.gov.gr. Επιπλέον ένας "Πίνακας αναφοράς ΚΑΠ" ανακοινώνεται στο Χώρο Αποθήκευσης στη διεύθυνση: http://www.yap.gov.gr, ώστε να επιτρέπει στους Τρίτους Συμμετέχοντες να προσδιορίσουν για κάθε ΥπΑΠ την ακριβή τοποθεσία αποθήκευσης του ΚΑΠ.

Οι εκδότριες ΑΠ προσδιορίζουν στη Δήλωση Πρακτικής τους, το χώρο δημοσίευσης των ΚΑΠ που εκδίδουν.

4.9.6 Συχνότητα Έκδοσης Καταλόγου Ανακληθέντων Πιστοποιητικών (ΚΑΠ)

Η ΑΠΕΔ και οι ΑΠ παρέχουν αδιάλειπτες υπηρεσίες ανάκλησης Πιστοποιητικών.

Η ΑΠΕΔ δημοσιεύει ΚΑΠ όπου εμπεριέχονται τα Πιστοποιητικά που έχουν ανακληθεί από την ίδια και προσφέρει παράλληλα υπηρεσίες ελέγχου κατάστασης Πιστοποιητικών. Οι ΚΑΠ για πιστοποιητικά που εκδίδει η ΑΠΕΔ δημοσιεύονται κάθε τρίμηνο, καθώς επίσης και κάθε φορά που ανακαλείται κάποιο Πιστοποιητικό. Οι ΚΑΠ για Πιστοποιητικά που εκδίδουν οι εκδότριες ΑΠ δημοσιεύονται καθημερινά. Τα Πιστοποιητικά δύνανται να αφαιρούνται από τους ΚΑΠ μετά από τη λήξη τους.

4.9.7 Μέγιστος Χρόνος Αναμονής για ΚΑΠ

Η δημοσίευση των ΚΑΠ στον χώρο πληροφοριών, γίνεται εντός εύλογου χρονικού διαστήματος μερικών λεπτών μετά τη δημιουργία τους, μέσω αυτοματοποιημένης διαδικασίας.

4.9.8 Διαθεσιμότητα Δικτυακού Ελέγχου Ανάκλησης/Κατάστασης Πιστοποιητικών

Οι πληροφορίες για την κατάσταση Πιστοποιητικών από τις εκδότριες ΑΠ δύνανται να είναι επίσης διαθέσιμες και μέσω της χρήσης του Πρωτοκόλλου Δικτυακού Ελέγχου Κατάστασης Πιστοποιητικών σε πραγματικό χρόνο (Online Certificate Status Protocol - OCSP).

Όταν οι εκδότριες ΑΠ χρησιμοποιούν το Πρωτόκολλο Δικτυακού Ελέγχου Κατάστασης Πιστοποιητικών σε πραγματικό χρόνο, τότε δημοσιεύουν στη Δήλωση Πρακτικής τους τις διευθύνσεις για τους OCSP Responders, καθώς και το προφίλ του Πιστοποιητικού OCSP σύμφωνα και με τις απαιτήσεις της ενότητας §7.3 της ΠΠ.

4.9.9 Απαιτήσεις Δικτυακού Ελέγχου Ανάκλησης
Κάθε Τρίτος Συμμετέχων δύναται να ελέγξει την κατάσταση ενός Πιστοποιητικού στο οποίο επιθυμεί να βασιστεί χρησιμοποιώντας τη μέθοδο που προσδιορίζεται στην §4.9.8.

4.9.10 Άλλες Διαθέσιμες Μορφές Αναγγελίας Ανάκλησης
Πλέον της δημοσίευσης ΚΑΠ, η ΑΠΕΔ και οι εκδότριες ΑΠ παρέχουν πληροφορίες για την κατάσταση πιστοποιητικών μέσω μηχανισμών αναζήτησης στο Χώρο Αποθήκευσης της.
Οι πληροφορίες για την κατάσταση Πιστοποιητικών ΥπΑΠ είναι διαθέσιμες από το Χώρο Αποθήκευσης της ΑΠΕΔ στη διεύθυνση: http://www.yap.gov.gr.
Οι πληροφορίες για την κατάσταση Πιστοποιητικών Τελικών Χρηστών είναι διαθέσιμες με τη χρήση διαδικτυακών μηχανισμών αναζήτησης που είναι προσβάσιμες από το Χώρο Αποθήκευσης της κάθε εκδότριας ΑΠ.

4.9.11 Ειδικές Απαιτήσεις Σχετικά με την Έκθεση σε Κίνδυνο του Κλειδιού
Πλέον των διαδικασιών που περιγράφονται στις §4.9.6-4.9.10 της ΠΠ, η ΑΠΕΔ καταβάλλει κάθε εύλογη προσπάθεια ώστε να ενημερώνει τους δυνητικούς Τρίτους Συμμετέχοντες με σχετική ανακοίνωση στις ηλεκτρονικές διευθύνσεις http://www.yap.gov.gr, http://www.syzefxis. gov.gr και http://www.ermis.gov.gr ή σε άλλα δημόσια προσβάσιμα μέσα, στην περίπτωση που ανακαλύψει ή έχει λόγο να πιστεύει, ότι έχει υπάρξει Έκθεση σε Κίνδυνο του ιδιωτικού κλειδιού μιας ΥπΑΠ.

4.9.12 Συνθήκες για Αναστολή Πιστοποιητικού
Η ΑΠΕΔ δεν παρέχει υπηρεσίες αναστολής για πιστοποιητικά ΥπΑΠ. Οι εκδότριες ΑΠ, δύνανται να παρέχουν υπηρεσίες αναστολής για Πιστοποιητικά Τελικού Χρήστη.
Ένα Πιστοποιητικό Τελικού Χρήστη αναστέλλεται εφόσον ο Τελικός Χρήστης έχει λόγο να πιστεύει ότι η ΑΔΔΥ δεν βρίσκεται πλέον στην κατοχή του, αλλά δεν είναι σε θέση να επιβεβαιώσει την οριστική απώλεια της ΑΔΔΥ.
Για αιτήματα από τελικούς χρήστες που δε μπορούν πλέον να χρησιμοποιούν (ή δεν επιθυμούν πλέον να χρησιμοποιούν) ένα Πιστοποιητικό για λόγο διαφορετικό από τον παραπάνω, ο τελικός χρήστης θα πρέπει να ανακαλέσει το Πιστοποιητικό του σύμφωνα με τα αναφερόμενα στις ενότητες §4.9.1 - §4.9.4 ανωτέρω.
Οι εκδότριες ΑΠ που παρέχουν υπηρεσίες αναστολής, δύνανται να ορίσουν στη Δήλωση Πρακτικής τους, επιπλέον λόγους αναστολής Πιστοποιητικού.

4.9.13 Ποιος Μπορεί να Ζητήσει Αναστολή Πιστοποιητικού
Οι εκδότριες ΑΠ που παρέχουν υπηρεσίες αναστολής Πιστοποιητικών Τελικών Χρηστών, έχουν δικαίωμα να ζητήσουν την αναστολή Πιστοποιητικού του Τελικού Χρήστη. Ο Τελικός Χρήστης ή νομίμως εξουσιοδοτημένος εκπρόσωπος τους, ή ο Εκπρόσωπος του Φορέα στην περίπτωση της ΠΠ 7, έχει δικαίωμα να ζητήσει αναστολή των δικών του Πιστοποιητικών.

4.9.14 Διαδικασία Υποβολής Αιτήματος Αναστολής
Οι εκδότριες ΑΠ που παρέχουν υπηρεσίες αναστολής Πιστοποιητικών Τελικών Χρηστών περιγράφουν στη Δήλωση Πρακτικής τους τις διαδικασίες αναστολής. Οι διαδικασίες αυτές, επιβεβαιώνουν ότι το πρόσωπο που αιτείται αναστολή του πιστοποιητικού του, είναι πράγματι το Υποκείμενο του προς αναστολή Πιστοποιητικού ή εξουσιοδοτημένο προς το σκοπό αυτό πρόσωπο.

4.9.15 Περιορισμοί για το Χρονικό Διάστημα Αναστολής
Ένα Πιστοποιητικό Τελικού Χρήστη μπορεί να παραμείνει σε κατάσταση αναστολής, έως ότου αρθούν οι λόγοι αναστολής του και ο Τελικός Χρήστης αιτηθεί τη λήξη της κατάστασης αναστολής. Οι εκδότριες ΑΠ που παρέχουν υπηρεσίες αναστολής Πιστοποιητικών Τελικών Χρηστών περιγράφουν στη Δήλωση Πρακτικής τους τις διαδικασίες άρσης αναστολής. Η Αρχή Εγγραφής των Εκδοτριών ΑΠ θα επαληθεύσει τα στοιχεία της ταυτότητας του Τελικού Χρήστη και θα προβεί σε άρση της κατάστασης αναστολής του Πιστοποιητικού.
Επιπρόσθετα, ένα ανασταλθέν Πιστοποιητικό μπορεί να ανακληθεί ύστερα από αίτημα του τελικού χρήστη, σύμφωνα με τη διαδικασία που περιγράφεται στην ενότητα §4.9.3 ανωτέρω.

Οι εκδότριες ΑΠ δύνανται να ανακαλέσουν ένα Πιστοποιητικό που παραμένει σε κατάσταση αναστολής πέραν του ενός (1) μηνός, ύστερα από ενημέρωση του Τελικού Χρήστη.

4.10 Υπηρεσίες Κατάστασης Πιστοποιητικού

4.10.1 Λειτουργικά Χαρακτηριστικά

Η Κατάσταση των Πιστοποιητικών διατίθεται μέσω των ΚΑΠ που βρίσκονται στους δικτυακούς τόπους των εκδοτριών ΑΠ σε δικτυακό κόμβο - URL που προσδιορίζεται στη Δήλωση Πρακτικής της κάθε εκδότριας ΑΠ, του καταλόγου LDAP και των OCSP responders (όπου διατίθενται).

4.10.2 Διαθεσιμότητα Υπηρεσίας

Οι Υπηρεσίες Κατάστασης Πιστοποιητικών είναι διαθέσιμες ανά πάσα στιγμή, χωρίς περιορισμούς πρόσβασης και προγραμματισμένες διακοπές.

4.11 Τερματισμός Εγγραφής

Οι Τελικοί Χρήστες ή ο Εκπρόσωπος του Φορέα στην περίπτωση της ΠΠ 7, μπορούν να διακόψουν τη χρήση των Πιστοποιητικών που κατέχουν είτε αφήνοντας το Πιστοποιητικό τους να λήξει χωρίς να προχωρήσουν σε επαναδημιουργία κλειδιών για το συγκεκριμένο Πιστοποιητικό, είτε ανακαλώντας το Πιστοποιητικό τους πριν από τη λήξη του χωρίς να το αντικαταστήσουν.

4.12 Παρακαταθήκη Κλειδιού και Ανάκτηση

Κανένας συμμετέχοντας στην ΥΔΚ της ΑΠΕΔ δεν μπορεί να παρακαταθέτει τα ιδιωτικά κλειδιά ΑΠ ή ΑΕ.
Η δυνατότητα της παρακαταθήκης κλειδιού (key escrow) και ανάκτησης (key recovery) αυτού υφίσταται μόνο στις περιπτώσεις ιδιωτικών κλειδιών
Πιστοποιητικών Τελικών Χρηστών, που έχουν εκδοθεί σύμφωνα με την ΠΠ 2 ή την ΠΠ 6 από εκδότρια ΑΠ που παρέχει υπηρεσίες αρχειοθέτησης του ιδιωτικού κλειδιού του Τελικού Χρήστη. Στην περίπτωση αυτή η εκδότρια ΑΠ μπορεί να διατηρεί προς φύλαξη τα αντίγραφα των ιδιωτικών κλειδιών των Τελικών Χρηστών για τους οποίους εγκρίνει Αίτηση για Πιστοποιητικό. Η φύλαξη αυτή, γίνεται σύμφωνα με αυστηρά μέτρα ελέγχου και τις διαδικασίες που περιγράφονται στην Δήλωση Πρακτικής της εκδότριας ΑΠ.

4.12.1 Πολιτική και Πρακτικές Παρακαταθήκης Κλειδιού και Ανάκτησης

Οι εκδότριες ΑΠ, οι οποίες εκδίδουν Πιστοποιητικά σύμφωνα με την ΠΠ 2 ή την ΠΠ 6, και παρέχουν υπηρεσίες αρχειοθέτησης ιδιωτικού κλειδιού, επιτρέπεται να διατηρούν προς φύλαξη τα ιδιωτικά κλειδιά Τελικών Χρηστών. Τα προς φύλαξη ιδιωτικά κλειδιά θα αποθηκεύονται σε κρυπτογραφημένη μορφή χρησιμοποιώντας κατάλληλο λογισμικό ή/και εξοπλισμό.
Οι εκδότριες ΑΠ που παρέχουν την υπηρεσία αυτή, πρέπει να:

- Ενημερώνουν τους Τελικούς Χρήστες σχετικά με την παρακαταθήκη των ιδιωτικών κλειδιών τους, μέσω των ΟΧΠ και της Δήλωσης Πρακτικής τους.
- Προστατεύουν τα παρακατατεθειμένα κλειδιά Τελικών Χρηστών από μη εξουσιοδοτημένη αποκάλυψη.
- Προστατεύουν κάθε πληροφορία, συμπεριλαμβανομένου του κλειδιού ή των κλειδιών του διαχειριστή, η οποία θα μπορούσε να χρησιμοποιηθεί για την ανάκτηση των παρακατατεθειμένων κλειδιών Τελικού Χρήστη.
- Παρέχουν τα παρακατατεθειμένα κλειδιά Τελικών Χρηστών αποκλειστικά κατόπιν πιστοποιημένων και εγκεκριμένων αιτημάτων ανάκτησης.
- Ανακαλούν το ζεύγος Κλειδιών του Τελικού Χρήστη πριν την ανάκτηση του κλειδιού κρυπτογράφησης, όταν αυτό κρίνεται απαραίτητο.
- Μην αποκαλύπτουν ή μην επιτρέπουν την αποκάλυψη των παρακατατεθειμένων κλειδιών ή πληροφοριών σχετικά με τα παρακατατεθειμένα κλειδιά σε τρίτα μέρη, εκτός εάν αυτό απαιτείται από τη νομοθεσία ή κατόπιν σχετικού εντάλματος των αρμόδιων δικαστικών αρχών.
  Η ανάκτηση των ιδιωτικών κλειδιών Τελικού Χρήστη θα είναι εφικτή μόνο υπό αυστηρές και συγκεκριμένες συνθήκες, οι οποίες κατ` ελάχιστο θα πρέπει να:
- Διασφαλίζουν ότι οι εκδότριες ΑΠ επαληθεύουν την ταυτότητα οποιουδήποτε παρουσιάζεται ως Τελικός Χρήστης, προκειμένου να διασφαλιστεί ότι το αίτημα του φερόμενου ως Τελικού Χρήστη σχετικά με το ιδιωτικό κλειδί του προέρχεται πράγματι από τον ίδιο και όχι από κάποιον κακόβουλο τρίτο.
- Διασφαλίζουν ότι οι εκδότριες ΑΠ θα προβαίνουν σε ανάκτηση του ιδιωτικού κλειδιού του Τελικού Χρήστη χωρίς την έγκριση του, μόνον για τους δικούς τους θεμιτούς και σύννομους σκοπούς, όπως είναι η συμμόρφωση προς διοικητικές διαδικασίες που να δικαιολογούν την ανάγκη πρόσβασης σε υπηρεσιακά

δεδομένα ή δικαστικές διαδικασίες/αποφάσεις ή εντάλματα έρευνας και όχι για παράνομους, δόλιους ή άλλους σκοπούς. Οι εκδότριες ΑΠ θα λαμβάνουν όλα τα απαραίτητα μέτρα ελέγχου για το προσωπικό τους, προκειμένου να αποτραπεί η αυθαίρετη πρόσβαση των διαχειριστών ή τρίτων σε ιδιωτικά κλειδιά.

- Διασφαλίζουν ότι αν ο αιτών δεν είναι ο Τελικός Χρήστης στον οποίο έχει εκδοθεί πιστοποιητικό σύμφωνα με την ΠΠ 6, ο αιτών αποτελεί νόμιμο εκπρόσωπο του νομικού προσώπου.
- Διασφαλίζουν ότι αν ο αιτών δεν είναι ο Τελικός Χρήστης στον οποίο έχει εκδοθεί πιστοποιητικό σύμφωνα με την ΠΠ 2 στο πλαίσιο της άσκησης των καθηκόντων του για την εξυπηρέτηση των αναγκών φορέα του δημοσίου, ο αιτών εξουσιοδοτείται από τον φορέα να υποβάλλει το σχετικό αίτημα.

Οι εκδότριες ΑΠ που εκδίδουν Πιστοποιητικά σύμφωνα με την ΠΠ 2 ή την ΠΠ 6 και παρέχουν υπηρεσίες αρχειοθέτησης ιδιωτικού κλειδιού περιγράφουν στη Δήλωση Πρακτικής τους τις τεχνικές πρακτικές παρακαταθήκης ιδιωτικού κλειδιού που ακολουθούν.

Η παρακαταθήκη διενεργείται με τη χρήση ειδικού λογισμικού ή/και εξοπλισμού, και κρυπτογραφικών μεθόδων, οι οποίες απαιτούν τη χρήση κλειδιού ισχυρής κρυπτογράφησης σε συνδυασμό με άλλα ισχυρά μέτρα ελέγχου, και εξασφαλίζουν ότι η ανάκτηση των ιδιωτικών κλειδιών είναι δυνατή μόνο από εγκεκριμένο διαχειριστή της εκδότριας ΑΠ.

Η ΑΠΕΔ αξιολογεί και προεγκρίνει την ασφάλεια της ακολουθούμενης μεθόδου παροχής της συγκεκριμένης υπηρεσίας από τις εκδότριες ΑΠ.

4.12.2 Πολιτική και Πρακτικές Ενθυλάκωσης Κλειδιού Συνεδρίας

Η ΑΠΕΔ και οι εκδότριες ΑΠ δε παρέχουν υπηρεσίες ενθυλάκωσης κλειδιού συνεδρίας (session key encapsulation).

5. Φυσικά, Διαδικαστικά Μέτρα Προστασίας και Ασφάλειας Προσωπικού

Η ΑΠΕΔ εφαρμόζει υψηλές προδιαγραφές ασφαλείας οι οποίες ανταποκρίνονται στην παρούσα ΠΠ.

5.1 Φυσικά Μέτρα Προστασίας

5.1.1 Χώρος Εγκατάστασης και Κατασκευή

Οι υπηρεσίες πιστοποίησης της ΑΠΕΔ διενεργούνται εντός φυσικά προστατευμένου περιβάλλοντος το οποίο έχει σχεδιαστεί έτσι ώστε να αποτρέπεται, να προλαμβάνεται και να εντοπίζεται κάθε εμφανής ή μη προσπάθεια πρόσβασης, ικανοποιώντας τους διεθνώς αναγνωρισμένους, βάσει προτύπων, όρους και προϋποθέσεις ασφαλείας. Οι υπηρεσίες πιστοποίησης των εκδοτριών ΑΠ διενεργούνται εντός φυσικά προστατευμένου περιβάλλοντος το οποίο πληρεί προδιαγραφές ανάλογου επιπέδου ασφαλείας με τις παραπάνω.

5.1.2 Φυσική Πρόσβαση

Για να επιτευχθεί πρόσβαση σε κάποιο ανώτερο επίπεδο πρόσβασης απαιτείται να επιτραπεί η είσοδος καταρχήν σε κάποιο κατώτερο επίπεδο πρόσβασης. Ειδικότερα, υπάρχουν επίπεδα πρόσβασης που περιλαμβάνουν:

- Κοινόχρηστους χώρους
- Επίπεδο στο οποίο λαμβάνει χώρα η ευαίσθητη λειτουργική δραστηριότητα των ΑΠ.
- Χώρο αποθήκευσης των Ασφαλών Κρυπτογραφικών Μονάδων (ΑΚΜ).

5.1.3 Παροχή Ηλεκτρικού Ρεύματος και Κλιματισμός

Οι ασφαλείς εγκαταστάσεις των υποδομών μέσω των οποίων παρέχονται οι υπηρεσίες πιστοποίησης βάσει των διατάξεων του παρόντος και τις συναφθείσες συμβάσεις, είναι εξοπλισμένες με κύρια και εφεδρικά:

- Συστήματα παροχής ηλεκτρικού ρεύματος για την εξασφάλιση συνεχούς και αδιάλειπτης παροχής.
- Συστήματα θέρμανσης / εξαερισμού / κλιματισμού για τον έλεγχο της θερμοκρασίας και της σχετικής υγρασίας.

5.1.4 Πλημμύρες

Λαμβάνονται οι απαιτούμενες προφυλάξεις για να ελαχιστοποιηθούν οι κίνδυνοι από πλημμύρες.

5.1.5 Πρόληψη και Προστασία από Φωτιά

Λαμβάνονται όλες οι απαραίτητες προφυλάξεις για την πρόληψη και κατάσβεση πυρκαγιάς ή άλλης επιζήμιας έκθεσης σε φωτιά ή καπνό. Τα μέτρα αυτά έχουν σχεδιαστεί ώστε να πληρούν τους εθνικούς κανονισμούς ασφάλειας από φωτιά.

5.1.6 Αποθήκευση Μέσων

Όλα τα μέσα τα οποία περιέχουν το λογισμικό και τα δεδομένα παραγωγής, καθώς και τα στοιχεία ελέγχων, αρχείου ή εφεδρικών αντιγράφων αποθηκεύονται σε ασφαλείς εγκαταστάσεις αποθήκευσης οι οποίες διαθέτουν τα απαραίτητα φυσικά και λογικά μέτρα ελέγχου πρόσβασης. Τα μέτρα αυτά σχεδιάζονται ώστε να περιορίζουν την πρόσβαση αποκλειστικά σε εξουσιοδοτημένο προσωπικό και να προστατεύουν τα μέσα αποθήκευσης έναντι οιασδήποτε καταστροφής (π.χ., από νερό, φωτιά ή/και ηλεκτρομαγνητική).

5.1.7 Καταστροφή Μη - Χρήσιμων Υλικών

Τα διαβαθμισμένα έγγραφα και υλικά καταστρέφονται σε καταστροφέα εγγράφων και τα μέσα που χρησιμοποιήθηκαν για τη συλλογή ή μεταβίβαση διαβαθμισμένων πληροφοριών καθίστανται μη - αναγνώσιμα. Οι συσκευές κρυπτογράφησης καταστρέφονται με φυσικό τρόπο ή διαγράφονται τα δεδομένα τους σύμφωνα με τις οδηγίες του κατασκευαστή.
Τα υπόλοιπα μη - χρήσιμα υλικά καταστρέφονται.

5.1.8 Δημιουργία Εφεδρικών Αντιγράφων Ασφαλείας Εκτός του Κύριου Χώρου

Ανά τακτά διαστήματα δημιουργούνται εφεδρικά αντίγραφα για τα δεδομένα των κυριότερων συστημάτων, των δεδομένων καταχώρισης ελέγχου, καθώς και άλλων διαβαθμισμένων πληροφοριών.

5.2 Διαδικαστικά Μέτρα Ελέγχου

5.2.1 Έμπιστοι Ρόλοι

Ως Έμπιστα Πρόσωπα θεωρούνται όλοι οι υπάλληλοι, εργολήπτες και σύμβουλοι οι οποίοι έχουν πρόσβαση ή ελέγχουν λειτουργίες ταυτοποίησης ή κρυπτογράφησης και οι οποίοι θα μπορούσαν να επηρεάσουν σημαντικά:

- Την εγκυρότητα των στοιχείων Εγγραφής και αίτησης για Πιστοποιητικά.
- Την αποδοχή, απόρριψη ή άλλη επεξεργασία των ηλεκτρονικών αιτήσεων για Πιστοποιητικά, των αιτημάτων για ανάκληση ή των αιτημάτων για ανανέωση ή των στοιχείων εγγραφής.
- Την έκδοση ή ανάκληση Πιστοποιητικών, περιλαμβανομένου του προσωπικού που έχει πρόσβαση στις περιοχές περιορισμένης πρόσβασης στο χώρο αποθήκευσης.
- Τον χειρισμό των στοιχείων ή των αιτημάτων των Τελικών χρηστών.

5.2.2 Αριθμός Προσώπων που Απαιτούνται για Κάθε Εργασία

Οι εκδότριες ΑΠ και οι ΑΕ υιοθετούν και εφαρμόζουν αυστηρά μέτρα ελέγχου, ώστε να εξασφαλίσουν τον διαχωρισμό των αρμοδιοτήτων για κάθε τομέα ευθύνης και να διασφαλίζουν ότι για την εκτέλεση εργασιών υψηλής διαβάθμισης απαιτούνται περισσότερα από ένα Έμπιστα Πρόσωπα.
Οι υψηλής διαβάθμισης εργασίες, όπως είναι η πρόσβαση και ο χειρισμός του κρυπτογραφικού υλικού των ΑΠ, απαιτούν πολλαπλά Έμπιστα πρόσωπα, ώστε να υπάρχει διαμοιρασμένος έλεγχος τόσο της φυσικής όσο και της λογικής πρόσβασης στο υλικό.
Τα πρόσωπα που έχουν φυσική πρόσβαση στον κρυπτογραφικό εξοπλισμό δεν τηρούν "Απόρρητα Μερίδια" (§6.2.2), και αντιστρόφως.

5.2.3 Ταυτοποίηση και Αυθεντικοποίηση Κάθε Ρόλου

Οι ΑΠ και οι ΑΕ επαληθεύουν τα στοιχεία ταυτότητας και την εξουσιοδότηση του προσωπικού που επιθυμεί να θεωρηθεί ως Έμπιστο, πριν το προσωπικό αυτό:

- λάβει συσκευές πρόσβασης και του χορηγηθούν άδειες πρόσβασης στις απαιτούμενες εγκαταστάσεις,
- λάβει ψηφιακά πιστοποιητικά για την πρόσβαση και τέλεση συγκεκριμένων αρμοδιοτήτων Πληροφοριακών συστημάτων και συστημάτων ΑΠ ή ΑΕ.

5.2.4 Ρόλοι που Απαιτούν Διαχωρισμό Καθηκόντων

Οι ρόλοι που απαιτούν Διαχωρισμό καθηκόντων περιλαμβάνουν, ενδεικτικά:

- Την επαλήθευση των στοιχείων στις Αιτήσεις για Πιστοποιητικό.
- Την αποδοχή, απόρριψη ή άλλη επεξεργασία των Αιτήσεων για Πιστοποιητικό, των αιτημάτων για ανάκληση ή των αιτημάτων για ανανέωση ή των στοιχείων εγγραφής.
- Την έκδοση ή ανάκληση Πιστοποιητικών Διαχειριστών και του προσωπικού που έχει πρόσβαση στις εγκαταστάσεις περιορισμένης πρόσβασης.
- Τη δημιουργία, έκδοση, "φόρτωση" ή καταστροφή ενός πιστοποιητικού ΑΠ.

5.3 Μέτρα Ελέγχου Προσωπικού

5.3.1 Απαιτήσεις Προσόντων, Εμπειρίας και Εξουσιοδότησης

Οι εκδότριες ΑΠ καταγράφουν λεπτομερώς τις πολιτικές ελέγχου προσωπικού και ασφαλείας που ακολουθούν, η συμμόρφωση προς τις οποίες αποτελεί μέρος του ανεξάρτητου ελέγχου που περιγράφονται στην ενότητα §8 της Πολιτικής Πιστοποιητικών.

5.3.2 Διαδικασίες Ελέγχου Παρελθόντος

Οι εκδότριες ΑΠ και οι ΑΕ διενεργούν ελέγχους σχετικά με το παρελθόν του προσωπικού που πρόκειται να θεωρηθεί ως Έμπιστο. Για το προσωπικό που κατέχει Έμπιστες θέσεις, οι έλεγχοι του παρελθόντος θα επαναλαμβάνονται τουλάχιστον κάθε πέντε (5) έτη. Οι διαδικασίες αυτές θα υπόκεινται στους όποιους περιορισμούς επιβάλλονται από την κείμενη νομοθεσία και το δημοσιοϋπαλληλικό κώδικα ως προς τους ελέγχους του παρελθόντος.

5.3.3 Απαιτήσεις Εκπαίδευσης

Η ΑΠΕΔ και οι εκδότριες ΑΠ διασφαλίζουν στο προσωπικό τους την απαραίτητη εκπαίδευση για την εκτέλεση των καθηκόντων τους με επαρκή και ικανοποιητικό τρόπο.

5.3.4 Συχνότητα και Απαιτήσεις Επανεκπαίδευσης

Η ΑΠΕΔ και οι εκδότριες ΑΠ διασφαλίζουν τη συνεχή εκπαίδευση και ενημέρωση για τις σύγχρονες εξελίξεις στο προσωπικό τους στο βαθμό και τη συχνότητα που είναι απαραίτητα ώστε να εξασφαλιστεί η διατήρηση του απαιτούμενου επιπέδου επάρκειας γνώσεων. Επίσης σε συνεχή βάση παρέχεται ενημέρωση αναφορικά με θέματα ασφαλείας.

5.3.5 Κυρώσεις για Μη Εξουσιοδοτημένη Χρήση

Οι εκδότριες ΑΠ και οι ΑΕ υιοθετούν και εφαρμόζουν το δημοσιοϋπαλληλικό κώδικα για την επιβολή κυρώσεων στο προσωπικό που ακολουθεί μη αποδεκτές ενέργειες.

5.3.6 Απαιτήσεις Ανεξάρτητου Αναδόχου

Οι εκδότριες ΑΠ και οι ΑΕ δύνανται να επιτρέψουν σε ανεξάρτητους εργολήπτες ή συμβούλους να λειτουργήσουν ως Έμπιστα Πρόσωπα μόνο στο βαθμό που κάτι τέτοιο είναι απαραίτητο για την εξυπηρέτηση ξεκάθαρα προσδιορισμένων σχέσεων παραχώρησης αρμοδιοτήτων και μόνο υπό αυστηρές προϋποθέσεις.

5.3.7`Εντυπα που Διατίθενται στο Προσωπικό

Το προσωπικό που αναλαμβάνει την εφαρμογή των υπηρεσιών πιστοποίησης της ΥΔΚ βάσει των διατάξεων του παρόντος, είναι σκόπιμο να λάβει πλήρη γνώση αυτής της Πολιτικής και της εκάστοτε εφαρμοστέας Δήλωσης Πρακτικής, για την άρτια εκτέλεση των καθηκόντων του.

5.4 Διαδικασίες Ελέγχου Ασφάλειας

5.4.1 Μορφές Συμβάντων που Καταγράφονται

Η ΑΠΕΔ διασφαλίζει, όπου απαιτείται, την καταγραφή των σημαντικών περιστατικών διαχείρισης του κύκλου ζωής των κλειδιών και Πιστοποιητικών της ΑΠΕΔ και των ΥπΑΠ, συμπεριλαμβανομένων:

- Της παραγωγής, δημιουργίας εφεδρικών αντιγράφων, αποθήκευσης, ανάκτησης, αρχειοθέτησης και καταστροφής κλειδιών και
- Περιστατικών διαχείρισης του κύκλου ζωής των συσκευών κρυπτογράφησης.

Οι εκδότριες ΑΠ διασφαλίζουν, όπου απαιτείται, την καταγραφή των σημαντικών περιστατικών διαχείρισης του κύκλου ζωής Πιστοποιητικών Τελικών Χρηστών, συμπεριλαμβανομένων:

- Στοιχείων Εγγραφής,
- Επιτυχούς ή μη επεξεργασίας των Ηλεκτρονικών Εγγραφών ή Αιτήσεων για Πιστοποιητικά, ανανέωση, επαναδημιουργία κλειδιού, ανάκληση και ανάκτηση, και
- Παραγωγής και έκδοσης Πιστοποιητικών και ΚΑΠ.

Η ΑΠΕΔ και οι εκδότριες ΑΠ διασφαλίζουν, όπου απαιτείται, την καταγραφή των παρακάτω περιστατικών που τις αφορούν σχετικά με την ασφάλεια, συμπεριλαμβανομένων:

- Επιτυχών ή μη προσπαθειών πρόσβασης στο σύστημα ΥΔΚ.
- Ενεργειών ΥΔΚ και συστήματος ασφάλειας.
- Πρόσβασης αρχείων ή μητρώων υψηλής ασφάλειας που είναι διαθέσιμα προς ανάγνωση, εγγραφή ή διαγραφή.
- Μεταβολών στο επίπεδο ασφάλειας.
- Εμπλοκών του συστήματος, βλαβών του εξοπλισμού ή άλλων ανωμαλιών.
- Δραστηριότητας του συστήματος προστασίας (firewall) και δρομολογητή (router).

Οι καταχωρίσεις αυτές περιλαμβάνουν τα ακόλουθα στοιχεία:

- Ημερομηνία και ώρα της καταχώρισης.
- Σειριακό ή αύξοντα αριθμό καταχώρισης, για αυτόματες καταχωρίσεις.
- Στοιχεία ταυτότητας του προσώπου που κάνει την καταχώριση.
- Είδος καταχώρισης.

Οι Αρχές Εγγραφής ή/και τα Εντεταλμένα Γραφεία καταγράφουν τα στοιχεία εγγραφής συμπεριλαμβάνοντας:

- Το είδος των αποδεικτικών εγγράφων για την ταυτοποίηση του Τελικού Χρήστη.
- Καταγραφή μοναδικών δεδομένων ταυτότητας, αριθμών ή συνδυασμού αυτών των αποδεικτικών στοιχείων ταυτότητας (π.χ. του αριθμού ταυτότητας του Αιτούντος Πιστοποιητικό), εφόσον ισχύουν.
- Τοποθεσία αποθήκευσης αντιγράφων των αποδεικτικών εγγράφων ταυτότητας.
- Στοιχεία ταυτότητας του προσώπου που διενεργεί την ταυτοποίηση
- Μέθοδο που εφαρμόστηκε για την επιβεβαίωση των εγγράφων ταυτοποίησης, εφόσον υπάρχει.

5.4.2 Συχνότητα Επεξεργασίας των Αρχείων Καταγραφής

Τα αρχεία καταγραφής εξετάζονται σε τακτική βάση για σημαντικά περιστατικά ασφάλειας και λειτουργίας. Επιπροσθέτως, η ΑΠΕΔ και αντίστοιχα οι εκδότριες ΑΠ διασφαλίζουν την ανασκόπηση των αρχείων καταγραφής για ύποπτη ή ασυνήθη δραστηριότητα βάσει των προειδοποιητικών μηνυμάτων που δημιουργούνται όταν υπάρχουν παρατυπίες ή προβλήματα εντός των συστημάτων της παρούσας ΥΔΚ.

5.4.3 Περίοδος Διατήρησης του Ημερολογίου Καταγραφής Ελέγχων

Τα αρχεία καταγραφής τηρούνται επιτόπια τουλάχιστον για δύο (2) μήνες μετά από την επεξεργασία τους, ενώ στη συνέχεια αρχειοθετούνται σύμφωνα με την §5.5.2 της ΠΠ.

5.4.4 Προστασία του Αρχείου Καταγραφής

Τα ηλεκτρονικά και χειρόγραφα αρχεία καταγραφής προστατεύονται από μη - εξουσιοδοτημένη ανάγνωση, τροποποίηση, διαγραφή ή άλλη παραποίηση με τη χρήση φυσικών και λογικών μέτρων ελέγχου πρόσβασης.

5.4.5 Διαδικασίες Εφεδρικών Αντιγράφων των Αρχείων Καταγραφής

Εφεδρικά αντίγραφα προσθήκης (incremental backups) στα αρχεία καταγραφής και πλήρη εφεδρικά αντίγραφα παράγονται σε τακτική βάση (full backups).

5.4.6 Σύστημα Ελέγχου

Αυτοματοποιημένα δεδομένα ελέγχου παράγονται και καταγράφονται σε επίπεδο εφαρμογής, δικτύου και λειτουργικού συστήματος.

5.4.7 Ενημέρωση του Υποκειμένου που Προκάλεσε το Περιστατικό

Στην περίπτωση καταγραφής περιστατικού από το σύστημα ελέγχου, δεν είναι απαραίτητη η ενημέρωση του φυσικού προσώπου, του οργανισμού, της συσκευής ή της εφαρμογής που προκάλεσε το περιστατικό.

5.4.8 Αξιολόγηση Τρωτών Σημείων

Τα περιστατικά που λαμβάνουν χώρα κατά τη διαδικασία ελέγχου καταγράφονται, ώστε να είναι δυνατή η παρακολούθηση των τρωτών σημείων του συστήματος.

Αξιολογήσεις για την τρωτότητα της λογικής ασφάλειας διενεργούνται, ανασκοπούνται και αναθεωρούνται μετά από εξέταση των περιστατικών που έχουν καταγραφεί. Οι αξιολογήσεις βασίζονται σε δεδομένα αυτοματοποιημένης καταγραφής πραγματικού χρόνου και διενεργούνται σε τακτική βάση.

5.5 Καταγραφή Αρχείων

5.5.1 Είδη Περιστατικών που Καταγράφονται

Πλέον των αρχείων ελέγχου καταγραφής για λόγους ασφάλειας που προσδιορίζονται στην §5.4 της ΠΠ, η ΑΠΕΔ διασφαλίζει την τήρηση αρχείων που περιλαμβάνουν τεκμηρίωση των ακόλουθων:

- Της συμμόρφωσης με την ΠΠ.
- Ενεργειών και πληροφοριών που είναι ουσιώδεις για την έκδοση κάθε Πιστοποιητικού καθώς και για τη δημιουργία, έκδοση, ανάκληση, λήξη και επαναδημιουργία κλειδιού ή ανανέωση όλων των Πιστοποιητικών ΥπΑΠ που εκδίδονται.

Τα αρχεία του κύκλου ζωής Πιστοποιητικών που τηρούνται από τις εκδότριες ΑΠ περιλαμβάνουν:

- Τις υποχρεώσεις που απορρέουν από τους ΟΧΠ Τελικού Χρήστη.
- Κάθε μεταβολή που έχει επέλθει στους ΟΧΠ.
- Την ταυτότητα του Τελικού Χρήστη που κατονομάζεται σε κάθε Πιστοποιητικό.
- Την ταυτότητα του προσώπου που αιτείται την ανάκληση ή ανάκτηση Πιστοποιητικού.
- Άλλα πραγματικά στοιχεία που δηλώνονται στο Πιστοποιητικό.
- Ορισμένα ουσιώδη στοιχεία τα οποία σχετίζονται με την έκδοση Πιστοποιητικών, συμπεριλαμβανομένων ενδεικτικά των πληροφοριών σχετικά με την επιτυχή ολοκλήρωση του Ελέγχου Συμμόρφωσης σύμφωνα με την §8 της ΠΠ.

Τα αρχεία που τηρούν οι εκδότριες ΑΠ αναφορικά με την ταυτότητα των τελικών χρηστών περιλαμβάνουν:

- Τα έγγραφα που προσκομίζονται από τους Τελικούς Χρήστες για την ταυτοποίηση.
- Ένα αρχείο μοναδικών στοιχείων ταυτοποίησης (πχ. αριθμός ταυτότητας, διαβατηρίου του Τελικού Χρήστη).
- Αποδεικτικά απόδοσης τομεακών αναγνωριστικών, όπου αυτό απαιτείται,
- Τα στοιχεία ταυτότητας του προσώπου που λαμβάνει και αποδέχεται Ηλεκτρονικές Εγγραφές ή Αιτήσεις για Πιστοποιητικά, και
- Ένα σχέδιο τεκμηρίωσης αναφορικά με τις μεθόδους που χρησιμοποιούνται για την αποδοχή εγγράφων ταυτοποίησης.

Τα αρχεία μπορεί να τηρούνται ηλεκτρονικά ή σε τυπωμένη μορφή, υπό την προϋπόθεση ότι έχουν ταξινομηθεί, αποθηκευθεί, τηρηθεί και αναπαραχθεί με ακρίβεια στο σύνολο τους.

5.5.2 Περίοδος Διατήρησης Αρχείου

Τα αρχεία που συνδέονται με κάποιο Πιστοποιητικό, καθώς και τα ίδια τα Πιστοποιητικά διατηρούνται τουλάχιστον για τα εξής χρονικά διαστήματα, μετά από την ημερομηνία λήξης ή ανάκλησης του Πιστοποιητικού:

- Για όλα τα Πιστοποιητικά που ακολουθούν την ΠΠ 1, ΠΠ 3, ΠΠ 4, ΠΠ 5 και ΠΠ 7, τηρούνται για τριάντα (30) έτη.
- Για τα Πιστοποιητικά που ακολουθούν την ΠΠ 2 ή την ΠΠ 6, τηρούνται για δέκα (10) έτη.

5.5.3 Προστασία του Αρχείου

Η ΑΠΕΔ διασφαλίζει την προστασία των αρχείων που καταγράφονται σύμφωνα με την §5.5.1 της ΠΠ, με τρόπο ώστε μόνο εξουσιοδοτημένα πρόσωπα να επιτρέπεται να έχουν πρόσβαση σε αυτά. Τα ηλεκτρονικά αρχειοθετημένα δεδομένα προστατεύονται έναντι μη - εξουσιοδοτημένης ανάγνωσης, τροποποίησης, διαγραφής ή άλλης παραποίησης με την εφαρμογή κατάλληλων φυσικών και λογικών μέτρων ελέγχου πρόσβασης. Τα μέσα τήρησης των δεδομένων που αρχειοθετούνται, καθώς και οι απαιτούμενες εφαρμογές για την επεξεργασία των δεδομένων αυτών, διατηρούνται με σκοπό να διασφαλιστεί η δυνατότητα προσπέλασης τους, για το χρονικό διάστημα που προσδιορίζεται στην §5.5.2 της ΠΠ.
Ανάλογα μέτρα εφαρμόζουν και οι εκδότριες ΑΠ για την προστασία των αρχείων που τηρούν.

5.5.4 Διαδικασίες Αρχειοθέτησης Εφεδρικών Αντιγράφων

Η ΑΠΕΔ δημιουργεί σε καθημερινή βάση, όπου αυτό απαιτείται, εφεδρικά αντίγραφα (back-up) των στοιχείων που υπάρχουν στα εκδοθέντα Πιστοποιητικά μέσω της αποθήκευσης των επιπρόσθετων πληροφοριών (incremental back up), ενώ παράγει πλήρη εφεδρικά αντίγραφα (full back up) σε εβδομαδιαία βάση.
Οι εκδότριες ΑΠ εφαρμόζουν μέτρα ανάλογου επιπέδου ασφαλείας.

5.5.5 Διαδικασίες για την Πρόσβαση και την Επαλήθευση Πληροφοριών Αρχείου

Βλ. ΠΠ §5.5.3.

5.6 Αντικατάσταση Κλειδιών

Τα ζεύγη κλειδιών που πιστοποιούν τις ΥπΑΠ αποσύρονται με το πέρας του αντίστοιχου ανώτατου χρόνου ζωής τους όπως ορίζεται στην §6.3.2 της ΠΠ.
Πριν από τη λήξη των Πιστοποιητικών που πιστοποιούν τις ΥπΑΠ, και αν η ΥπΑΠ δε προβεί σε ανανέωση του Πιστοποιητικού της σύμφωνα με την §4.6, εφαρμόζονται διαδικασίες αντικατάστασης των κλειδιών. Η διαδικασία αντικατάστασης κλειδιών που πιστοποιούν τις ΥπΑΠ προϋποθέτει ότι:

- Η ΥπΑΠ διακόπτει την έκδοση νέων Πιστοποιητικών όχι αργότερα από 60 ημέρες πριν από την ημερομηνία λήξεως του ζεύγους των κλειδιών της.
- Τα Πιστοποιητικά Τελικών Χρηστών μετά την επαναδημιουργία του ζεύγους κλειδιών που πιστοποιούν τις ΥπΑΠ θα υπογράφονται από το νέο ζεύγος κλειδιών της ΥπΑΠ.
- Η ΥπΑΠ θα συνεχίζει να εκδίδει ΚΑΠ υπογεγραμμένους από το αρχικό ιδιωτικό κλειδί της μέχρι την επέλευση της ημερομηνίας λήξεως του τελευταίου Πιστοποιητικού που εκδόθηκε με τη χρήση αυτού του αρχικού ζεύγους κλειδιών.

5.7 Αποκατάσταση Καταστροφών και Έκθεσης σε Κίνδυνο του Κλειδιού

Η ΑΠΕΔ και οι εκδότριες ΑΠ διασφαλίζουν μέσω των υποδομών τους, την υλοποίηση ενός ισχυρού συνδυασμού φυσικών, λογικών και διαδικαστικών μέτρων ελέγχου ώστε να ελαχιστοποιήσει τον κίνδυνο και τον πιθανό αντίκτυπο της Έκθεσης σε Κίνδυνο ή της καταστροφής κάποιου κλειδιού. Επιπρόσθετα, εφαρμόζονται μέτρα αποκατάστασης καταστροφών όπως περιγράφεται στην §5.7.3 της ΠΠ και μέτρα αντιμετώπισης της Έκθεσης Κλειδιού σε Κίνδυνο όπως περιγράφεται στην §5.7.2 της ΠΠ. Τα μέτρα για την αποκατάσταση Έκθεσης σε Κίνδυνο ή καταστροφής αναπτύσσονται με στόχο την ελαχιστοποίηση του πιθανού αντίκτυπου από τέτοιο συμβάν και την αποκατάσταση της λειτουργίας της ΥΔΚ.

5.7.1 Φθορά Εξοπλισμού, Λογισμικού, Δεδομένων

Σε περίπτωση φθοράς του εξοπλισμού, λογισμικού ή/και δεδομένων εφαρμόζονται τα μέτρα αντιμετώπισης επεισοδίων. Τα μέτρα αυτά απαιτούν ανάλογη κλιμάκωση, διερεύνηση του επεισοδίου και ανταπόκριση στο επεισόδιο. Τα μέτρα για την αποκατάσταση καταστροφής ή έκθεσης σε κίνδυνο του κλειδιού θα τεθούν σε ισχύ εφόσον κριθεί απαραίτητο.

5.7.2`Εκθεση σε Κίνδυνο Ιδιωτικού Κλειδιού

Κατά την υποτιθέμενη ή πραγματική Έκθεση σε Κίνδυνο του ιδιωτικού κλειδιού της ΑΠΕΔ ή των εκδοτριών ΑΠ, εφαρμόζονται ειδικά μέτρα για την Αντιμετώπιση της Έκθεσης Κλειδιού σε Κίνδυνο από στελέχη του φορέα διαχείρισης της Υποδομής Δημοσίου Κλειδιού. Τα στελέχη αυτά, αξιολογούν την κατάσταση, αναπτύσσουν σχέδιο δράσης και εκτελούν το σχέδιο αυτό με την έγκριση της ΑΠΕΔ.

Εφόσον απαιτείται ανάκληση Πιστοποιητικού ΑΠ, λαμβάνονται τα ακόλουθα μέτρα:

- Η κατάσταση ανάκλησης του Πιστοποιητικού κοινοποιείται στους Τελικούς Χρήστες και Τρίτους Συμμετέχοντες μέσω του Χώρου Αποθήκευσης της ΑΠΕΔ και της εκδότριας ΑΠ σύμφωνα με την §4.9.5 της ΠΠ.
- Καταβάλλεται εύλογη προσπάθεια ώστε να υπάρξει πρόσθετη ενημέρωση σχετικά με την ανάκληση προς όλους τους συμμετέχοντες που δύναται να επηρεαστούν.
- Η ΑΠ θα παράγει ένα νέο ζεύγος κλειδιών σύμφωνα με την §5.6 της ΠΠ, εκτός της περίπτωσης όπου διακόπτεται η παροχή των υπηρεσιών πιστοποίησης σύμφωνα με την §5.8 της ΠΠ.

5.7.3 Δυνατότητες Συνέχισης Επιχειρηματικών Λειτουργιών Μετά Από Καταστροφή

Για την εξασφάλιση της συνέχισης των επιχειρηματικών λειτουργιών μετά από καταστροφή δημιουργούνται εφεδρικά αρχεία για τα κρίσιμα στοιχεία της ΑΠΕΔ και των εκδοτριών ΑΠ για την ΥΔΚ, τόσο εξοπλισμού όσο και

λογισμικού. Επιπλέον, λαμβάνονται αντίγραφα των ιδιωτικών κλειδιών της ΑΠΕΔ και των εκδοτριών ΑΠ με σκοπό την αποκατάσταση από καταστροφή. Επίσης, αναπτύσσονται μέτρα εφαρμογής ενός σχεδίου αποκατάστασης από καταστροφή. Στο σχέδιο αυτό περιλαμβάνεται η ύπαρξη χώρου αποκατάστασης από καταστροφή ώστε να ελαχιστοποιηθούν οι συνέπειες οιασδήποτε φυσικής ή άλλης καταστροφής. Η παραπάνω στρατηγική αναθεωρείται τακτικά, ελέγχεται και ενημερώνεται για να είναι λειτουργική σε περίπτωση καταστροφής. Τα μέτρα αυτά είναι σε θέση να επιτύχουν αποκατάσταση των πληροφοριακών συστημάτων και των βασικών επιχειρησιακών λειτουργιών. Τέλος, διατηρούνται αντίγραφα σε άλλο χώρο των σημαντικών πληροφοριών της ΑΠΕΔ και των εκδοτριών ΑΠ. Τέτοιες πληροφορίες περιλαμβάνουν ιδίως, αρχεία καταγραφής των συστημάτων και των εφαρμογών, στοιχεία ελέγχου, καθώς και τα αρχεία βάσεων δεδομένων για όλα τα Πιστοποιητικά που εκδίδονται.

5.8 Διακοπή/Παύση Παροχής των Υπηρεσιών της ΑΠΕΔ ή μιας Αρχής Πιστοποίησης

Στην περίπτωση που είναι απαραίτητη η διακοπή παροχής των υπηρεσιών πιστοποίησης μιας ΥπΑΠ ή σε περίπτωση παύσης εργασιών ενός Τρίτου Φορέα - Παρόχου Υπηρεσιών Πιστοποίησης, η εν λόγω ΑΠ υποχρεούται με κάθε πρόσφορο μέσο να ενημερώσει όσους επηρεάζονται άμεσα από την εν λόγω διακοπή, τους Τελικούς Χρήστες, Τρίτους Συμμετέχοντες κ.α. για τη διακοπή παροχής των υπηρεσιών πιστοποίησης πριν αυτή επέλθει, με σχετική ανακοίνωση της στην ηλεκτρονική διεύθυνση της. Για τη διακοπή παροχής των υπηρεσιών πιστοποίησης της ΑΠΕΔ, η σχετική ανακοίνωση της δημοσιεύεται στις ηλεκτρονικές διευθύνσεις http://www.yap.gov.gr, http://www.ermis.gov.gr, και http:// www.syzefxis.gov.gr.

Ενόψει της διακοπής παροχής των υπηρεσιών πιστοποίησης της ΑΠΕΔ ή μιας εκδότριας ΑΠ σύμφωνα με τα παραπάνω, αναπτύσσεται από την εν λόγω ΑΠ σχέδιο δράσης το οποίο συμμορφώνεται με το άρθρο 6, της υπ. αριθ. 248/71 Απόφαση της ΕΕΤΤ "Κανονισμός Παροχής Υπηρεσιών Πιστοποίησης Ηλεκτρονικής Υπογραφής" (ΦΕΚ 603/Β/16.05.2002), και δύναται να περιλαμβάνει κατ` ελάχιστο, τα ακόλουθα:

- Αναγγελία στους φορείς ή τα πρόσωπα που επηρεάζονται από τη διακοπή των υπηρεσιών πιστοποίησης , όπως είναι οι Τελικοί Χρήστες, οι Τρίτοι Συμμετέχοντες κ.α.
- Ανάκληση του Πιστοποιητικού ΥπΑΠ που εκδόθηκε από την ΑΠΕΔ (σε περίπτωση που διακόπτει τις υπηρεσίες πιστοποίησης μιας ΥπΑΠ).
- Διατήρηση των αρχείων και των εγγράφων της ΑΠ για τα χρονικά διαστήματα που απαιτούνται από την §5.5.2 της ΠΠ.
- Συνεχή και αδιάκοπη παροχή των υπηρεσιών υποστήριξης του Τελικού Χρήστη.
- Συνεχή παροχή των υπηρεσιών ανάκλησης, όπως είναι η έκδοση ΚΑΠ ή η υποστήριξη υπηρεσιών δικτυακού ελέγχου κατάστασης Πιστοποιητικών.
- Ανάκληση των Πιστοποιητικών Τελικών Χρηστών τα οποία δεν έχουν λήξει ή ανακληθεί.
- Προϋποθέσεις διάθεσης του ιδιωτικού κλειδιού της ΑΠ και των Ασφαλών Κρυπτογραφικών Μονάδων που περιλαμβάνουν αυτό το ιδιωτικό κλειδί με ασφαλή μέσα.

Σε περίπτωση "παύσης", δηλ. κατάργησης της αρμόδιας υπηρεσίας (εργασιών παρόχου, ΑΠΕΔ, ή εκδότριας ΑΠ) οι αρμοδιότητες και τα τηρούμενα στοιχεία μεταβιβάζονται σε άλλον φορέα ο οποίος πληροί τις απαιτούμενες προϋποθέσεις.

Εάν η παύση αφορά εκδότρια ΑΠ που αποτελεί νομικό πρόσωπο ιδιωτικού δικαίου οι αρμοδιότητες και τα τηρούμενα στοιχεία μεταβιβάζονται στην ΑΠΕΔ.

6. Τεχνικά Μέτρα Ασφαλείας

6.1 Δημιουργία και Εγκατάσταση Ζεύγους Κλειδιών

6.1.1 Δημιουργία Ζεύγους Κλειδιών

Η δημιουργία ζεύγους κλειδιών Αρχών Πιστοποίησης διενεργείται από εκπαιδευμένα και έμπιστα πρόσωπα που χρησιμοποιούν Αξιόπιστα Συστήματα και διαδικασίες οι οποίες εγγυώνται την ασφάλεια και την απαραίτητη κρυπτογραφική ισχύ για τα παραγόμενα κλειδιά. Τα κλειδιά ΑΠ παράγονται σε Τελετές Δημιουργίας Κλειδιών, οι οποίες συμμορφώνονται προς τις απαιτήσεις που περιλαμβάνονται στις καταγεγραμμένες εμπιστευτικές πολιτικές και διαδικασίες που εφαρμόζει η ΑΠΕΔ.

Η δημιουργία ζεύγους κλειδιών υπογραφής τόσο για τον Υπεύθυνο Αρχής Εγγραφής όσο και για τους Τελικούς Χρήστες διενεργείται με τη χρήση Ασφαλούς Διατάξεως Δημιουργίας Υπογραφής (ΑΔΔΥ) η οποία ακολουθεί τα κριτήρια του παραρτήματος ΙΙΙ του Π.Δ. 150/2001. Ειδικότερα, κατά τη διαδικασία της Ηλεκτρονικής Εγγραφής ή Αίτησης για Πιστοποιητικά:

- Δημιουργείται ένα ζεύγος δημόσιου - ιδιωτικού κλειδιού υπογραφής μέσα στην ΑΔΔΥ του τελικού χρήστη (όταν πρόκειται για Πιστοποιητικά που ακολουθούν την ΠΠ 1 και την ΠΠ 5).
- Το ιδιωτικό κλειδί υπογραφής παραμένει στην ΑΔΔΥ (όταν πρόκειται για Πιστοποιητικά που ακολουθούν την ΠΠ 1 και την ΠΠ 5).
- Το δημόσιο κλειδί με τα στοιχεία του τελικού χρήστη αποστέλλονται στην Αρχή Πιστοποίησης για να υπογραφούν.
- Το ιδιωτικό - δημόσιο κλειδί κρυπτογράφησης του πιστοποιητικού που ακολουθεί την ΠΠ 2 ή την ΠΠ 6 δύναται να δημιουργηθεί κεντρικά. Στην περίπτωση αυτή, η Αρχή Πιστοποίησης επιστρέφει στον Τελικό Χρήστη τα υπογεγραμμένα δημόσια κλειδιά, μαζί με το ιδιωτικό κλειδί κρυπτογράφησης που δημιουργήθηκε κεντρικοποιημένα.

6.1.2 Παράδοση Ιδιωτικού Κλειδιού

Το ζεύγος κλειδιών υπογραφής ή/και αυθεντικοποίησης (ΠΠ 1, ΠΠ 3, ΠΠ 4, ΠΠ 5 και ΠΠ 7) παράγεται από τον Τελικό Χρήστη. Ως εκ τούτου, σε αυτή την περίπτωση δεν υφίσταται παράδοση του ιδιωτικού κλειδιού στον Τελικό Χρήστη.
Όταν στην ΠΠ 2 ή/και την ΠΠ 6 το ζεύγος κλειδιών κρυπτογράφησης Τελικού Χρήστη παράγεται κεντρικοποιημένα, το ιδιωτικό κλειδί κρυπτογράφησης, παραδίδεται στον τελικό χρήστη μέσω ασφαλούς συνδέσεως SSL (Secure Socket Layer - Επιπέδου Ασφαλών Συνδέσεων).

6.1.3 Παράδοση Δημόσιου Κλειδιού στον Εκδότη του Πιστοποιητικού

Οι Τελικοί Χρήστες υποβάλλουν ηλεκτρονικά το δημόσιο κλειδί τους (ΠΠ 1, ΠΠ 3, ΠΠ 4, ΠΠ 5 και ΠΠ 7) στην εκδότρια ΑΠ που θα παράσχει τις υπηρεσίες πιστοποίησης, με τη χρήση ηλεκτρονικού αιτήματος υπογραφής πιστοποιητικού (ΑΥΠ / CSR), PKCS#10 ή άλλης ηλεκτρονικά υπογεγραμμένης μορφής, μέσω ασφαλούς συνδέσεως SSL (Secure Socket Layer - Επιπέδου Ασφαλών Συνδέσεων). Το ίδιο ισχύει και για τα Πιστοποιητικά που ακολουθούν την ΠΠ 2 ή ΠΠ 6, όταν τα κλειδιά τους δεν δημιουργούνται κεντρικοποιημένα.

6.1.4 Παράδοση Δημόσιου Κλειδιού ΑΠ σε Χρήστες

Η ΑΠΕΔ καθιστά διαθέσιμα τα Πιστοποιητικά των ΥπΑΠ στους Τελικούς Χρήστες και τους Τρίτους Συμμετέχοντες από το χώρο αποθήκευσης της.
Τα Πιστοποιητικά ΑΠ της ΑΠΕΔ μπορούν επίσης να "φορτωθούν" από Κατάλογο Lightweight Directory Access Protocol (LDAP).
Οι εκδότριες ΑΠ καθιστούν διαθέσιμη την πλήρη αλυσίδα πιστοποιητικών στον Τελικό Χρήστη κατά την έκδοση ενός Πιστοποιητικού.

6.1.5 Μέγεθος Κλειδιού

Τα ζεύγη κλειδιών της ΑΠΕΔ και των εκδοτριών ΑΠ είναι τουλάχιστον 2048 bit RSA.
Τα ζεύγη κλειδιών των Τελικών Χρηστών ορίζονται τουλάχιστον στα 1024 bit RSA.

6.1.6 Δημιουργία Κλειδιών σε Εξοπλισμό / Λογισμικό

Η ΑΠΕΔ και οι εκδότριες ΑΠ, παράγουν τα δικά τους ζεύγη κλειδιών σε Ασφαλείς Κρυπτογραφικές Μονάδες, σύμφωνα με την §6.2.1 της ΠΠ.

6.1.6.1 Δημιουργία Κλειδιών σε Ασφαλή Διάταξη Δημιουργίας Υπογραφής

Οι Τελικοί Χρήστες δημιουργούν τα ιδιωτικά κλειδιά των Πιστοποιητικών υπογραφής ή/και αυθεντικοποίησης τους (ΠΠ 1 και ΠΠ 5), κάνοντας χρήση Ασφαλούς Διάταξης Δημιουργίας Υπογραφής (ΑΔΔΥ) η οποία πληρεί τις προϋποθέσεις του παραρτήματος ΙΙΙ του ΠΔ 150/2001.

6.1.7 Σκοποί της Χρήσης Κλειδιού Πιστοποιητικού

Βλ. ΠΠ §7.1.2.1.

6.2 Προστασία Ιδιωτικού Κλειδιού

Η ΑΠΕΔ διασφαλίζει την εφαρμογή συνδυασμού φυσικών, λογικών και διαδικαστικών μέτρων τα οποία εγγυώνται την ασφάλεια των ιδιωτικών κλειδιών των ΑΠ της. Τα φυσικά μέτρα ελέγχου πρόσβασης περιγράφονται στην §5.1.2 της ΠΠ. Οι εκδότριες ΑΠ, εφαρμόζουν μέτρα ασφαλείας ανάλογου επιπέδου με αυτά που εφαρμόζει η ΑΠΕΔ.

Οι Τελικοί Χρήστες απαιτείται να λαμβάνουν τις απαραίτητες προφυλάξεις ώστε να αποτρέψουν την απώλεια, αποκάλυψη, τροποποίηση ή μη- εξουσιοδοτημένη χρήση των ιδιωτικών τους κλειδιών.

6.2.1 Πρότυπα για τις Ασφαλείς Κρυπτογραφικές Μονάδες (ΑΚΜ)
Για τη δημιουργία και αποθήκευση ιδιωτικών κλειδιών της ΑΠΕΔ και των εκδοτριών ΑΠ χρησιμοποιούνται Ασφαλείς Κρυπτογραφικές Μονάδες (ΑΚΜ) οι οποίες έχουν αξιολογηθεί με βάση τα κριτήρια που ορίζει η κείμενη νομοθεσία.

6.2.2 Έλεγχος Πολλαπλών Προσώπων (m από η) Ιδιωτικού Κλειδιού
Ο έλεγχος από πολλαπλά πρόσωπα αποσκοπεί στην προστασία των δεδομένων ενεργοποίησης που απαιτούνται για την ενεργοποίηση των ιδιωτικών κλειδιών ΑΠ, τα οποία φυλάσσονται από τις Αρχές Πιστοποίησης. Η ΑΠΕΔ και οι εκδότριες ΑΠ χρησιμοποιούν τον "Διαχωρισμό Απόρρητων Μεριδίων" μέσω του οποίου διαχωρίζουν τα ιδιωτικά κλειδιά ή τα δεδομένα ενεργοποίησης που είναι απαραίτητα για τη λειτουργία ενός ιδιωτικού κλειδιού σε ξεχωριστά μέρη, τα οποία καλούνται "Απόρρητα Μερίδια" και τα οποία τηρούνται από πρόσωπα που ονομάζονται "Τηρητές Μεριδίων". Για τη λειτουργία ενός ιδιωτικού κλειδιού θα απαιτείται ένας οριακός αριθμός Απόρρητων Μεριδίων (m) εκ του συνολικού αριθμού των Απόρρητων Μεριδίων (η). Ο οριακός αριθμός μεριδίων που απαιτείται για την υπογραφή μίας Αρχής Πιστοποίησης είναι 3.

6.2.3 Παρακαταθήκη Ιδιωτικού Κλειδιού
Για τα Πιστοποιητικά που εκδίδονται σύμφωνα με την ΠΠ 2 ή την ΠΠ 6, η εκδότρια ΑΠ δύναται να τηρεί τα ιδιωτικά κλειδιά των τελικών χρηστών, αποκλειστικά για εξουσιοδοτημένους σκοπούς ανάκτησης. Οι εκδότριες ΑΠ που παρέχουν αυτή την υπηρεσία, περιγράφουν στη Δήλωση Πρακτικής τους τις διαδικασίες που εφαρμόζονται και όλα τα σχετικά μέτρα ελέγχου.
Για τις υπόλοιπες πολιτικές πιστοποιητικών η ΑΠΕΔ και οι εκδότριες ΑΠ δεν τηρούν ιδιωτικά κλειδιά ΑΠ ή τελικού χρήστη.

6.2.4 Δημιουργία Εφεδρικού Αντιγράφου Ιδιωτικού Κλειδιού
Δημιουργούνται εφεδρικά αντίγραφα των ιδιωτικών κλειδιών ΑΠ για την περίπτωση ανάκτησης (τακτικής ή έκτακτης). Τα κλειδιά αυτά αποθηκεύονται σε κρυπτογραφημένη μορφή εντός Ασφαλών Κρυπτογραφικών Μονάδων οι οποίες πληρούν τις προδιαγραφές της §6.2.1 της ΠΠ. Τα ιδιωτικά κλειδιά ΑΠ αντιγράφονται σε εφεδρικές Ασφαλείς Κρυπτογραφικές Μονάδες σύμφωνα με την §6.2.5 της ΠΠ.Οι Ασφαλείς Κρυπτογραφικές Μονάδες που περιέχουν τα εφεδρικά αντίγραφα των ιδιωτικών κλειδιών ΑΠ υπόκεινται στις προδιαγραφές της §6.2.1 της ΠΠ. Οι Ασφαλείς Κρυπτογραφικές Μονάδες που περιέχουν αντίγραφα για την περίπτωση αποκατάστασης από καταστροφή του ιδιωτικού κλειδιού ΑΠ υπόκεινται στις προδιαγραφές της §6.2.1 της ΠΠ.
Για τα ιδιωτικά κλειδιά των Πιστοποιητικών υπογραφής ή/και αυθεντικό ποίησης των Τελικών Χρηστών (ΠΠ 1 και ΠΠ 5) δεν παρέχεται η δυνατότητα δημιουργίας εφεδρικού αντιγράφου (Π.Δ. 150/2001).

6.2.5 Αρχειοθέτηση Ιδιωτικών Κλειδιών
Με το τέλος της περιόδου ισχύος τους το ζεύγος κλειδιών της ΑΠΕΔ αρχειοθετείται για χρονικό διάστημα 30 ετών. Το αρχειοθετημένο ζεύγος κλειδιών ΑΠ αποθηκεύεται με ασφαλή τρόπο με τη χρήση Ασφαλών Κρυπτογραφικών Μονάδων οι οποίες πληρούν τις προδιαγραφές της §6.2.1 της ΠΠ. Διαδικαστικά μέτρα ελέγχου αποτρέπουν την επιστροφή των αρχειοθετημένων ζευγών κλειδιών ΑΠΕΔ σε παραγωγική χρήση. Με το πέρας του χρονικού διαστήματος αρχειοθέτησης, τα αρχειοθετημένα ιδιωτικά κλειδιά της ΑΠΕΔ θα καταστραφούν με ασφαλή τρόπο και σύμφωνα με την §6.2.10 της ΠΠ.
Με το τέλος της περιόδου ισχύος τους τα ζεύγη κλειδιών των εκδοτριών ΑΠ αρχειοθετούνται για χρονικό διάστημα 30 ετών. Τα αρχειοθετημένα ζεύγη κλειδιών ΑΠ αποθηκεύονται με ασφαλή τρόπο με τη χρήση Ασφαλών Κρυπτογραφικών Μονάδων οι οποίες πληρούν τις προδιαγραφές της §6.2.1 της ΠΠ. Διαδικαστικά μέτρα ελέγχου αποτρέπουν την επιστροφή των αρχειοθετημένων ζευγών κλειδιών ΑΠ σε παραγωγική χρήση. Με το πέρας του χρονικού διαστήματος αρχειοθέτησης, τα αρχειοθετημένα ιδιωτικά κλειδιά της ΑΠ θα καταστραφούν με ασφαλή τρόπο και σύμφωνα με την §6.2.10 της ΠΠ.
Η ΑΠΕΔ και οι εκδότριες ΑΠ δεν αρχειοθετούν αντίγραφα των ιδιωτικών κλειδιών Τελικών χρηστών, πάρα μόνο στην περίπτωση της ΠΠ 2 ή της ΠΠ 6, όταν η εκδότρια ΑΠ παρέχει την υπηρεσία αρχειοθέτησης, για σκοπούς ανάκτησης του κλειδιού κρυπτογράφησης.

6.2.6 Μεταφορά Ιδιωτικού Κλειδιού Από και Προς Μια Κρυπτογραφική Μονάδα

Όταν απαιτείται η μεταφορά ενός εφεδρικού αντιγράφου ζεύγους κλειδιών ΑΠ σε άλλη ΑΚΜ, η μεταφορά πραγματοποιείται με ασφάλεια, ούτως ώστε να αποτραπεί ο κίνδυνος απώλειας, κλοπής, τροποποίησης, μη εξουσιοδοτημένης αποκάλυψης ή μη εξουσιοδοτημένης χρήσης του. Τα ιδιωτικά κλειδιά είναι σε κρυπτογραφημένη μορφή κατά τη μεταφορά.

6.2.7 Αποθήκευση Ιδιωτικού Κλειδιού σε Κρυπτογραφική Μονάδα

Τα ιδιωτικά κλειδιά ΑΠ ή ΑΕ, τα οποία φυλάσσονται σε Ασφαλείς Κρυπτογραφικές Μονάδες, αποθηκεύονται σε κρυπτογραφημένη μορφή.

6.2.8 Μέθοδος Ενεργοποίησης Ιδιωτικού Κλειδιού

6.2.8.1 Ιδιωτικά Κλειδιά Τελικού Χρήστη σε ΑΔΔΥ

Οι Τελικοί Χρήστες που αποκτούν Πιστοποιητικά σύμφωνα με την ΠΠ 1 ή ΠΠ 5, ή/και στις περιπτώσεις που το απαιτεί η εκδότρια ΑΠ, θα πρέπει να κάνουν χρήση των Ασφαλών Διατάξεων Δημιουργίας Υπογραφής (ΑΔΔΥ) που τους έχουν χορηγηθεί προκειμένου να αποθηκεύσουν, χρησιμοποιήσουν ή ενεργοποιήσουν τα ιδιωτικά τους κλειδιά. Παράλληλα θεωρείται υποχρεωτική από τους Τελικούς Χρήστες:

- Η χρήση του συνθηματικού πρόσβασης στην ΑΔΔΥ PIN/Personal Identification Number (ή του μυστικού αριθμού PUK/Personal Unblocking Key στην περίπτωση απώλειας του PIN), σύμφωνα με την §6.4.1 της ΠΠ για την εξακρίβωση της ταυτότητας τους πριν από την ενεργοποίηση του ιδιωτικού τους κλειδιού.
- Η λήψη ευλόγων μέτρων για τη φυσική προστασία του χώρου και σταθμού εργασίας τους ώστε να αποτραπεί η χρήση των ανωτέρω καθώς και των αντίστοιχων ιδιωτικών κλειδιών χωρίς την έγκριση τους.

6.2.8.2 Ιδιωτικά Κλειδιά Τελικού Χρήστη Χαλαρής Αποθήκευσης

Οι Τελικοί Χρήστες που αποκτούν πιστοποιητικά που δεν αποθηκεύονται σε ΑΔΔΥ, ή/και στις περιπτώσεις που το απαιτεί η εκδότρια ΑΠ, θα πρέπει να λαμβάνουν εύλογα μέτρα για τη φυσική προστασία του χώρου και σταθμού εργασίας τους ώστε να αποτραπεί η χρήση των ανωτέρω καθώς και των αντίστοιχων ιδιωτικών κλειδιών χωρίς την έγκριση τους.

Η παράγραφος αυτή αφορά στα Πιστοποιητικά που ακολουθούν την ΠΠ3, καθώς και τις ΠΠ2, ΠΠ4 και ΠΠ6, όταν για τα Πιστοποιητικά αυτά δεν υπάρχει απαίτηση δημιουργίας και αποθήκευσης σε ΑΔΔΥ.

6.2.9 Μέθοδος Απενεργοποίησης Ιδιωτικού Κλειδιού

Τα ιδιωτικά κλειδιά ΑΠ απενεργοποιούνται με την αφαίρεση τους από τη συσκευή ανάγνωσης.

Τα ιδιωτικά κλειδιά Τελικών Χρηστών (για την ΠΠ 1 και ΠΠ 5) καθώς και των Υπεύθυνων ΑΕ μπορούν να απενεργοποιηθούν με την αφαίρεση της ΑΔΔΥ από τη συσκευή ανάγνωσης καρτών ή τη θύρα του ηλεκτρονικού υπολογιστή. Τα ιδιωτικά κλειδιά Τελικών Χρηστών για τις υπόλοιπες ΠΠ, μπορούν να απενεργοποιηθούν μετά από κάθε εφαρμογή, με την αποσύνδεση του συστήματος. Σε κάθε περίπτωση, οι Υπεύθυνοι ΑΕ καθώς και οι Τελικοί Χρήστες έχουν υποχρέωση να προστατεύουν επαρκώς τα ιδιωτικά κλειδιά τους σύμφωνα με την §6.4 της ΠΠ.

6.2.10 Μέθοδος Καταστροφής Ιδιωτικού Κλειδιού

Με το πέρας του λειτουργικού χρόνου ζωής μιας ΑΠ, ένα ή περισσότερα αντίγραφα του ιδιωτικού κλειδιού της ΑΠ αρχειοθετούνται σύμφωνα με την §6.2.5 της ΠΠ.

Τα υπόλοιπα αντίγραφα του ιδιωτικού κλειδιού της ΑΠ καταστρέφονται με ασφαλή τρόπο.

Επιπλέον, τα αρχειοθετημένα ιδιωτικά κλειδιά της ΑΠ καταστρέφονται με ασφαλή τρόπο με το πέρας του χρονικού διαστήματος αρχειοθέτησης τους.

Όταν είναι απαραίτητο, η ΑΠΕΔ καταστρέφει τα ιδιωτικά κλειδιά ΥπΑΠ με τρόπο που λογικά εξασφαλίζει ότι δεν θα παραμείνουν μέρη του κλειδιού αυτού τα οποία θα μπορούσαν να οδηγήσουν στην ανασύνθεση του. Η ΑΠΕΔ χρησιμοποιεί τη λειτουργία διαγραφής του περιεχομένου των Ασφαλών Κρυπτογραφικών Μονάδων της
καθώς και άλλα κατάλληλα μέτρα ώστε να εξασφαλίζει την πλήρη καταστροφή των ιδιωτικών κλειδιών ΑΠ. Οι ενέργειες καταστροφής κλειδιών ΑΠ καταγράφονται κατά την εκτέλεση τους.

Ανάλογα μέτρα εφαρμόζονται και από τις εκδότριες ΑΠ.

6.2.11 Αξιολόγηση Κρυπτογραφικής Μονάδας

Βλ. §6.2.1 της ΠΠ.

6.3 Άλλα Θέματα Διαχείρισης του Ζεύγους Κλειδιών

6.3.1 Αρχειοθέτηση Δημόσιου Κλειδιού

Από τα Πιστοποιητικά ΑΠ και τελικών χρηστών δημιουργούνται αντίγραφα ασφαλείας τα οποία αρχειοθετούνται ως μέρος της τακτικής διαδικασίας δημιουργίας αντιγράφων.

6.3.2 Περίοδος Χρήσης των Δημόσιων και Ιδιωτικών Κλειδιών

Η Λειτουργική Περίοδος ενός Πιστοποιητικού ολοκληρώνεται με τη λήξη ή την ανάκληση του. Η Λειτουργική Περίοδος για τα ζεύγη κλειδιών είναι ίδια με τη Λειτουργική Περίοδο των αντίστοιχων Πιστοποιητικών. Τα ιδιωτικά κλειδιά βέβαια μπορούν να συνεχίσουν να χρησιμοποιούνται για αποκρυπτογράφηση και τα δημόσια κλειδιά για επαλήθευση υπογραφής. Οι μέγιστες Λειτουργικές Περίοδοι των Πιστοποιητικών των ΑΠ για Πιστοποιητικά που εκδίδονται από την έναρξη ισχύος της παρούσας ΠΠ και μετά παρατίθενται στον Πίνακα 7.
Επιπροσθέτως, η ΑΠΕΔ και οι εκδότριες ΑΠ παύουν να εκδίδουν νέα Πιστοποιητικά εγκαίρως πριν από τη λήξη του Πιστοποιητικού τους, έτσι ώστε να διασφαλίζεται ότι κανένα Πιστοποιητικό το οποίο θα εκδοθεί από την ΑΠΕΔ ή τις εκδότριες ΑΠ δεν θα λήγει μετά τη λήξη του δικού τους Πιστοποιητικού.

Πίνακας 7: Λειτουργικές Περίοδοι Πιστοποιητικών

Πιστοποιητικό	Λειτουργική Περίοδος
Πρωτεύουσας Αρχής Πιστοποίησης (ΑΠΕΔ) αυτοϋπογραφόμενο	Μέχρι 20 έτη
ΑΠΕΔ προς ΥπΑΠ	Μέχρι 10 έτη
Εκδότρια ΑΠ προς Τελικό Χρήστη	Μέχρι 5 έτη

Η ΑΠΕΔ και οι εκδότριες ΑΠ παύουν να χρησιμοποιούν τα ζεύγη κλειδιών ΑΠ μετά τη λήξη της περιόδου χρήσης τους.

6.4 Δεδομένα Ενεργοποίησης

6.4.1 Δημιουργία και Εγκατάσταση Δεδομένων Ενεργοποίησης

Η ΑΠΕΔ και οι εκδότριες ΑΠ συνιστούν σε όλους τους Τελικούς Χρήστες να χρησιμοποιούν πάντα συνθηματικά πρόσβασης (Personal identification number - PIN), τόσο για την προστασία των κλειδιών που είναι αποθηκευμένα στο σταθμό εργασίας τους αλλά και του ίδιου του σταθμού εργασίας τους, όσο και για την προστασία της ΑΔΔΥ τους, όταν γίνεται χρήση αυτής.

6.4.2 Προστασία Δεδομένων Ενεργοποίησης

Οι Τελικοί Χρήστες οφείλουν να λαμβάνουν κάθε απαραίτητο μέτρο για τη διαφύλαξη και μη γνωστοποίηση των δεδομένων ενεργοποίησης των ιδιωτικών τους κλειδιών.

6.5 Μέτρα Ασφαλείας των Υπολογιστών

Όλες οι αρμοδιότητες των ΑΠ ασκούνται χρησιμοποιώντας Αξιόπιστα Συστήματα.

6.5.1 Τεχνικές Προδιαγραφές Ασφάλειας Υπολογιστών

Όλα τα συστήματα λογισμικού και αρχείων των ΑΠ αποτελούν Αξιόπιστα Συστήματα ασφαλή από μη - εξουσιοδοτημένη πρόσβαση. Οι χρήστες γενικών εφαρμογών δεν διαθέτουν λογαριασμούς σε εξυπηρετητές παραγωγής (production servers).
Επίσης υπάρχει λογικός διαχωρισμός του δικτύου παραγωγής από τα άλλα τμήματα έτσι ώστε να επιτρέπεται η πρόσβαση μόνο μέσω καθορισμένων διαδικασιών.
Επίσης χρησιμοποιούνται συστήματα προστασίας (firewalls) για την προστασία του δικτύου παραγωγής από εσωτερική και εξωτερική διείσδυση, καθώς και για τον περιορισμό της φύσης και της προέλευσης των δραστηριοτήτων οι οποίες θα μπορούσαν να προσπελάσουν τα συστήματα αυτά.
Τέλος απαιτείται η χρήση συνθηματικών πρόσβασης (passwords), που θα αλλάζουν σε περιοδική βάση, με συγκεκριμένο αριθμό χαρακτήρων και συνδυασμό αλφαριθμητικών και ειδικών χαρακτήρων.

6.5.2 Όρια Ασφαλείας των Υπολογιστών

Η έκδοση του βασικού λογισμικού του Κέντρου Επεξεργασίας που χρησιμοποιεί η ΑΠΕΔ πληρεί τις προδιαγραφές εγγυήσεων EAL 4 του ISO/IEC 15408-3:1999, Information technology - Security techniques - Evaluation criteria για IT

security - Part 3: Security assurance requirements (Πληροφορική - Τεχνικές ασφάλειας - Κριτήρια αξιολόγησης για την ασφάλεια πληροφορικών συστημάτων - Μέρος 3: Προδιαγραφές εγγυήσεων ασφάλειας) για την αξιολόγηση του λογισμικού από ανεξάρτητο εργαστήριο βάσει των Common Criteria.

6.6 Τεχνικοί Έλεγχοι κατά τον Κύκλο Ζωής Πιστοποιητικού

6.6.1 Μέτρα Ελέγχου Ανάπτυξης Συστήματος

Η ΑΠΕΔ, οι εκδότριες ΑΠ και οι ΑΕ, χρησιμοποιούν λογισμικό διαχείρισης Πιστοποιητικών το οποίο σχεδιάζεται και αναπτύσσεται μέσω διαδικασιών διασφάλισης ποιότητας, ώστε να μπορεί να επαληθευτεί ότι το λογισμικό του συστήματος δεν έχει τροποποιηθεί πριν από την εγκατάσταση και είναι κατάλληλο για τη συγκεκριμένη χρήση.

6.6.2 Μέτρα Ελέγχου Διαχείρισης Ασφάλειας

Η ΑΠΕΔ διασφαλίζει την τήρηση των όρων και προϋποθέσεων της παρούσας ΠΠ από τα συστήματα της ΑΠΕΔ και των εκδοτριών ΑΠ. Η ΑΠΕΔ επαληθεύει περιοδικά, την αρτιότητα των συστημάτων της ΑΠΕΔ και των ΥπΑΠ.

6.7 Μέτρα Ελέγχου Ασφάλειας Δικτύου

Όλες οι υπηρεσίες πιστοποίησης των ΑΠ παρέχονται χρησιμοποιώντας ασφαλή δίκτυα σύμφωνα με την ισχύουσα Πολιτική Ασφαλείας ώστε να αποτραπεί μη - εξουσιοδοτημένη πρόσβαση ή άλλη κακόβουλη ενέργεια.
Επίσης προστατεύεται η κοινοποίηση εμπιστευτικών πληροφοριών με τη χρήση κρυπτογράφησης και ψηφιακών υπογραφών.

6.8 Χρονοσήμανση

Τα αρχεία καταγραφής, τα Πιστοποιητικά, οι ΚΑΠ και άλλες εγγραφές ανάκλησης περιλαμβάνουν πληροφορίες ημερομηνίας και ώρας. Ο χρόνος αυτός θα πρέπει να λαμβάνεται από μια αξιόπιστη πηγή χρόνου.

7. Προφίλ Πιστοποιητικού, Καταλόγου Ανακληθέντων Πιστοποιητικών (ΚΑΠ) και OCSP

7.1 Προφίλ Πιστοποιητικού

Στην παρούσα παράγραφο ορίζονται οι προδιαγραφές του Προφίλ και του περιεχομένου των Πιστοποιητικών της ΑΠΕΔ και των εκδοτριών ΑΠ που εκδίδονται σύμφωνα με την παρούσα ΠΠ.
Τα Πιστοποιητικά της ΑΠΕΔ) συμμορφώνονται με (α) το ITU-T Recommendation X.509 (1997):Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 και (β) το RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 5280") [Προφίλ Πιστοποιητικού Υποδομής Δημοσίου Κλειδιού Δια-δικτύου X.509 και ΚΑΠ].
Το περιεχόμενο των Πιστοποιητικών που ακολουθούν την ΠΠ 1, ΠΠ 3, ΠΠ 4 και ΠΠ 5 συμφωνεί με το "Προφίλ Αναγνωρισμένου Πιστοποιητικού" ("Qualified Certificate Profile") της τεχνικής προδιαγραφής "ETSI 101 86Z. Η συμμόρφωση με το "Προφίλ Αναγνωρισμένου Πιστοποιητικού" ("Qualified Certificate Profile") έχει ως αποτέλεσμα τα Πιστοποιητικά που ακολουθούν την ΠΠ 1, ΠΠ 3, ΠΠ 4 και ΠΠ 5 να βρίσκονται σε συμφωνία με το RFC 3739, όπου αυτό δεν συγκρούεται με αυτό το Προφίλ. Επίσης τα βασικά πεδία των Πιστοποιητικών ΠΠ 1, ΠΠ 3, ΠΠ 4 και ΠΠ 5 βρίσκονται σε συμμόρφωση με την Ευρωπαϊκή Οδηγία 99/93/ΕΚ όπως έχει ενσωματωθεί στην ελληνική έννομη τάξη με το ΠΔ 150/2001.
Αυτό σημαίνει ότι στα Πιστοποιητικά που ακολουθούν την ΠΠ 1, ΠΠ 3, ΠΠ 4 και ΠΠ 5 περιλαμβάνονται:

- Στοιχεία επαλήθευσης υπογραφής (δημόσιο κλειδί υποκειμένου - subject public key).
- Ένδειξη έναρξης και λήξης της περιόδου ισχύος (valid from-valid to).
- Ο κώδικας ταυτοποίησης του πιστοποιητικού (serial number).
- Η Προηγμένη Ηλεκτρονική Υπογραφή του παρόχου υπηρεσιών πιστοποίησης που εκδίδει το πιστοποιητικό.

Αντίστοιχες υποχρεώσεις αναλαμβάνονται και για τα Πιστοποιητικά που ακολουθούν την ΠΠ 2, ΠΠ 6 και ΠΠ 7, αν και δεν ακολουθείται το ανωτέρω πρότυπο.
Κατ` ελάχιστο, τα Πιστοποιητικά X.509 της ΑΠΕΔ και των εκδοτριών ΑΠ περιλαμβάνουν τα βασικά πεδία X.509 Έκδοσης 3 και τις προτεινόμενες καθορισμένες τιμές ή περιορισμούς τιμών που αναφέρονται στον ακόλουθο πίνακα.

Πίνακας 8 : Βασικά πεδία προφίλ Πιστοποιητικού

Πεδίο	Τιμή ή Περιορισμός Τιμής
Version (Έκδοση)	Βλ. ΠΠ §7.1.1
Serial Number (Αριθμός Σειράς)	Μοναδική τιμή ανά Διακριτικό Όνομα Εκδότη (Issuer DN)
Signature Algorithm (Αλγόριθμος Υπογραφής)	Ο αλγόριθμος που χρησιμοποιήθηκε για την υπογραφή του Πιστοποιητικού (Βλ. §7.1.3 της ΠΠ)
Issuer DN (Διακριτικό Όνομα Εκδότη)	Βλ. §7.1.4 της ΠΠ
Valid From (Ισχύει Από)	Βάσει του Universal Coordinate Time. Κωδικοποίηση σύμφωνα με το RFC 5280.
Valid To (Ισχύει Μέχρι)	Βάσει του Universal Coordinate Time. Κωδικοποίηση σύμφωνα με το RFC 5280. Η περίοδος ισχύος θα καθορίζεται σύμφωνα με τους περιορισμούς που ορίζει η §6.3.2 της ΠΠ.
Subject DN (Διακριτικό Όνομα Υποκειμένου)	Βλ. §7.1.4 της ΠΠ
Subject Public Key (Δημόσιο Κλειδί Υποκειμένου)	Κωδικοποιημένο σύμφωνα με το RFC 5280 με τη χρήση αλγορίθμων που προσδιορίζονται στην §7.1.3 της ΠΠ και με μήκη κλειδιών που προσδιορίζονται στην §6.1.5 της ΠΠ.
Signature (Υπογραφή)	Παράγεται και κωδικοποιείται σύμφωνα με το RFC 5280

Ο πίνακας 8 αντικαταστάθηκε ως άνω, με την ΚΥΑ με αριθμ. ΥΑΠ/Φ.60/3431 (ΦΕΚ Β 3320/27.12.2013) παρ.3.

7.1.1 Αριθμός (-οί) έκδοσης

Τα Πιστοποιητικά των εκδοτριών ΑΠ και Τελικών Χρηστών αποτελούν Πιστοποιητικά X.509 Έκδοσης 3 και το πεδίο έκδοσης τους (version) θα έχει την τιμή V3 (2) σύμφωνα με το RFC 5280.

Η παρ. 7.1.1. αντικαταστάθηκε ως άνω, με την ΚΥΑ με αριθμ. ΥΑΠ/Φ.60/3431 (ΦΕΚ Β 3320/27.12.2013) παρ.4.

7.1.2 Επεκτάσεις Πιστοποιητικών

Στα Πιστοποιητικά X.509 Έκδοσης 3, αναγράφονται οι επεκτάσεις που απαιτούνται σύμφωνα με τις §7.1.2.1 - §7.1.2.9 της ΠΠ.

7.1.2.1 Χρήση Κλειδιού (Key Usage)

Τα στοιχεία που υπάρχουν στην επέκταση KeyUsage (Χρήση Κλειδιού) για τα Πιστοποιητικά X.509 Έκδοσης 3 της ΑΠΕΔ και των εκδοτριών ΑΠ είναι σύμφωνα με το RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL (Προφίλ Πιστοποιητικού Υποδομής Δημοσίου Κλειδιού Διαδικτύου X.509 και ΚΑΠ).

Η επέκταση KeyUsage (Χρήση Κλειδιού) στην ουσία ορίζει την προβλεπόμενες χρήσεις του Πιστοποιητικού, όπως αυτές έχουν οριστεί από την εκδότρια ΑΠ. Η επέκταση αυτή, για τα Πιστοποιητικά της ΑΠΕΔ και των εκδοτριών ΑΠ και των Πιστοποιητικών Τελικού Χρήστη παρατίθεται στον Πίνακα 9 με την ακόλουθη εξαίρεση:

- Το πεδίο κρισιμότητας (criticality) της επέκτασης KeyUsage (Χρήση Κλειδιού) ορίζεται ως ΑΛΗΘΕΣ (TRUE) για τα πιστοποιητικά ΑΠ και ως ΨΕΥΔΕΣ (FALSE) γιατα Πιστοποιητικά Τελικών Χρηστών.

Η μόνη διάκριση που υπάρχει μεταξύ των πολιτικών για τα Πιστοποιητικά τελικών χρηστών είναι ότι:

- Για την ΠΠ 1, ΠΠ 3, ΠΠ 5, και ΠΠ 7, και όταν πρόκειται για Πιστοποιητικά υπογραφής ορίζεται η ψηφιακή υπογραφή (digitalSignature, 0) και η μη αποκήρυξη (nonRepudiation, 1).
- Για την ΠΠ 1, ΠΠ 3, ΠΠ5, και ΠΠ 7 και όταν πρόκειται για Πιστοποιητικά αυθεντικοποίησης ως χρήση κλειδιού ορίζεται η ψηφιακή υπογραφή (digitalSignature, 0).
- Για την ΠΠ 2, και την ΠΠ 6 ορίζεται η κρυπτογράφηση κλειδιού (keyEncipherment, 2) και δεδομένων (dataEncipherment, 3).
- Για την ΠΠ 7 ορίζεται η ψηφιακή υπογραφή (digitalSignature, 0) και η μη αποκήρυξη (nonRepudiation, 1) και η κρυπτογράφηση κλειδιού (keyEncipherment, 2)και δεδομένων (dataEncipherment, 3).

Για την ΠΠ 4 η επέκταση αυτή δε συμπεριλαμβάνεται στο πιστοποιητικό.

Πίνακας 9: Ρυθμίσεις για την Επέκταση Χρήση Κλειδιού (KeyUsage)

		Αρχές Πιστοποίησης	Πιστοποιητικό Υπογραφής – Αυθεντικοποίησης Τελικών Χρηστών (ΠΠ 1, ΠΠ 3, ΠΠ 5)	Πιστοποιητικό Κρυπτογράφησης Τελικών Χρηστών (ΠΠ 2 και ΠΠ 6)	Πιστοποιητικό Φορέα Δημοσίου Τομέα (ΠΠ 7)
	Κρισιμότητα	**ΑΛΗΘΕΣ (TRUE)**	**ΨΕΥΔΗΣ (FALSE)**	**ΨΕΥΔΗΣ (FALSE)**	**ΨΕΥΔΗΣ (FALSE)**
0	digitalSignature (Ψηφιακή Υπογραφή)	Ελεύθερο	Ορίζεται (set)	Ελεύθερο Ορίζεται (set)	
1	nonRepudiation (Μη Αποκήρυξη)	Ελεύθερο	Ορίζεται (set)	Ελεύθερο	Ορίζεται (set)
2	keyEncipherment (Κρυπτογράφηση Κλειδιού)	Ελεύθερο	Ελεύθερο	Ορίζεται (set)	Ορίζεται (set)
3	dataEncipherment (Κρυπτογράφηση Δεδομένων)	Ελεύθερο	Ελεύθερο	Ορίζεται (set)	Ορίζεται (set)
4	keyAgreement (Συμφωνία Κλειδιού	Ελεύθερο	Ελεύθερο	Ελεύθερο	Ελεύθερο
5	keyCertSign (Κλειδί Υπογραφής Πιστοποιητικού)	Ορίζεται (set)	Ελεύθερο	Ελεύθερο	Ελεύθερο
6	CRLSign (Υπογραφή ΚΑΠ)	Ορίζεται (set)	Ελεύθερο	Ελεύθερο	Ελεύθερο
7	encipherOnly (Μόνο κρυπτογράφηση)	Ελεύθερο	Ελεύθερο	Ελεύθερο	Ελεύθερο
8	decipherOnly (Μόνο αποκρυπτογράφηση)	Ελεύθερο	Ελεύθερο	Ελεύθερο	Ελεύθερο

7.1.2.2 Επέκταση Πολιτικών Πιστοποιητικού (Certificate Policies extension)

Τα Πιστοποιητικά Τελικού Χρήστη Χ.509Έκδοσης 3 δύναται να χρησιμοποιήσουν επέκταση CertificatePolicies (Πολιτικές Πιστοποιητικού) όπου θα αναγράφεται ο ισχύων προσδιοριστής αντικειμένου (object identifier) σύμφωνα με την §7.1.5 της ΠΠ και οι περιγραφείς πολιτικής (policy qualifiers) που παρατίθενται στην §7.1.6 της ΠΠ. Το πεδίο κρισιμότητας της επέκτασης αυτής ορίζεται ως ΨΕΥΔΕΣ (FALSE).

7.1.2.3 Εναλλακτικά Ονόματα Υποκειμένου (Subject Alternative Names)

Η επέκταση subjectAltName υποστηρίζεται για τα πιστοποιητικά Χ.509`Εκδοσης 3 σύμφωνα με το RFC 5280. Το πεδίο κρισιμότητας της επέκτασης αυτής ορίζεται ως ΨΕΥΔΕΣ (FALSE).

Στην επέκταση αυτή και πιο συγκεκριμένα, στο ίδιο χαρακτηριστικό του τύπου rfc822Name περιλαμβάνεται προαιρετικά η διεύθυνση ηλεκτρονικής αλληλογραφίας του κατόχου του Πιστοποιητικού.

Για Πιστοποιητικά που εκδίδονται σύμφωνα με την ΠΠ 4 η επέκταση αυτή περιλαμβάνει και τομεακά αναγνωριστικά ώστε να διευκολυνθεί η μονοσήμαντη αναγνώριση του κατόχου του Πιστοποιητικού, όπου αυτό κρίνεται απαραίτητο.

Η πρόσβαση στα τομεακά αναγνωριστικά παρέχεται μόνο σε εξουσιοδοτημένους χρήστες και προστατεύεται με κατάλληλους μηχανισμούς κρυπτογράφησης αυτών.

7.1.2.4 Βασικοί Περιορισμοί (Basic Constraints)

Η ΑΠΕΔ αναγράφει στα Πιστοποιητικά ΥπΑΠ Χ.509 Έκδοσης 3 την επέκταση BasicConstraints (Βασικοί Περιορισμοί όπου το πεδίο CA (ΑΠ) έχει οριστεί ως ΑΛΗΘΕΣ (TRUE).

Στα Πιστοποιητικά Τελικού Χρήστη που εκδίδουν οι εκδότριες ΑΠ το πεδίο της επέκτασης BasicConstraints (Βασικοί Περιορισμοί παραμένει κενό υποδηλώνοντας πως έχει οριστεί ως End Entity (Τελικό Πρόσωπο). Το πεδίο κρισιμότητας (criticality) της επέκτασης BasicConstraints (Βασικοί Περιορισμοί ορίζεται ως ΑΛΗΘΕΣ (TRUE) για τα Πιστοποιητικά εκδοτριών ΑΠ και ΨΕΥΔΕΣ (FALSE) για τα Πιστοποιητικά των Τελικών Χρηστών.

Τα Πιστοποιητικά εκδοτριών ΑΠ Χ.509`Εκδοσης 3 εκδίδονται ορίζοντας στο πεδίο pathLenConstraint (περιορισμός Μήκους Διαδρομής) της επέκτασης Basic Constraints (Βασικοί Περιορισμοί) το μέγιστο αριθμό πιστοποιητικών ΑΠ που μπορούν να ακολουθήσουν το Πιστοποιητικό αυτό σε μια διαδρομή πιστοποίησης. Τα Πιστοποιητικά εκδοτριών ΑΠ, έχουν στο πεδίο pathLenConstraint (περιορισμός Μήκους Διαδρομής) την τιμή "0" υποδεικνύοντας ότι μόνο ένα Πιστοποιητικό Τελικού Χρήστη μπορεί να ακολουθήσει τη διαδρομή πιστοποίησης.

7.1.2.5 Εκτεταμένη Χρήση Κλειδιού (Extended Key Usage)

Η επέκταση ExtendedKeyUsage (Εκτεταμένη Χρήση Κλειδιού) χρησιμοποιείται από την ΑΠΕΔ και τις εκδότριες ΑΠ για τα Πιστοποιητικά Τελικών Χρηστών που εκδίδει (Χ.509`Εκδοσης 3) στις ακόλουθες περιπτώσεις (Πίνακας 10).

Πίνακας 10: Ρυθμίσεις για την Επέκταση - Εκτεταμένη Χρήση Κλειδιού

		Πιστοποιητικό Υπογραφής – Αυθεντικοποίησης Τελικών Χρηστών (ΠΠ 1, ΠΠ 3, και ΠΠ 5)	Πιστοποιητικό Τομεακής Αυθεντικοποίησης Τελικών Χρηστών (ΠΠ 4)	Πιστοποιητικό Κρυπτογράφησης Τελικών Χρηστών (ΠΠ 2 και ΠΠ 6)
Criticality (κρισιμότητα)		**ΨΕΥΔΗΣ (FALSE)**	**ΨΕΥΔΗΣ (FALSE)**	**ΨΕΥΔΗΣ (FALSE)**
0	ServerAuth (Ταυτοποίηση Εξυπηρετητή)	Ελεύθερο	Ελεύθερο	Ελεύθερο
1	ClientAuth (Ταυτοποίηση Χρήστη)	Ορίζεται	Ορίζεται	Ελεύθερο
2	CodeSigning (Υπογραφή Κωδικού)	Ελεύθερο	Ελεύθερο	Ελεύθερο
3	EmailProtection (Προστασία Email)	Ορίζεται	Ελεύθερο	Ορίζεται
4	IpsecEndSystem (τελικό Σύστημα IPsec)	Ελεύθερο	Ελεύθερο	Ελεύθερο
5	ipsecTunnel (δίαυλος IPsec)	Ελεύθερο	Ελεύθερο	Ελεύθερο
6	ipsecUser (Χρήστης IPsec)	Ελεύθερο	Ελεύθερο	Ελεύθερο
7	TimeStamping (Χρονοσήμανση)	Ελεύθερο	Ελεύθερο	Ελεύθερο
8	OCSP Signing (Υπογραφή OCSP)	Ελεύθερο	Ελεύθερο	Ελεύθερο

7.1.2.6 Σημεία Διανομής ΚΑΠ (CRL Distribution Points)

Στα Πιστοποιητικά Τελικού Χρήστη περιλαμβάνεται η επέκταση CRLDistributionPoints (Σημεία Διανομής ΚΑΠ) η οποία παραπέμπει στο δικτυακό κόμβο (URL) από όπου κάποιος Τρίτος Συμμετέχων μπορεί να λάβει έναν ΚΑΠ ώστε να ελέγξει την κατάσταση ενός Πιστοποιητικού. Το πεδίο κρισιμότητας στην επέκταση αυτή ορίζεται ως ΨΕΥΔΕΣ (FALSE).

7.1.2.7 Προσδιοριστής Κλειδιού Αρχής (Authority Key Identifier)

Η δυνατότητα χρήσης της επέκτασης Authority Key Identifier (Προσδιοριστής Κλειδιού Αρχής) παρέχεται για τα Πιστοποιητικά των εκδοτριών ΑΠ, και των Τελικών Χρηστών.
Η μέθοδος δημιουργίας του keyIdentifier (Προσδιοριστής Κλειδιού) υπολογίζεται τουλάχιστον σύμφωνα με τις μεθόδους που περιγράφονται στο RFC 5280 (ασφαλέστερες μέθοδοι δεν αποκλείονται). Το πεδίο κρισιμότητας στην επέκταση αυτή ορίζεται ως ΨΕΥΔΕΣ (FALSE).

7.1.2.8 Προσδιοριστής Κλειδιού Υποκειμένου (Subject Key Identifier)

Η δυνατότητα χρήσης της επέκτασης Subject Key Identifier (Προσδιοριστής Κλειδιού Υποκειμένου) παρέχεται για το αυτουπογραφόμενο Πιστοποιητικό της ΑΠΕΔ, τα Πιστοποιητικά εκδοτριών ΑΠ, και τα Πιστοποιητικά Τελικών Χρηστών. Η μέθοδος δημιουργίας του keyIdentifier (Προσδιοριστής Κλειδιού) υπολογίζεται τουλάχιστον σύμφωνα με τις μεθόδους που περιγράφονται στο RFC 5280 (ασφαλέστερες μέθοδοι δεν αποκλείονται). Το πεδίο κρισιμότητας στην επέκταση αυτή ορίζεται ως ΨΕΥΔΕΣ (FALSE).

7.1.2.9 Ιδιωτικές Επεκτάσεις Πιστοποιητικού

Τα Πιστοποιητικά υπογραφής και αυθεντικό ποίησης που ακολουθούν την ΠΠ 1, ΠΠ 3, ΠΠ 4 και ΠΠ 5, περιέχουν μια ιδιωτική επέκταση (private extension) η οποία περιέχει ένα Προσδιοριστή Αντικειμένου (OID) που δηλώνει ότι το Πιστοποιητικό εκδίδεται σύμφωνα με την Ευρωπαϊκή Οδηγία 99/93/ΕΚ που έχει ενσωματωθεί στην Ελληνική νομοθεσία με το ΠΔ 150/2001. Αυτή η επέκταση βρίσκεται σε συμφωνία με τον ορισμό της παραγράφου 4.2.1 (2) του "Προφίλ Αναγνωρισμένου Πιστοποιητικού" ("Qualified Certificate Profile") της τεχνικής προδιαγραφής "ETS1101 862" και του κειμένου πολιτικής "ETS1101 456" και μπορεί να χαρακτηριστεί ως κρίσιμη ή μη κρίσιμη.
Επίσης είναι στην επιλογή της ΑΠΕΔ και των εκδοτριών ΑΠ να χρησιμοποιηθούν οι ακόλουθες πρόσθετες ιδιωτικές επεκτάσεις:

- Επέκταση που περιλαμβάνει δήλωση για τυχόν ύπαρξη ορίου στην αξία των συναλλαγών όπου το Πιστοποιητικό μπορεί να χρησιμοποιηθεί σύμφωνα με την παράγραφο 4.2.2 του "Προφίλ Αναγνωρισμένου Πιστοποιητικού" ("Qualified Certificate Profile") της τεχνικής προδιαγραφής "ETS1101 862`.
- Επέκταση που περιλαμβάνει δήλωση για την περίοδο διατήρησης αρχείων σύμφωνα με την §5.5.2 της ΠΠ και την παράγραφο 4.2.3 του "Προφίλ Αναγνωρισμένου Πιστοποιητικού" ("Qualified Certificate Profile") της τεχνικής προδιαγραφής "ETSI 101 862".

7.1.3 Προσδιοριστές Αντικειμένου Αλγορίθμου Υπογραφής (Algorithm Object Identifiers)

Τα Πιστοποιητικά X.509 της ΑΠΕΔ και των εκδοτριών ΑΠ υπογράφονται με shaIRSA (OID: 1.2.840.113549.1.1.5) σύμφωνα με το RFC 3279 ή/και με sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11) σύμφωνα με το RFC 4055.

7.1.4 Μορφές Ονομάτων

Η ΑΠΕΔ και οι εκδότριες ΑΠ αναγράφουν στα Πιστοποιητικά τους το Διακριτικό Όνομα του Εκδότη και του Υποκειμένου σύμφωνα με την §3.1.1 της ΠΠ.

Για πιστοποιητικά που εκδίδονται σύμφωνα με την ΠΠ 5 και ΠΠ 6 στο πεδίο Organization αναγράφεται το όνομα του νομικού προσώπου το οποίο εκπροσωπείται από το φυσικό πρόσωπο, με λατινικούς χαρακτήρες. Επιπρόσθετα, σε πεδίο του τύπου Organization Unit αναγράφεται το ο Αριθμός Φορολογικού Μητρώου του νομικού προσώπου χρησιμοποιώντας το πρόθεμα "AFM-", π.χ. "AFM-123456789".

7.1.5 Προσδιοριστής Αντικειμένου Πολιτικής Πιστοποιητικού (Certificate Policy Object Identifier)

Τα Πιστοποιητικά των Τελικών Χρηστών θα περιλαμβάνουν προσδιοριστή αντικειμένου για την Πολιτική Πιστοποιητικού (Certificate Policy Object Identifier) που θα ακολουθούν, σύμφωνα με την §1.2.5 της ΠΠ. Τα Πιστοποιητικά ΥπΑΠ της ΑΠΕΔ θα περιλαμβάνουν προσδιοριστή αντικειμένου για την πολιτική πιστοποιητικού (Certificate Policy Object Identifier), ήτοι 1.2.300.0.110001.1.7.1.1.

7.1.6 Σύνταξη και Σημασιολογία Περιγραφέων Πολιτικής (Policy Qualifiers Syntax and Semantics)

Τα Πιστοποιητικά X.509 Έκδοσης 3 των εκδοτριών ΑΠ, και των Τελικών Χρηστών θα περιλαμβάνουν, στην επέκταση πολιτικής πιστοποιητικού, ένα περιγραφέα πολιτικής που θα παραπέμπει στη Δήλωση Πρακτικής που κάθε φορά εφαρμόζεται. Βλ. και §7.1.5 της ΠΠ.

7.2 Προφίλ Καταλόγου Ανακληθέντων Πιστοποιητικών (ΚΑΠ)

Η ΑΠΕΔ και οι εκδότριες ΑΠ εκδίδουν ΚΑΠ οι οποίοι είναι σύμφωνοι με το RFC 5280.

Κατ` ελάχιστο, οι εν λόγω ΚΑΠ περιλαμβάνουν τα βασικά πεδία και περιεχόμενα που προσδιορίζονται στον Πίνακα 11:

Πίνακας 11: Βασικά Πεδία Προφίλ ΚΑΠ

Πεδίο	Τιμή ή Περιορισμός Τιμής
Version (Έκδοση)	Βλ. §7.2.1 της ΠΠ.
Signature Algorithm (Αλγόριθμος Υπογραφής)	Αλγόριθμος που χρησιμοποιείται για την υπογραφή του ΚΑΠ. Οι ΚΑΠ της ΑΠΕΔ και των εκδοτριών ΑΠ υπογράφονται με τη χρήση sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) ή md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) σύμφωνα με το RFC 3279 ή με τη χρήση sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11) σύμφωνα με το RFC 4055
Issuer (Εκδότης)	Ο Φορέας που υπογράφει και εκδίδει τον ΚΑΠ. Το Όνομα Εκδότη ΚΑΠ είναι σύμφωνο με τις προδιαγραφές του Διακριτικού Ονόματος Εκδότη που ορίζονται στην §7.1.4 της ΠΠ.
Effective Date (Ημερομηνία Ισχύος)	Ημερομηνία έκδοσης του ΚΑΠ. Οι ΚΑΠ της ΑΠΕΔ, και των εκδοτριών ΑΠ ισχύουν με την έκδοσή τους.
Next Update (Επόμενη Ενημέρωση	Ημερομηνία κατά την οποία θα εκδοθεί ο επόμενος ΚΑΠ. Η συχνότητα έκδοσης ΚΑΠ είναι σύμφωνη με τις προδιαγραφές της §4.9.6 της ΠΠ.
Revoked Certificates (Ανακληθέντα Πιστοποιητικά)	Καταγραφή των ανακληθέντων πιστοποιητικών, περιλαμβανομένων του Αριθμού Σειράς του ανακληθέντος Πιστοποιητικού και της Ημερομηνίας Ανάκλησης.

7.2.1 Αριθμός(-οί) Έκδοσης

Η ΑΠΕΔ και οι εκδότριες ΑΠ εκδίδουν ΚΑΠ X.509Έκ-δοσης 1.

7.3 Προφίλ OCSP

Οι εκδότριες ΑΠ δύναται να παρέχουν υπηρεσίες OCSP (Πρωτόκολλο Κατάστασης Πιστοποιητικών Δικτύου). Τα Συστήματα Απόκρισης (Responders) OCSP συμμορφώνονται προς το πρότυπο RFC2560.

7.3.1 Αριθμός(-οι) Έκδοσης

Οι εκδότριες ΑΠ που παρέχουν υπηρεσίες OCSP, εκδίδουν Πιστοποιητικά Έκδοσης 1, όπως προδιαγράφονται στο RFC2560.

7.3.2 Επεκτάσεις OCSP

Κατ` ελάχιστο, τα Πιστοποιητικά OCSP περιλαμβάνουν τα βασικά πεδία και περιεχόμενα που προσδιορίζονται στον Πίνακα 12:

Πεδίο	Τιμή ή Περιορισμός Τιμής
Version (Έκδοση)	Βλ. ΠΠ §7.1.1
Serial Number (Αριθμός Σειράς)	Μοναδική τιμή ανά Διακριτικό Όνομα Εκδότη (Issuer DN)
Signature Algorithm (Αλγόριθμος Υπογραφής)	Ο αλγόριθμος που χρησιμοποιήθηκε για την υπογραφή του Πιστοποιητικού (Βλ. §7.1.3 της ΠΠ)
Issuer DN (Διακριτικό Όνομα Εκδότη)	Εκδότρια ΑΠ
Valid From (Ισχύει Από)	Βάσει του Universal Coordinate Time. Κωδικοποίηση σύμφωνα με το RFC 5280.
Valid To (Ισχύει Μέχρι)	Έως δέκα (10) έτη (όσο και ο λειτουργικός χρόνος ζωής της εκδότριας ΑΠ)
Subject DN (Διακριτικό Όνομα Υποκειμένου)	Όπως ακριβώς και η εκδότρια ΑΠ με τη διαφοροποίηση της προσθήκης «OCSP Responder» στο τέλος του Common Name
Subject Public Key (Δημόσιο Κλειδί Υποκειμένου)	Κωδικοποιημένο σύμφωνα με το RFC 5280 με τη χρήση αλγορίθμων που προσδιορίζονται στην §7.1.3 της ΠΠ και με μήκη κλειδιών που προσδιορίζονται στην §6.1.5 της ΠΠ.
Signature (Υπογραφή)	Παράγεται και κωδικοποιείται σύμφωνα με το RFC 5280

8. Έλεγχος Συμμόρφωσης και Άλλες Αξιολογήσεις

Για τις υπηρεσίες πιστοποίησης και διαχείρισης κλειδιών που παρέχονται από την ΑΠΕΔ και τις εκδότριες ΑΠ διενεργείται τακτικός εσωτερικός ή εξωτερικός έλεγχος ούτως ώστε να διαπιστώνεται η συμμόρφωση τους προς τις απαιτήσεις της παρούσας ΠΠ, σύμφωνα με τις προδιαγραφές της ΕΕΤΤ. Επιπρόσθετα προς τους ελέγχους συμμόρφωσης, η ΑΠΕΔ έχει δικαίωμα να διενεργεί και άλλες επιθεωρήσεις ή έρευνες ώστε να εξασφαλίσει την αξιοπιστία των υπηρεσιών που παρέχει. Οι επιθεωρήσεις αυτές περιλαμβάνουν ενδεικτικά διενέργεια "Εκτάκτων Ελέγχων" ή "Επιπρόσθετες Επιθεωρήσεις Διαχείρισης Κινδύνου", ιδίως εφόσον προκύψουν ελλείψεις ή ελαττώματα κατά τον Έλεγχο Συμμόρφωσης.

Οι Φορείς και τα νομικά πρόσωπα που υπόκεινται σε έλεγχο, επιθεώρηση ή έρευνα θα πρέπει να συνεργάζονται με την ΑΠΕΔ και το προσωπικό που διενεργεί τον έλεγχο, την επιθεώρηση ή την έρευνα.

8.1 Συχνότητα Ελέγχου Συμμόρφωσης Φορέα

Οι έλεγχοι συμμόρφωσης διενεργούνται σε ετήσια βάση σε συμφωνία με το ελληνικό δίκαιο περί ηλεκτρονικών υπογραφών/Ελεγχοι Συμμόρφωσης δύνανται να πραγματοποιούνται και προτού μια εκδότρια ΑΠ επιθυμεί να διαλειτουργήσει με την ΑΠΕΔ, ή σε συνέχεια ενός περιστατικού ασφαλείας.

Οι δαπάνες για τη διεξαγωγή των Ελέγχων Συμμόρφωσης βαρύνουν αποκλειστικά τον υπό έλεγχο φορέα.

8.2 Ταυτότητα/Προσόντα Ελεγκτή

Οι Έλεγχοι Συμμόρφωσης της ΑΠΕΔ θα διενεργούνται είτε από εξουσιοδοτημένη ομάδα εσωτερικών επιθεωρητών της ΑΠΕΔ είτε από ανεξάρτητη εταιρεία ελέγχου.

Οι επιθεωρήσεις και οι έλεγχοι από ανεξάρτητες εταιρείες ελέγχου θα πραγματοποιούνται από πιστοποιημένες δημόσιες ελεγκτικές εταιρείες, με αποδεδειγμένη εμπειρία σε ζητήματα ασφάλειας υπολογιστών ή από πιστοποιημένους επαγγελματίες στον τομέα της ασφάλειας υπολογιστών υπό την ιδιότητα των υπαλλήλων μίας αρμόδιας επιχείρησης συμβούλων ασφαλείας.

Επιπλέον, οι εν λόγω εταιρείες θα πρέπει να διαθέτουν αποδεδειγμένη εμπειρία στην διενέργεια ελέγχων συμμόρφωσης στους τομείς ασφάλειας πληροφορικών συστημάτων και ΥΔΚ, που θα βασίζεται σε διεθνή και ευρωπαϊκά αποδεκτά πρότυπα (π.χ. μεθοδολογία WebTrust for CAs).

8.3 Σχέση Ελεγκτή με Ελεγχόμενο

Οι εσωτερικοί Έλεγχοι Συμμόρφωσης θα πραγματοποιούνται από εξουσιοδοτημένες ομάδες εσωτερικών επιθεωρητών, τα μέλη των οποίων δεν θα έχουν άμεση σχέση/ρόλο στις παρεχόμενες από την Αρχή Πιστοποίησης υπηρεσίες ΥΔΚ.

Οι εξωτερικοί Έλεγχο ι Συμμόρφωσης θα πραγματοποιούνται από εταιρείες ελέγχου ανεξάρτητες από την υπό έλεγχο νομική οντότητα. Οι εταιρείες αυτές δεν θα έχουν αντικρουόμενα συμφέροντα τα οποία θα παρεμποδίζουν την ικανότητα τους να παράσχουν υπηρεσίες ελέγχου.

8.4 θέματα που Καλύπτει ο Έλεγχος

Αντικείμενο του ελέγχου συμμόρφωσης αποτελούν τα μέτρα ασφάλειας που λαμβάνονται, οι υπηρεσίες διαχείρισης κλειδιών και τα μέτρα ελέγχου της υποδομής δημοσίου κλειδιού, και γενικότερα η συμμόρφωση της υπό επιθεώρηση Αρχής Πιστοποίησης με την παρούσα Πολιτική Πιστοποιητικών και με το ισχύον ελληνικό δίκαιο περί ηλεκτρονικών υπογραφών.

8.5 Λήψη Μέτρων ως Αποτέλεσμα Ανεπάρκειας

Εάν κατά τη διάρκεια του Ελέγχου Συμμόρφωσης αποκαλυφθούν σημαντικές ελλείψεις ή ανεπάρκειες, επιβάλλεται να ληφθούν τα απαιτούμενα μέτρα. Ο προσδιορισμός των μέτρων αυτών θα γίνει από την ΑΠΕΔ ή/και την αρμόδια εκδότρια ΑΠ κατόπιν της εισήγησης του ελεγκτή. Η ΑΠΕΔ ή/και η αρμόδια εκδότρια ΑΠ είναι σε κάθε περίπτωση αρμόδια για την ανάπτυξη και εφαρμογή αυτού του επανορθωτικού σχεδίου δράσης εντός εύλογου χρονικού διαστήματος.

8.6 Επικοινωνία των Αποτελεσμάτων

Μετά από κάθε Έλεγχο Συμμόρφωσης, η υπό έλεγχο οντότητα θα υποβάλλει στην ΑΠΕΔ την αναφορά επιθεώρησης, καθώς και τα αποδεικτικά στοιχεία του ελέγχου ή της αυτοαξιολόγησής της εντός τριάντα (30) ημερών από την ολοκλήρωση του ελέγχου.

9. Άλλα Επιχειρησιακά και Νομικά Ζητήματα

9.1 Τέλη Παροχής Υπηρεσιών Πιστοποίησης

9.1.1 Τέλη Έκδοσης ή Ανανέωσης Πιστοποιητικού

Η ΑΠΕΔ δύναται να χρεώνει τις ΥπΑΠ για την έκδοση, το χειρισμό και την ανανέωση Πιστοποιητικών ΑΠ. Οι εκδότριες ΑΠ δύνανται να χρεώνουν τους τελικούς χρήστες για την έκδοση, το χειρισμό και την ανανέωση Πιστοποιητικών Τελικών Χρηστών.

9.1.2 Τέλη για την Πρόσβαση σε Πιστοποιητικό

Η ΑΠΕΔ και οι εκδότριες ΑΠ δε χρεώνουν τέλη για τη διαθεσιμότητα ενός Πιστοποιητικού σε χώρο αποθήκευσης ή για τη με άλλον τρόπο διαθεσιμότητα Πιστοποιητικών προς Τρίτους Συμμετέχοντες.

9.1.3 Τέλη Πρόσβασης σε Πληροφορίες Ανάκλησης ή Κατάστασης

Η ΑΠΕΔ και οι εκδότριες ΑΠ δεν χρεώνουν τέλη ως προϋπόθεση για τη διαθεσιμότητα πληροφοριών ανάκλησης ή κατάστασης πιστοποιητικών όπως προβλέπεται από στις §4.9.6 και 4.9.8 του παρόντος ή για τη με άλλον τρόπο διαθεσιμότητα ΚΑΠ προς Τρίτους Συμμετέχοντες. Η ΑΠΕΔ και οι ΥπΑΠ δεν επιτρέπουν την πρόσβαση σε πληροφορίες ανάκλησης ή κατάστασης Πιστοποιητικού στο χώρο αποθήκευσης της σε τρίτα πρόσωπα τα οποία παρέχουν προϊόντα ή υπηρεσίες και κάνουν χρήση αυτών των πληροφοριών χωρίς την προηγούμενη ρητή συγκατάθεση της.

9.1.4 Τέλη για Άλλες Υπηρεσίες

Η ΑΠΕΔ δε χρεώνει τέλη για την πρόσβαση στην παρούσα πράξη. Οποιαδήποτε χρήση γίνεται για σκοπούς διαφορετικούς από την απλή ανάγνωση αυτών των εγγράφων, όπως είναι η αναπαραγωγή, αναδιανομή, τροποποίηση ή δημιουργία αντιγράφων απαιτεί προηγούμενη αίτηση, σύμφωνα με όσα προβλέπονται στο άρθρο 5 του Νόμου 3448/2006, προς την ΑΠΕΔ, η οποία κατέχει και τα δικαιώματα πνευματικής ιδιοκτησίας.

9.1.5 Πολιτική Επιστροφής Χρημάτων

Όταν οι εκδότριες ΑΠ επιβάλλουν τέλη έκδοσης ή ανανέωσης Πιστοποιητικών, περιγράφουν στην Δήλωση Πρακτικής τους την Πολιτική Επιστροφής Χρημάτων που εφαρμόζουν.

9.2 Χρηματοοικονομικές Ευθύνες

9.2.1 Ασφαλιστική Κάλυψη

Όταν οι εκδότριες ΑΠ αποτελούν νομικά πρόσωπα ιδιωτικού δικαίου, τότε διαθέτουν ασφαλιστική κάλυψη έναντι σφαλμάτων και παραλείψεων, είτε μέσω ασφαλιστικού προγράμματος αστικής ευθύνης που παρέχεται από ασφαλιστική εταιρεία είτε μέσω αποθεματικού αυτασφάλισης.

9.2.2 Άλλα Περιουσιακά Στοιχεία

Όταν οι εκδότριες ΑΠ αποτελούν νομικά πρόσωπα ιδιωτικού δικαίου, διαθέτουν επαρκείς οικονομικούς πόρους για να διασφαλίσουν τη συνεχή παροχή των υπηρεσιών τους, ενώ σε εύλογα πλαίσια βρίσκονται σε θέση να αναλάβουν κίνδυνο ευθύνης προς τους Τελικούς τους Χρήστες.

9.2.3 Ασφαλιστική Κάλυψη ή Εγγύηση για Τελικούς Χρήστες

Οι εκδότριες ΑΠ που προσφέρουν προγράμματα εγγυητικής κάλυψης προς τους Τελικούς Χρήστες υποχρεούνται να περιλαμβάνουν πληροφορίες σχετικά με τα προγράμματα αυτά στη Δήλωση Πρακτικής τους.

9.3 Εμπιστευτικότητα Πληροφοριών

9.3.1 Κατηγορίες Πληροφοριών που Θεωρούνται Εμπιστευτικές

Εν προκειμένω εφαρμόζονται οι διατάξεις για την προστασία των προσωπικών δεδομένων, του απορρήτου των επικοινωνιών και κάθε άλλη σχετική διάταξη.
Συγκεκριμένα, τα παρακάτω αρχεία θεωρούνται εμπιστευτικά:

- Αρχεία της ΑΠ σχετικά με αιτήσεις, είτε εγκεκριμένες είτε απορριφθείσες.
- Αρχεία Αιτήσεων για Πιστοποιητικό.
- Ιδιωτικά κλειδιά που τηρούνται από εκδότριες ΑΠ που προσφέρουν υπηρεσίες αρχειοθέτησης ιδιωτικών κλειδιών για την ΠΠ 2 και την ΠΠ 6, καθώς και οι πληροφορίες που είναι απαραίτητες για την ανάκτηση αυτών των Ιδιωτικών Κλειδιών.
- Αρχεία ελέγχου της ΑΠΕΔ και των εκδοτριών ΑΠ.
- Σχεδιασμός πρόληψης απρόοπτων καταστάσεων και σχέδια αποκατάστασης καταστροφών.
- Μέτρα ασφαλείας που ελέγχουν τις λειτουργίες του εξοπλισμού και του λογισμικού της ΑΠΕΔ και των εκδοτριών ΑΠ.

9.3.2 Κατηγορίες Πληροφοριών που Δε Θεωρούνται Εμπιστευτικές

Τα Πιστοποιητικά, η ανάκληση ή άλλες πληροφορίες σχετικές με την κατάσταση Πιστοποιητικών, οι διαδικτυακοί χώροι πληροφοριών της ΑΠΕΔ και των εκδοτριών ΑΠ, καθώς και οι πληροφορίες που περιλαμβάνονται σε αυτούς δε θεωρούνται Εμπιστευτικές Πληροφορίες.

9.3.3 Ευθύνη για την Προστασία Εμπιστευτικών Πληροφοριών

Οι Συμμετέχοντες στην ΥΔΚ της ΑΠΕΔ και των εκδοτριών ΑΠ, οι οποίοι λαμβάνουν γνώση Εμπιστευτικών Πληροφοριών, μεριμνούν ούτως ώστε να μην εκτεθούν σε κίνδυνο και να μην αποκαλυφθούν σε τρίτα μέρη.

9.4 Προστασία Δεδομένων Προσωπικού Χαρακτήρα

Η Υποδομή Δημοσίου Κλειδιού όπως προβλέπεται στον παρόντα κανονισμό υπόκειται στην νομοθεσία περί προστασίας των δεδομένων προσωπικού χαρακτήρα.

9.4.1 Πολιτική Προστασίας της Ιδιωτικότητας

Η ΑΠΕΔ και οι εκδότριες ΑΠ εφαρμόζουν πολιτική για την προστασία δεδομένων προσωπικού χαρακτήρα σύμφωνα με τις διατάξεις για την προστασία των προσωπικών δεδομένων, του απορρήτου των επικοινωνιών και κάθε άλλη σχετική διάταξη. Η ΑΠΕΔ και οι εκδότριες ΑΠ δεν αποκαλύπτουν, ούτε εκμεταλλεύονται τα ονόματα των Τελικών Χρηστών ή άλλα προσωπικά τους στοιχεία, σύμφωνα με την §9.3.3.

9.4.2 Πληροφορίες που Αντιμετωπίζονται ως Προσωπικά Δεδομένα

Εφαρμόζεται εν προκειμένω η νομοθεσία για την προστασία των προσωπικών δεδομένων.

9.4.3 Ευθύνη για την Προστασία Δεδομένων Προσωπικού Χαρακτήρα

Οι Συμμετέχοντες στην ΥΔΚ της ΑΠΕΔ και των εκδοτριών ΑΠ, οι οποίοι λαμβάνουν γνώση Δεδομένων Προσωπικού Χαρακτήρα, μεριμνούν ούτως ώστε να μην εκτεθούν σε κίνδυνο και να μην αποκαλυφθούν σε τρίτα μέρη και συμμορφώνονται με την εφαρμοστέα νομοθεσία περί προστασίας προσωπικών δεδομένων.

9.4.4 Ενημέρωση και Συγκατάθεση του Υποκειμένου για την Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα

Ισχύουν όσα προβλέπονται στην κείμενη νομοθεσία για την προστασία δεδομένων προσωπικού χαρακτήρα

9.4.5 Αποκάλυψη κατόπιν Δικαστικών ή Διοικητικών Διαδικασιών

Η ΑΠΕΔ και οι εκδότριες ΑΠ αποκαλύπτουν Εμπιστευτικές Πληροφορίες και Δεδομένα Προσωπικού Χαρακτήρα μόνο σε συμμόρφωση με το σχετικό νομοθετικό πλαίσιο. Τα ιδιωτικά κλειδιά των Πιστοποιητικών υπογραφής τελικών χρηστών που ακολουθούν την ΠΠ 1, ΠΠ 3, ΠΠ 4 και την ΠΠ 5, δεν αποκαλύπτονται ποτέ σε τρίτο, συμπεριλαμβανομένης και της ΑΠΕΔ.

9.5 Δικαιώματα Πνευματικής Ιδιοκτησίας

9.5.1 Δικαιώματα Πνευματικής Ιδιοκτησίας στα Πιστοποιητικά και Πληροφορίες Ανάκλησης

Η ΑΠΕΔ και αντίστοιχα οι εκδότριες ΑΠ διατηρούν όλα τα δικαιώματα πνευματικής ιδιοκτησίας για τα Πιστοποιητικά και τις πληροφορίες ανάκλησης που εκδίδουν.

Η ΑΠΕΔ και αντίστοιχα οι εκδότριες ΑΠ εκχωρούν μη αποκλειστική, χωρίς χρέωση άδεια αναπαραγωγής και διανομής των Πιστοποιητικών που εκδίδουν εφόσον αυτά αναπαράγονται πλήρως και εφόσον η χρήση τους υπόκειται στους ΟΤΣ. Η ΑΠΕΔ και αντίστοιχα οι εκδότριες ΑΠ χορηγούν πληροφορίες ανάκλησης σε κάθε Τρίτο Συμμετέχοντα σύμφωνα με τους ισχύοντες ΟΤΣ.

9.5.2 Δικαιώματα Ιδιοκτησίας επί των Κλειδιών και του Υλικού Κλειδιών

Σε όλες τις περιπτώσεις, τα δημόσια κλειδιά των τελικών χρηστών αποτελούν πνευματική ιδιοκτησία των εκδοτριών ΑΠ που εκδίδουν τα Πιστοποιητικά.

9.5.3 Διαδικασίες για την προστασία Τελικών Χρηστών ή Τρίτων Συμμετεχόντων

Η ΑΠΕΔ διασφαλίζει τον Τελικό Χρήστη ή Τρίτο Συμμετέχοντα από αστοχίες της Υποδομής Δημοσίου Κλειδιού βάσει των διατάξεων του παρόντος.

9.6 Δηλώσεις και Εγγυήσεις

9.6.1 Δηλώσεις και Εγγυήσεις ΑΠ

Η ΑΠΕΔ και οι ΥπΑΠ εγγυώνται στους Τελικούς Χρήστες και στους Τρίτους Συμμετέχοντες, κατ` ελάχιστον ότι:

- Δεν υπάρχει καμία αναφορά ψευδών στοιχείων στο Πιστοποιητικό η οποία να είναι γνωστή ή να οφείλεται σε υπαιτιότητα των οντοτήτων τα οποία εγκρίνουν την Αίτηση για Πιστοποιητικό ή εκδίδουν το Πιστοποιητικό.
- Δεν υπάρχουν λάθη στα στοιχεία του Πιστοποιητικού τα οποία να προκλήθηκαν από τις ΑΕ που ενέκριναν την Αίτηση για Πιστοποιητικό ή από τις ΑΠ που εξέδωσαν το Πιστοποιητικό ως αποτέλεσμα αποτυχίας να επιδείξουν τη μέγιστη επιμέλεια κατά το χειρισμό της Αίτησης για Πιστοποιητικό ή τη δημιουργία του Πιστοποιητικού.
- Τα Πιστοποιητικά τους πληρούν όλες τις ουσιαστικές απαιτήσεις της παρούσας ΠΠ και της εκάστοτε εφαρμοστέας Δήλωσης Πρακτικής, όπως επίσης και οι υπηρεσίες ανάκλησης και η χρήση του χώρου πληροφοριών.

Οι τρίτοι φορείς - Πάροχοι Υπηρεσιών Πιστοποίησης θα πρέπει στο πλαίσιο της συμμόρφωσης τους με την παρούσα ΠΠ να εγγυώνται στους Τελικούς Χρήστες και στους Τρίτους Συμμετέχοντες όλα τα παραπάνω.

9.6.2 Δηλώσεις και Εγγυήσεις ΑΕ

Οι ΑΕ των ΥπΑΠ εγγυώνται στους Τελικούς Χρήστες και στους Τρίτους
Συμμετέχοντες, κατ` ελάχιστον ότι:

- Δεν υπάρχει καμία αναφορά ψευδών στοιχείων στο Πιστοποιητικό η οποία να είναι γνωστή ή να οφείλεται σε υπαιτιότητα των ίδιων.
- Δεν υπάρχουν λάθη στα στοιχεία του Πιστοποιητικού τα οποία προκλήθηκαν από τις οντότητες που ενέκριναν την Αίτηση για Πιστοποιητικό ως αποτέλεσμα αποτυχίας να επιδείξουν εύλογη μέριμνα κατά το χειρισμό της Αίτησης για Πιστοποιητικό.
- Τα Πιστοποιητικά τους πληρούν όλες τις ουσιαστικές απαιτήσεις της παρούσας ΠΠ και της εφαρμοστέας Δήλωσης Πρακτικής, όπως επίσης και οι υπηρεσίες ανάκλησης και η χρήση του χώρου πληροφοριών.

Οι ΑΕ των τρίτων φορέων - Παροχών Υπηρεσιών Πιστοποίησης θα πρέπει στο πλαίσιο της συμμόρφωσης τους με την παρούσα ΠΠ να εγγυώνται στους Τελικούς Χρήστες και στους Τρίτους Συμμετέχοντες όλα τα παραπάνω.

9.6.3 Δηλώσεις και Εγγυήσεις του Τελικού Χρήστη

Οι Τελικοί Χρήστες εγγυώνται, κατ` ελάχιστον ότι:

- Κάθε ψηφιακή υπογραφή που δημιουργείται χρησιμοποιώντας το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που αναγράφεται στο Πιστοποιητικό, αποτελεί την ψηφιακή υπογραφή του Τελικού Χρήστη, ενώ το Πιστοποιητικό έχει γίνει αποδεκτό και είναι σε ισχύ (δεν έχει λήξει ή ανακληθεί) κατά το χρόνο δημιουργίας αυτής της ψηφιακής υπογραφής.
- Το ιδιωτικό τους κλειδί προστατεύεται και κανένα μη εξουσιοδοτημένο πρόσωπο δεν είχε ποτέ πρόσβαση σε αυτό.
- Όλες οι παραδοχές και τα στοιχεία του Τελικού Χρήστη στην Αίτηση για Πιστοποιητικό την οποία έχει υποβάλλει είναι αληθή.
- Όλες οι πληροφορίες που παρέχονται από τον Τελικό Χρήστη είναι αληθείς.
- Το Πιστοποιητικό χρησιμοποιείται αποκλειστικά για εγκεκριμένους και σύννομους σκοπούς, σύμφωνα με όλες τις απαιτήσεις της παρούσας ΠΠ και της εκάστοτε εφαρμοστέας Δήλωσης Πρακτικής.
- Ο Τελικός Χρήστης δεν αποτελεί ΑΠ, και επομένως δεν χρησιμοποιείτο ιδιωτικό του κλειδί που αντιστοιχεί στο δημόσιο κλειδί που αναγράφεται στο Πιστοποιητικό για να υπογράψει ψηφιακά οποιοδήποτε Πιστοποιητικό (ή οποιαδήποτε άλλη μορφή πιστοποιημένου δημόσιου κλειδιού) ή ΚΑΠ, ως ΑΠ ή με άλλη ιδιότητα.

9.6.4 Δηλώσεις και Εγγυήσεις Τρίτου Συμμετέχοντα

Οι Όροι Τρίτου Συμμετέχοντα απαιτούν από τους τελευταίους τη διαβεβαίωση ότι διαθέτουν επαρκείς πληροφορίες για να αποφασίσουν σε ποιο βαθμό θα βασιστούν στις πληροφορίες που αναγράφονται στο Πιστοποιητικό, ότι είναι αποκλειστικά υπεύθυνοι για το εάν θα βασιστούν ή όχι στις πληροφορίες αυτές και ότι θα υποστούν τις νόμιμες συνέπειες από την αποτυχία τους να εκπληρώσουν τις υποχρεώσεις του Τρίτου Συμμετέχοντα σύμφωνα με την παρούσα ΠΠ.

9.7 Αποποιήσεις Εγγυήσεων

Στην έκταση που επιτρέπεται από την ισχύουσα νομοθεσία, οι ΟΧΠ και οι ΟΤΣ των εκδοτριών ΑΠ, μπορούν να περιέχουν αποποίηση των πιθανών εγγυήσεων τους, περιλαμβανομένων κάθε είδους εγγυήσεων ως προς την εμπορευσιμότητα ή καταλληλότητα για συγκεκριμένο σκοπό.

9.8 Περιορισμοί Ευθύνης

Οι Δηλώσεις Πρακτικής, οι ΟΧΠ και οι ΟΤΣ των εκδοτριών ΑΠ δύνανται, μετά από έγκριση της ΑΠΕΔ, να περιορίζουν την ευθύνη τους περιλαμβάνοντας τον αποκλεισμό έμμεσων, εξαιρετικών, θετικών, τυχαίων, συνεπαγόμενων και αποθετικών ζημιών.

9.9 Διάρκεια Ισχύος και Τερματισμός

9.9.1 Έναρξη Ισχύος

Η ισχύς της παρούσας ΠΠ της ΑΠΕΔ, άρχεται με την δημοσίευση της στο Φύλλο της Εφημερίδας της Κυβέρνησης. Κατόπιν, η παρούσα ΠΠ δημοσιεύεται άμεσα στον δικτυακό αποθηκευτικό χώρο της ΑΠΕΔ.

9.9.2 Λήξη Ισχύος

Η παρούσα ΠΠ θα παραμείνει εν ισχύ έως την αντικατάσταση της από τυχόν νέα, τροποποιημένη έκδοση, σύμφωνα με τα αναφερόμενα στην παρ. §9.11 της παρούσας.

9.9.3 Συνέπειες Λήξης Ισχύος

Με την κατάργηση της παρούσας ΠΠ, οι ΥπΑΠ, οι Τελικοί Χρήστες και οι Τρίτοι Συμμετέχοντες της Υποδομής Δημοσίου Κλειδιού της ΑΠΕΔ, εξακολουθούν να δεσμεύονται από τους όρους της, ως προς όλα τα πιστοποιητικά που έχουν εκδοθεί κατά τη διάρκεια ισχύος της παρούσας, και για το υπόλοιπο της περιόδου ισχύος τους.

9.10 Ειδοποίηση Προσώπων και Επικοινωνία με τους Συμμετέχοντες

Η ΑΠΕΔ και οι ΥπΑΠ, οφείλουν να χρησιμοποιούν εύλογες μεθόδους για την μεταξύ τους επικοινωνία καθώς και την επικοινωνία με τους Τελικούς Χρήστες και τους Τρίτους Συμμετέχοντες, όταν αυτό απαιτείται, λαμβάνοντας υπόψη την κρισιμότητα και το σκοπό της επικοινωνίας-ενημέρωσης.

9.11 Τροποποιήσεις

Τροποποιήσεις της παρούσας ΠΠ επιτρέπονται ύστερα από πρόταση της ΑΠΕΔ. Οι τροποποιήσεις θα είναι είτε υπό μορφή εγγράφου που περιέχει τις τροποποιήσεις της ΠΠ ή με νέα έκδοση της ΠΠ. Οι τροποποιημένες ή νέες εκδόσεις παρατίθενται στο τμήμα του Χώρου Αποθήκευσης της ΑΠΕΔ για Ενημερώσεις και Ανακοινώσεις επί των Κανονισμών στις διευθύνσεις: http://www. yap.gov.gr, http://www.ermis.gov.gr, και http://www.syzefxis.gov.gr. Οι νέες εκδόσεις της ΠΠ υπερισχύουν έναντι οποιωνδήποτε προηγούμενων.

9.11.1 Στοιχεία που Μπορούν να Τροποποιηθούν Χωρίς Προειδοποίηση

Η ΑΠΕΔ δύναται να προτείνει τροποποιήσεις του παρόντος χωρίς προειδοποίηση των Τελικών Χρηστών και Τρίτων Συμμετεχόντων, για μεταβολές που δεν είναι ουσιώδους σημασίας, περιλαμβανομένων ενδεικτικά, διορθώσεων τυπογραφικών λαθών, αλλαγών των δικτυακών κόμβων (URL) και μεταβολών των στοιχείων επικοινωνίας.

9.11.2 Στοιχεία που Μπορούν να Τροποποιηθούν Με Προειδοποίηση

Η ΑΠΕΔ δύναται να προβεί σε ουσιώδεις τροποποιήσεις της ΠΠ ύστερα από προειδοποίηση των Τελικών Χρηστών τουλάχιστον με σχετική ανακοίνωση στον Χώρο Αποθήκευσης της που προορίζεται για Ενημερώσεις και Ανακοινώσεις επί των Κανονισμών στις διευθύνσεις: http://www.yap.gov.gr, http://www.ermis.gov.gr, και http://www.syzefxis.gov.gr.

9.11.3 Ανακοίνωση Τροποποιήσεων

Η ΑΠΕΔ ανακοινώνει τις τροποποιήσεις της ΠΠ στο τμήμα του Χώρου Αποθήκευσης της που προορίζεται για Ενημερώσεις και Ανακοινώσεις επί των Κανονισμών, στις διευθύνσεις: http://www.yap.gov.gr, http://www.ermis. gov.gr, και http://www.syzefxis.gov.gr.

9.12 Πολιτική Δημοσίευσης και Κοινοποίησης

9.12.1 Στοιχεία που δεν δημοσιεύονται στην ΠΠ

Τα έγγραφα ασφαλείας που θεωρούνται εμπιστευτικά από την ΑΠΕΔ ή/και τις εκδότριες ΑΠ δεν αποκαλύπτονται σε τρίτους.

9.12.2 Δημοσίευση της ΠΠ

Η παρούσα ΠΠ δημοσιεύεται σε ηλεκτρονική μορφή στο Χώρο Αποθήκευσης της ΑΠΕΔ στη διεύθυνση http:// www.yap.gov.gr όπου βρίσκεται διαθέσιμος σε μορφή εγγράφου Adobe Acrobat® pdf ή/και Microsoft Word® ή HTML. Η ΑΠΕΔ επίσης διαθέτει την ΠΠ σε μορφή Adobe Acrobat® pdf ή Microsoft Word® στις διευθύνσεις http:// www.ermis.gov.gr, και http://www.syzefxis.gov.gr.

9.13 Επίλυση Διαφορών

Διαφορές ανάμεσα στην ΑΠΕΔ, τις εκδότριες ΑΠ, τους Τελικούς Χρήστες και Τρίτους Συμμετέχοντες θα επιλύονται σύμφωνα με την ισχύουσα νομοθεσία που διέπει τη σχέση μεταξύ των μερών, ανάλογα με την ιδιότητα τους (πολίτες, ιδιωτικές επιχειρήσεις, φορείς δημοσίου και ιδιωτικού τομέα).

9.14 Εφαρμοστέο Δίκαιο

Η ερμηνεία, η εγκυρότητα, η ισχύς και η εφαρμογή της παρούσας ΠΠ διέπεται από την κοινοτική και την κείμενη ελληνική νομοθεσία.

9.15 Ανωτέρα Βία

Η ΑΠΕΔ καθώς και οι ΥπΑΠ δεν ευθύνονται για περιπτώσεις καταστροφής που οφείλονται σε λόγους ανωτέρας βίας.

Β. Δήλωση Πρακτικής των Υποκείμενων Αρχών Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΠΠ 1 - ΠΠ 4)

1. Εισαγωγή

Η παρούσα Δήλωση Πρακτικής των Υποκείμενων Αρχών Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ), εφεξής ΥπΑΠ, εξειδικεύει την Πολιτική Πιστοποίησης της ΑΠΕΔ για συγκεκριμένες πολιτικές πιστοποιητικών (§1.2.1), και ειδικότερα τους όρους και τις προϋποθέσεις καθώς και τις τεχνικές προδιαγραφές για την έγκριση, έκδοση, χειρισμό, χρήση, ανάκληση και ανανέωση των ψηφιακών πιστοποιητικών τελικών χρηστών σύμφωνα με τις διατάξεις της παραγράφου 2 του Άρθρου 20 του Νόμου 3448/2006 (ΦΕΚ 57/Α).
Η παρούσα δήλωση πρακτικής εφαρμόζει και υλοποιεί την Πολιτική Πιστοποίησης της ΑΠΕΔ εκτός και αν από τις διατάξεις της παρούσας ορίζεται διαφορετικά.

1.1 Περίληψη

Η παρούσα Δήλωση Πρακτικής (ΔΠ) καθορίζει:

- Τις υποχρεώσεις των ΥπΑΠ, των Αρχών Εγγραφής (Registration Authorities), των Τελικών Χρηστών και των Τρίτων Συμμετεχόντων.
- Τα θέματα που αφορούν στους Όρους Χρήσης Πιστοποιητικών (ΟΧΠ) Τελικού Χρήστη και τους Όρους Τρίτων Συμμετεχόντων (ΟΤΣ).
- Τις μεθόδους που χρησιμοποιούνται για την επιβεβαίωση της ταυτότητας των Τελικών Χρηστών.
- Τις λειτουργικές διαδικασίες ως προς τις υπηρεσίες κύκλου ζωής Πιστοποιητικού: υποβολή αιτήματος για έκδοση, αποδοχή, ανάκληση και ανανέωση Πιστοποιητικού.
- Το περιεχόμενο των Πιστοποιητικών, των Καταλόγων Ανακληθέντων Πιστοποιητικών (ΚΑΠ), και των Πιστοποιητικών της υπηρεσίας δικτυακού ελέγχου κατάστασης πιστοποιητικών σε πραγματικό χρόνο (Online Certificate Status Protocol - OCSP), όταν διατίθεται
- Τις λειτουργικές διαδικασίες ασφάλειας ως προς την καταγραφή στοιχείων ελέγχου, την τήρηση αρχείων και την αποκατάσταση καταστροφών.
- Τους κανονισμούς φυσικής ασφάλειας, ασφάλειας προσωπικού, διαχείρισης κλειδιών και λογικής ασφάλειας.
- Τη διαχείριση της ΔΠ, συμπεριλαμβανομένων των μεθόδων τροποποίησης της.

Ο Πίνακας 1 περιλαμβάνει τον κατάλογο των προς δημοσίευση εγγράφων των ΥπΑΠ, καθώς και των τοποθεσιών δημοσίευσης αυτών. Τα έγγραφα που δε διατίθενται προς δημοσίευση αποτελούν εμπιστευτικό υλικό της ΑΠΕΔ.

Πίνακας 1: Διαθέσιμα Έγγραφα Κανονισμών

Έγγραφα	Κατάσταση	Τοποθεσία Δημοσίευσης για το Κοινό
Πολιτική Πιστοποιητικών της ΑΠΕΔ	Δημόσιο	Χώρος Αποθήκευσης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου, σύμφωνα με την §2.2 της ΠΠ της ΑΠΕΔ
Όροι Χρήσης Πιστοποιητικών (ΟΧΠ) Τελικών Χρηστών και Όροι Τρίτου Συμμετέχοντα (ΟΤΣ)	Δημόσιο	Χώρος Αποθήκευσης των ΥπΑΠ, σύμφωνα με την §2.2 της παρούσας ΔΠ
Δήλωση Πρακτικής των ΥπΑΠ	Δημόσιο	Χώρος Αποθήκευσης των ΥπΑΠ, σύμφωνα με την §2.2 της παρούσας ΔΠ

1.2 Όνομα και Ταυτότητα Εγγράφου

Οι ΥπΑΠ έχουν προσαρμόσει την παρούσα ΔΠ στο πρότυπο Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (Πλαίσιο Πολιτικής Πιστοποιητικού Υποδομής Δημόσιου Κλειδιού και Κανονισμών Πιστοποίησης X.509 για το Διαδίκτυο), γνωστό και ως RFC 3647, της Ομάδας Δράσης για την Διαδικτυακή Μηχανική (Internet Engineering Task Force), φορέας ο οποίος είναι υπεύθυνος για τον καθορισμό προτύπων στο Διαδίκτυο, για να διευκολύνει την απεικόνιση της εφαρμοζόμενης πολιτικής πιστοποιητικού. Μικρές αποκλίσεις από την δομή του RFC 3647 σε επιμέρους λεπτομέρειες, είναι απαραίτητες εξαιτίας της εφαρμογής του λειτουργικού μοντέλου της ΑΠ στο δημόσιο τομέα.

1.2.1 Προσφερόμενες Υπηρεσίες των ΥπΑΠ

Οι ΥπΑΠ που εφαρμόζουν την παρούσα ΔΠ διαχειρίζονται τον κύκλο ζωής των ψηφιακών πιστοποιητικών τελικών χρηστών (έκδοση, ανάκληση, αναστολή και ανανέωση) σύμφωνα με την ΠΠ 1, ΠΠ 2, ΠΠ 3, και ΠΠ 4 της Πολιτικής Πιστοποίησης της ΑΠΕΔ.

1.2.2 Τιμές Προσδιοριστή Αντικειμένου

Τα Πιστοποιητικά που εκδίδονται από τις ΥπΑΠ σύμφωνα με την παρούσα ΔΠ περιλαμβάνουν τιμές προσδιοριστή αντικειμένου (Object Identifier) που αντιστοιχούν στην εκάστοτε πολιτική πιστοποιητικού που ακολουθείται. Η τιμή προσδιοριστή αντικειμένου για την:

- ΠΠ 1 είναι: 1.2.300.0.110001.1.7.1.1.1
- ΠΠ 2 είναι: 1.2.300.0.110001.1.7.1.1.2
- ΠΠ 3 είναι: 1.2.300.0.110001.1.7.1.1.3
- ΠΠ 4 είναι: 1.2.300.0.110001.1.7.1.1.4

1.3 Συμμετέχοντες στην Υποδομή Δημοσίου Κλειδιού

Σύμφωνα με τα προβλεπόμενα στην §1.3 της ΠΠ της ΑΠΕΔ.

1.4 Εφαρμογή των Πιστοποιητικών

Σύμφωνα με τα προβλεπόμενα στην §1.4 της ΠΠ της ΑΠΕΔ.
Επιπρόσθετα, πιστοποιητικά τα οποία εκδίδονται σε φυσικά πρόσωπα (όπως πολιτικοί προϊστάμενοι και δημόσιοι υπάλληλοι) στο πλαίσιο της άσκησης των καθηκόντων τους για την εξυπηρέτηση των αναγκών φορέα του δημοσίου, αποτελούν και πιστοποιητικά γενικής χρήσης και μπορούν να χρησιμοποιηθούν από τον
Τελικό Χρήστη στις ιδιωτικές τους συναλλαγές με φορείς οι οποίοι τα αποδέχονται.

1.5 Διαχείριση Δήλωσης Πρακτικής

1.5.1 Οργανισμός που διαχειρίζεται το έγγραφο

Την παρούσα ΔΠ εκδίδει η Αρχή Πιστοποίησης του Ελληνικού Δημοσίου σύμφωνα με τις διατάξεις της παραγράφου 2 του άρθρου 1 του Ν 3448/2006 (ΦΕΚ 57/Α). Τυχόν αιτήματα για διευκρινίσεις επί των κεφαλαίων του παρόντος θα απευθύνονται προς την Αρχή Πιστοποίησης του Ελληνικού Δημοσίου.

1.5.2 Στοιχεία επικοινωνίας

Τα στοιχεία επικοινωνίας για τις ΥπΑΠ δημοσιεύονται στις παρακάτω ιστοσελίδες:

- http://www.ermis.gov.gr
- http://www.yap.gov.gr
- http://www.syzefxis.gov.gr

1.6 Ορισμοί και ακρωνύμια

Στο Παράρτημα Α παρατίθεται Πίνακας Ορισμών και Ακρωνυμίων.

2. Δημοσίευση και Χώρος Αποθήκευσης

2.1 Χώροι Αποθήκευσης

Σύμφωνα με τα προβλεπόμενα στην §2.1 της ΠΠ της ΑΠΕΔ.

2.2 Δημοσίευση Πληροφοριών

Σύμφωνα με τα προβλεπόμενα στην §2.2 της ΠΠ της ΑΠΕΔ.

2.2.1 Δημοσίευση της ΔΠ

Η παρούσα ΔΠ δημοσιεύεται σε ηλεκτρονική μορφή στις διευθύνσεις https://pki.ermis.gov.gr/repository. html, http://www.yap.gov.gr, και http://www.syzefxis.gov.gr όπου βρίσκεται διαθέσιμη σε μορφή εγγράφου Adobe Acrobat® pdf ή/και Microsoft Word®ή HTML.

2.2.2 Στοιχεία που δε δημοσιεύονται στη ΔΠ

Τα έγγραφα ασφαλείας που θεωρούνται εμπιστευτικά από τις ΥπΑΠ δεν αποκαλύπτονται σε τρίτους.

2.3 Χρόνος ή Συχνότητα Δημοσίευσης

Οι ΥπΑΠ ανακοινώνουν τις τροποποιήσεις της ΔΠ, μέσα σε εύλογο χρονικό διάστημα στο Χώρο Αποθήκευσης τους, στις διευθύνσεις που αναφέρονται στην ενότητα §2.2.1.
Τα Πιστοποιητικά Τελικών Χρηστών δημοσιεύονται κατά την έκδοση. Πληροφορίες αναφορικά με την κατάσταση Πιστοποιητικών δημοσιεύονται σύμφωνα με τις §4.9.6 και §4.9.8 της ΔΠ.

2.4 Έλεγχοι Πρόσβασης σε Χώρους Αποθήκευσης

Σύμφωνα με τα προβλεπόμενα στην §2.4 της ΠΠ της ΑΠΕΔ.

3. Αναγνώριση και Ταυτοποίηση

3.1 Ονοματοδοσία

Σύμφωνα με τα προβλεπόμενα στην §3.1 της ΠΠ της ΑΠΕΔ.

3.1.1 Τύποι Ονομάτων

Σύμφωνα με τα προβλεπόμενα στην §3.1.1 της ΠΠ της ΑΠΕΔ.
Ειδικότερα, τα πιστοποιητικά τα οποία εκδίδονται σε φυσικά πρόσωπα (όπως πολιτικοί προϊστάμενοι και δημόσιοι υπάλληλοι) στο πλαίσιο της άσκησης των καθηκόντων τους για την εξυπηρέτηση των αναγκών φορέα του δημοσίου, και μόνο αυτά, αναγράφουν στα πεδία Organization (O) και, προαιρετικά, Organization Unit (OU), στοιχεία του φορέα ανάγκες του οποίου εξυπηρετεί ο Τελικός Χρήστης.

3.1.2 Ανάγκη Κατανόησης των Ονομάτων

Σύμφωνα με τα προβλεπόμενα στην §3.1.2 της ΠΠ της ΑΠΕΔ.

3.1.3 Ανωνυμία ή ψευδωνυμία τελικού χρήστη

Οι ΥπΑΠ δεν εκδίδουν πιστοποιητικά όπου στα στοιχεία του Τελικού Χρήστη αναγράφεται ψευδώνυμο.

3.1.4 Μοναδικότητα των Ονομάτων

Σύμφωνα με τα προβλεπόμενα στην §3.1.4 της ΠΠ της ΑΠΕΔ. Επιπρόσθετα, η μοναδικότητα του Διακριτικού Ονόματος του Υποκειμένου εξασφαλίζεται και από τη μοναδικότητα του Κωδικού Διαχείρισης Πιστοποιητικού.

3.1.5 Αναγνώριση και Αυθεντικοποίηση

Σύμφωνα με τα προβλεπόμενα στην §3.1.5 της ΠΠ της ΑΠΕΔ.

3.2 Αρχική Εγγραφή

3.2.1 Μέθοδος Απόδειξης της Κατοχής Ιδιωτικού Κλειδιού

Σύμφωνα με τα προβλεπόμενα στην §3.2.1 της ΠΠ της ΑΠΕΔ.

3.2.2 Μέθοδος Απόδειξης της Ταυτότητας Φυσικού Προσώπου

Σύμφωνα με τα προβλεπόμενα στην §3.2.3 της ΠΠ της ΑΠΕΔ.
Επιπρόσθετα, για πιστοποιητικά τα οποία εκδίδονται σε φυσικά πρόσωπα (όπως πολιτικοί προϊστάμενοι και δημόσιοι υπάλληλοι) στο πλαίσιο της άσκησης των καθηκόντων τους για την εξυπηρέτηση των αναγκών φορέα του

δημοσίου, το φυσικό πρόσωπο θα πρέπει να υποβάλλει σχετικό έγγραφο που να αποδεικνύει τη σχέση εργασίας του με το φορέα ανάγκες του οποίου εξυπηρετεί.

3.2.3 Πληροφορίες Τελικού Χρήστη που Δεν Επαληθεύονται

Σύμφωνα με τα προβλεπόμενα στην §3.2.4 της ΠΠ της ΑΠΕΔ.

3.3 Ταυτοποίηση και Αυθεντικοποίηση για Επαναδημιουργία Κλειδιών

3.3.1 Ταυτοποίηση και Αυθεντικοποίηση για Τακτική Επαναδημιουργία Κλειδιών

Για τα Πιστοποιητικά τελικού χρήστη, τα οποία δεν έχουν ανακληθεί και είναι σε ισχύ, είναι δυνατή η ανανέωση τους με ταυτόχρονη επαναδημιουργία κλειδιών δεδομένης της επιβεβαίωσης της ορθότητας των στοιχείων του Τελικού Χρήστη.

3.3.2 Ταυτοποίηση και Αυθεντικό ποίηση για Επαναδημιουργία Κλειδιών Μετά την Ανάκληση

Σύμφωνα με τα προβλεπόμενα στην §3.3.2 της ΠΠ της ΑΠΕΔ.

3.4 Ταυτοποίηση και Αυθεντικοποίηση για Αίτηση Ανάκλησης

Για την ανάκληση Πιστοποιητικών Τελικών Χρηστών είναι απαραίτητη η ταυτοποίηση του Τελικού Χρήστη σύμφωνα με τις διαδικασίες που περιγράφονται στην §4.9.3.

4. Λειτουργικές Απαιτήσεις Κύκλου Ζωής Πιστοποιητικών

4.1 Αίτηση για Έκδοση Πιστοποιητικού

4.1.1 Ποιος Μπορεί να Υποβάλλει Αίτηση για Έκδοση Πιστοποιητικού

Σύμφωνα με τα προβλεπόμενα στην §4.1.1 της ΠΠ της ΑΠΕΔ.

4.1.2 Διαδικασίες για τη χορήγηση Πιστοποιητικού

4.1.2.1 Διαδικασίες για τη χορήγηση Πιστοποιητικού Τελικού Χρήστη

Για τη χορήγηση Πιστοποιητικών Τελικού Χρήστη, όλοι οι Τελικοί Χρήστες υποβάλλονται σε διαδικασία εγγραφής και επαλήθευσης της ταυτότητας η οποία συνίσταται σε:

- Υποβολή αιτήματος χορήγησης πιστοποιητικού.
- Φυσική παρουσία του ίδιου του Τελικού Χρήστη στο αρμόδιο Εντεταλμένο Γραφείο ή, αν αυτό κρίνεται απαραίτητο, σε εκπροσώπους της Αρχής Εγγραφής ή της Αρχής Πιστοποίησης, για επιβεβαίωση της ταυτότητας του Τελικού Χρήστη.
- Γραπτή ή ηλεκτρονική αποδοχή των Όρων Χρήσης Πιστοποιητικού (ΟΧΠ).
- Παραγωγή ή υποβολή αιτήματος για παραγωγή ζεύγους κλειδιών σύμφωνα με την §6.1 της ΠΠ.
- Αποστολή του δημόσιου κλειδιού από τον Τελικό Χρήστη, στην εκδότρια ΑΠ, σύμφωνα με την §6.1.3 της ΠΠ.
- Ο Τελικός Χρήστης αποδεικνύει στην εκδότρια ΑΠ σύμφωνα με την §3.2.1 της ΠΠ ότι έχει στην κατοχή του το ιδιωτικό κλειδί υπογραφής που αντιστοιχεί στο δημόσιο κλειδί που απέστειλε στην εκδότρια ΑΠ.

Τα αρχεία που διατηρούνται από την ΥπΑΠ περιλαμβάνουν τις πληροφορίες που καταγράφονται στην §5.5.1 της ΠΠ.

Στην περίπτωση μιας αίτησης για ανανέωση ή επανέκδοση:

- οποιεσδήποτε αλλαγές στους ΟΧΠ μετά από την προηγούμενη εγγραφή ή επανεγγραφή είναι σύμφωνες με την §2.2 της ΠΠ και
- τα αρχεία που διατηρούνται σύμφωνα με την §5.5.1 της ΠΠ επίσης περιλαμβάνουν τη συγκατάθεση του Τελικού Χρήστη σε οποιεσδήποτε τέτοιες αλλαγές.

4.2 Επεξεργασία Αίτησης Έκδοσης Πιστοποιητικού

4.2.1 Έκδοση Πιστοποιητικού Τελικού Χρήστη

Σύμφωνα με τα προβλεπόμενα στην §4.2.1 της ΠΠ της ΑΠΕΔ.

4.2.2 Χρόνος Επεξεργασίας Αιτήσεων

Σύμφωνα με τα προβλεπόμενα στην §4.2.3 της ΠΠ της ΑΠΕΔ.

4.3 Έκδοση Πιστοποιητικού

4.3.1 Ενέργειες της εκδότριας ΑΠ κατά τη Διάρκεια Έκδοσης Πιστοποιητικού Τελικού Χρήστη

Σύμφωνα με τα προβλεπόμενα στην §4.3.1 της ΠΠ της ΑΠΕΔ.

4.3.2 Ενημέρωση του Τελικού Χρήστη για την Έκδοση Πιστοποιητικού

Οι ΥπΑΠ ενημερώνουν τους Τελικούς Χρήστες για τη διαδικασία έκδοσης των ψηφιακών πιστοποιητικών, για τη διαθεσιμότητα αυτών και τους τρόπους παραλαβής των μέσα από τη διεύθυνση http://www.ermis.gov.gr. Οι σχετικές πληροφορίες είναι διαθέσιμες στον ενδιαφερόμενο κατόπιν εισόδου του στο σύστημα.

4.4 Αποδοχή Πιστοποιητικού

4.4.1 Ενέργειες που Αποτελούν Αποδοχή Πιστοποιητικού

Σύμφωνα με τα προβλεπόμενα στην §4.4.1 της ΠΠ της ΑΠΕΔ.

4.4.2 Δημοσίευση Πιστοποιητικού από την Αρχή Πιστοποίησης

Σύμφωνα με τα προβλεπόμενα στην §4.4.2 της ΠΠ της ΑΠΕΔ.
Επιπρόσθετα, τα πιστοποιητικά που εκδίδουν οι ΥπΑΠ είναι διαθέσιμα μέσω αναζήτησης στον εξυπηρετητή (server) του καταλόγου LDAP στη διεύθυνση https://pki.ermis.gov.gr/repository.html.

4.5 Ζεύγος κλειδιών και Χρήση Πιστοποιητικών

4.5.1 Χρήση Ιδιωτικού Κλειδιού και Πιστοποιητικού από Τελικό Χρήστη

Σύμφωνα με τα προβλεπόμενα στην §4.5.1 της ΠΠ της ΑΠΕΔ.

4.5.2 Χρήση Δημοσίου Κλειδιού και Πιστοποιητικού από Τρίτο Συμμετέχοντα

Σύμφωνα με τα προβλεπόμενα στην §4.5.2 της ΠΠ της ΑΠΕΔ.

4.6 Ανανέωση Πιστοποιητικού

4.6.1 Συνθήκες για Ανανέωση Πιστοποιητικού

Σύμφωνα με τα προβλεπόμενα στην §4.6.1 της ΠΠ της ΑΠΕΔ. Οι ΥπΑΠ δε προσφέρουν δυνατότητα ανανέωσης πιστοποιητικών χωρίς την επαναδημιουργία κλειδιών.

4.7 Επαναδημιουργία Κλειδιών Πιστοποιητικού

4.7.1 Συνθήκες Επαναδημιουργίας Κλειδιών Πιστοποιητικού

Σύμφωνα με τα προβλεπόμενα στην §4.7.1 της ΠΠ της ΑΠΕΔ.

4.7.2 Ποιος Μπορεί να Αιτηθεί Πιστοποίηση Νέου Κλειδιού

Σύμφωνα με τα προβλεπόμενα στην §4.7.2 της ΠΠ της ΑΠΕΔ.

4.7.3 Επεξεργασία Αιτημάτων Επαναδημιουργίας Κλειδιών Πιστοποιητικού

Σύμφωνα με τα προβλεπόμενα στην §4.7.3 της ΠΠ της ΑΠΕΔ.

4.7.4 Ενημέρωση Χρήστη για την Έκδοση Νέου Πιστοποιητικού.

Η κοινοποίηση έκδοσης Πιστοποιητικού με επαναδημιουργημένα κλειδιά στον Τελικό Χρήστη πραγματοποιείται σύμφωνα με τα προβλεπόμενα στην §4.3.2 της ΔΠ.

4.7.5 Ενέργειες που Αποτελούν Αποδοχή Πιστοποιητικού με Νέο Κλειδί

Σύμφωνα με τα προβλεπόμενα στην §4.7.5 της ΠΠ της ΑΠΕΔ.

4.7.6 Δημοσίευση του Νέου Πιστοποιητικού από την Αρχή Πιστοποίησης

Οι εκδότριες ΑΠ δημοσιεύουν τα Πιστοποιητικά με επαναδημιουργημένα κλειδιά σε χώρο πληροφοριών προσβάσιμο από το κοινό, σύμφωνα με την §4.4.2 της ΔΠ.

4.8 Μετατροπή Πιστοποιητικού

Σύμφωνα με τα προβλεπόμενα στην §4.8 της ΠΠ της ΑΠΕΔ.

4.9 Αναστολή και Ανάκληση Πιστοποιητικού

4.9.1 Συνθήκες Ανάκλησης

Σύμφωνα με τα προβλεπόμενα στην §4.9.1 της ΠΠ της ΑΠΕΔ.

4.9.2 Ποιος Μπορεί να Ζητήσει Ανάκληση

Σύμφωνα με τα προβλεπόμενα στην §4.9.2 της ΠΠ της ΑΠΕΔ.

4.9.3 Διαδικασία για Υποβολή Αιτήματος Ανάκλησης Πιστοποιητικού

Ένας Τελικός Χρήστης που επιθυμεί ανάκληση του Πιστοποιητικού του πρέπει να υποβάλλει αίτημα ανάκλησης με τους παρακάτω τρόπους:

- Στη διεύθυνση http://www.ermis.gov.gr, όπου η υποβολή του αιτήματος επιτρέπεται μόνο κατόπιν εισόδου του στο σύστημα.
- Μέσω τηλεφωνικής επικοινωνίας με στελέχη των Εντεταλμένων Γραφείων. Η ταυτοποίηση και επιβεβαίωση των στοιχείων του αιτούντα γίνεται από εκπρόσωπο του Εντεταλμένου Γραφείου με ταυτόχρονη καταγραφή της συνομιλίας.
- Με φυσική παρουσία του ίδιου του Τελικού Χρήστη (ή άλλου νομίμως εξουσιοδοτημένου προσώπου) σε εκπροσώπους των Εντεταλμένων Γραφείων, ή όπου αυτό κρίνεται απαραίτητο, σε εκπροσώπους της Αρχής Εγγραφής ή της Αρχής Πιστοποίησης.
- Με ενυπόγραφη αίτηση του ενδιαφερόμενου (ιδίου Τελικού Χρήστη ή άλλου νομίμως εξουσιοδοτημένου προσώπου) από όπου να τεκμηριώνεται επαρκώς η νομιμότητα αυτής η ταυτότητα του αιτούντα καθώς και η σχέση του με τον Τελικό Χρήστη, όπου αυτό έχει εφαρμογή.

4.9.4 Χρονικό Διάστημα Μέσα στο Οποίο η ΑΠ θα Πρέπει να Επεξεργαστεί το Αίτημα Ανάκλησης

Σύμφωνα με τα προβλεπόμενα στην §4.9.4 της ΠΠ της ΑΠΕΔ.

4.9.5 Απαιτήσεις Ελέγχου Ανάκλησης για Τρίτους Συμμετέχοντες

Σύμφωνα με τα προβλεπόμενα στην §4.9.5 της ΠΠ της ΑΠΕΔ.
Ειδικότερα, οι ΚΑΠ των ΥπΑΠ είναι διαθέσιμες από τη διεύθυνση https://pki.ermis.gov.gr/repository.html.

4.9.6 Συχνότητα Έκδοσης Καταλόγου Ανακληθέντων Πιστοποιητικών (ΚΑΠ)

Σύμφωνα με τα προβλεπόμενα στην §4.9.6 της ΠΠ της ΑΠΕΔ.

4.9.7 Μέγιστος Χρόνος Αναμονής για ΚΑΠ

Σύμφωνα με τα προβλεπόμενα στην §4.9.7 της ΠΠ της ΑΠΕΔ.

4.9.8 Διαθεσιμότητα Δικτυακού Ελέγχου Ανάκλησης/Κατάστασης Πιστοποιητικών

Οι πληροφορίες για την κατάσταση Πιστοποιητικών που εκδίδουν οι ΥπΑΠ είναι επίσης διαθέσιμες και μέσω της χρήσης του Πρωτοκόλλου Δικτυακού Ελέγχου Κατάστασης Πιστοποιητικών σε πραγματικό χρόνο (Online Certificate Status Protocol - OCSP).

4.9.9 Απαιτήσεις Δικτυακού Ελέγχου Ανάκλησης

Σύμφωνα με τα προβλεπόμενα στην §4.9.9 της ΠΠ της ΑΠΕΔ.

4.9.10 Άλλες Διαθέσιμες Μορφές Αναγγελίας Ανάκλησης

Σύμφωνα με τα προβλεπόμενα στην §4.9.10 της ΠΠ της ΑΠΕΔ.

4.9.11 Ειδικές Απαιτήσεις Σχετικά με την Έκθεση σε Κίνδυνο του Κλειδιού

Σύμφωνα με τα προβλεπόμενα στην §4.9.11 της ΠΠ της ΑΠΕΔ.

4.9.12 Συνθήκες για Αναστολή Πιστοποιητικού

Οι ΥπΑΠ δε παρέχουν υπηρεσίες αναστολής πιστοποιητικού σε Τελικούς Χρήστες. Η δυνατότητα της αναστολής πιστοποιητικού Τελικού Χρήστη παρέχεται μόνο σε στελέχη της Αρχής Εγγραφής σε περιπτώσεις όπου υπάρχουν ενδείξεις ή σοβαρές υπόνοιες για χρήση του πιστοποιητικού που δεν είναι σύμφωνη με τους ΟΧΠ κάτω από τους οποίους έχει χορηγηθεί το εν λόγω πιστοποιητικό.
Το στέλεχος της ΑΕ που θα προβεί στην αναστολή πιστοποιητικού Τελικού Χρήστη οφείλει να ενημερώσει τον ενδιαφερόμενο σε εύλογο χρονικό διάστημα για αυτήν του την ενέργεια καθώς και για τις ενέργειες που απαιτούνται από πλευράς Τελικού Χρήστη ώστε να αλλάξει η κατάσταση του πιστοποιητικού.

4.10 Υπηρεσίες Κατάστασης Πιστοποιητικού

4.10.1 Λειτουργικά Χαρακτηριστικά

Η κατάσταση των Πιστοποιητικών διατίθεται μέσω των διευθύνσεων που ορίζονται στην §4.9.5 για τον ΚΑΠ και §4.9.8 για τον OCSP Responder.

4.10.2 Διαθεσιμότητα Υπηρεσίας

Σύμφωνα με τα προβλεπόμενα στην §4.10.2 της ΠΠ της ΑΠΕΔ.

4.11 Τερματισμός Εγγραφής

Σύμφωνα με τα προβλεπόμενα στην §4.11 της ΠΠ της ΑΠΕΔ.

4.12 Παρακαταθήκη Κλειδιού και Ανάκτηση

Κανένας συμμετέχοντας στην ΥΔΚ της ΑΠΕΔ δεν μπορεί να παρακαταθέτει τα ιδιωτικά κλειδιά ΑΠ ή ΑΕ.
Η δυνατότητα της παρακαταθήκης κλειδιού (key escrow) και ανάκτησης (key recovery) αυτού υφίσταται μόνο στις περιπτώσεις ιδιωτικών κλειδιών Πιστοποιητικών Τελικών Χρηστών, που έχουν εκδοθεί σύμφωνα με την ΠΠ 2 σε φυσικό πρόσωπο (όπως πολιτικό προϊστάμενο ή δημόσιο υπάλληλο) στο πλαίσιο της άσκησης των καθηκόντων του για την εξυπηρέτηση των αναγκών φορέα του δημοσίου.
Επίσης δύναται να παρέχεται προς όλα τα φυσικά πρόσωπα κατ` επιλογήν τους κατά τη διαδικασία υποβολής της αίτησης για απόκτηση ψηφιακού πιστοποιητικού.

4.12.1 Πολιτική και Πρακτικές Παρακαταθήκης Κλειδιού και Ανάκτησης

Σύμφωνα με τα προβλεπόμενα στην §4.12.1 της ΠΠ της ΑΠΕΔ.

5. Φυσικά, Διαδικαστικά Μέτρα Προστασίας και Ασφάλειας Προσωπικού

Σύμφωνα με τα προβλεπόμενα στην §5 της ΠΠ της ΑΠΕΔ.

6. Τεχνικά Μέτρα Ασφαλείας

Σύμφωνα με τα προβλεπόμενα στην §6 της ΠΠ της ΑΠΕΔ.
Ειδικότερα, αναφορικά με την παρακαταθήκη ιδιωτικού κλειδιού οι ΥπΑΠ δεν καταθέτουν τα ιδιωτικά κλειδιά Τελικών Χρηστών σε οιοδήποτε τρίτο πρόσωπο.
Επιπρόσθετα, πρόσβαση στα ιδιωτικά κλειδιά κρυπτογράφησης Τελικών Χρηστών για τους σκοπούς της ανάκτησης παρέχεται μόνο σε στελέχη της Αρχής Εγγραφής ή της ΥπΑΠ και επιτρέπεται μόνο κατόπιν σχετικής αίτησης από τον Τελικό Χρήστη. Όλες οι ενέργειες των στελεχών της Αρχής Εγγραφής ή της ΥπΑΠ αναφορικά με την ανάκτηση των κλειδιών καταγράφονται για τη διενέργεια σχετικών ελέγχων.

7. Προφίλ Πιστοποιητικού, Καταλόγου Ανακληθέντων Πιστοποιητικών (ΚΑΠ) και OCSP

Σύμφωνα με τα προβλεπόμενα στην §7 της ΠΠ της ΑΠΕΔ.

8. Έλεγχος Συμμόρφωσης και Άλλες Αξιολογήσεις

Σύμφωνα με τα προβλεπόμενα στην §8 της ΠΠ της ΑΠΕΔ.

9. Άλλα Επιχειρησιακά και Νομικά Ζητήματα

9.1 Τέλη Παροχής Υπηρεσιών Πιστοποίησης

9.1.1 Τέλη Έκδοσης ή Ανανέωσης Πιστοποιητικού

Οι ΥπΑΠ δύνανται να χρεώνουν τους τελικούς χρήστες για την έκδοση, το χειρισμό και την ανανέωση Πιστοποιητικών Τελικών Χρηστών καθώς και για τις απαιτούμενες Ασφαλείς Διατάξεις Δημιουργίας Υπογραφών.

9.1.2 Τέλη για την Πρόσβαση σε Πιστοποιητικό

Σύμφωνα με τα προβλεπόμενα στην §9.1.2 της ΠΠ της ΑΠΕΔ.

9.1.3 Τέλη Πρόσβασης σε Πληροφορίες Ανάκλησης ή Κατάστασης

Σύμφωνα με τα προβλεπόμενα στην §9.1.3 της ΠΠ της ΑΠΕΔ.

9.1.4 Τέλη για Άλλες Υπηρεσίες

Οι ΥπΑΠ δε χρεώνουν τέλη για την πρόσβαση στην παρούσα πράξη. Οποιαδήποτε χρήση γίνεται για σκοπούς διαφορετικούς από την απλή ανάγνωση αυτών των εγγράφων, όπως είναι η αναπαραγωγή, αναδιανομή, τροποποίηση ή δημιουργία αντιγράφων απαιτεί έγκριση ύστερα από αίτηση, σύμφωνα με όσα προβλέπονται στο άρθρο 5 του Νόμου 3448/2006, προς την ΥπΑΠ, η οποία κατέχει και τα δικαιώματα πνευματικής ιδιοκτησίας.

9.2 Εμπιστευτικότητα Πληροφοριών

Σύμφωνα με τα προβλεπόμενα στην §9.2 της ΠΠ της ΑΠΕΔ.

9.3 Προστασία Δεδομένων Προσωπικού Χαρακτήρα

Σύμφωνα με τα προβλεπόμενα στην §9.4 της ΠΠ της ΑΠΕΔ.

9.4 Δικαιώματα Πνευματικής Ιδιοκτησίας

Σύμφωνα με τα προβλεπόμενα στην §9.5 της ΠΠ της ΑΠΕΔ.

9.5 Δηλώσεις και Εγγυήσεις

Σύμφωνα με τα προβλεπόμενα στην §9.6 της ΠΠ της ΑΠΕΔ.

9.6 Αποποιήσεις Εγγυήσεων

Σύμφωνα με τα προβλεπόμενα στην §9.7 της ΠΠ της ΑΠΕΔ.

9.7 Περιορισμοί Ευθύνης

Οι ΥπΑΠ δε φέρουν καμία ευθύνη για τις όποιες έμμεσες, εξαιρετικές, θετικές, τυχαίες, συνεπαγόμενες και αποθετικές ζημιές.

9.8 Διάρκεια Ισχύος και Τερματισμός

9.8.1 Έναρξη Ισχύος

Η ισχύς της παρούσας άρχεται με την δημοσίευση της στο Φύλλο της Εφημερίδας της Κυβέρνησης. Κατόπιν, η παρούσα ΔΠ δημοσιεύεται άμεσα στον δικτυακό αποθηκευτικό χώρο της ΥπΑΠ.

9.8.2 Λήξη Ισχύος

Η παρούσα ΔΠ θα παραμείνει εν ισχύ έως την αντικατάσταση της από τυχόν νέα, τροποποιημένη έκδοση, σύμφωνα με τα αναφερόμενα στην παρ. §9.11 της παρούσας.

9.8.3 Συνέπειες Λήξης Ισχύος

Με την κατάργηση της παρούσας ΔΠ, οι ΥπΑΠ, οι Τελικοί Χρήστες και οι Τρίτοι Συμμετέχοντες της Υποδομής Δημοσίου Κλειδιού της ΑΠΕΔ, εξακολουθούν να δεσμεύονται από τους όρους της, ως προς όλα τα πιστοποιητικά που έχουν εκδοθεί κατά τη διάρκεια ισχύος της παρούσας, και για το υπόλοιπο της περιόδου ισχύος τους.

9.9 Ειδοποίηση Προσώπων και Επικοινωνία με τους Συμμετέχοντες

Σύμφωνα με τα προβλεπόμενα στην §9.10 της ΠΠ της ΑΠΕΔ.

9.10 Τροποποιήσεις

Τροποποιήσεις της παρούσας ΔΠ επιτρέπονται ύστερα από πρόταση της ΥπΑΠ και με τη σύμφωνη γνώμη της ΑΠΕΔ. Οι τροποποιήσεις θα είναι είτε υπό μορφή εγγράφου που περιέχει τις τροποποιήσεις της ΔΠ ή με νέα έκδοση της ΔΠ. Οι τροποποιημένες ή νέες εκδόσεις παρατίθενται στο τμήμα του Χώρου Αποθήκευσης της ΥπΑΠ στις διευθύνσεις: http://www.yap.gov.gr, http://www.ermis.gov. gr, και http://www.syzefxis.gov.gr. Οι νέες εκδόσεις της ΔΠ υπερισχύουν έναντι οποιωνδήποτε προηγούμενων.

9.10.1 Στοιχεία που Μπορούν να Τροποποιηθούν Χωρίς Προειδοποίηση

Οι ΥπΑΠ δύνανται να προτείνουν τροποποιήσεις του παρόντος χωρίς προειδοποίηση των Τελικών Χρηστών και Τρίτων Συμμετεχόντων, για μεταβολές που δεν είναι ουσιώδους σημασίας, περιλαμβανομένων ενδεικτικά, διορθώσεων τυπογραφικών λαθών, αλλαγών των δικτυακών κόμβων (URL) και μεταβολών των στοιχείων επικοινωνίας.

9.10.2 Στοιχεία που Μπορούν να Τροποποιηθούν Με Προειδοποίηση

Οι ΥπΑΠ δύνανται να προβούν σε ουσιώδεις τροποποιήσεις της ΔΠ ύστερα από προειδοποίηση των Τελικών Χρηστών τουλάχιστον με σχετική ανακοίνωση στον Χώρο Αποθήκευσης της στις διευθύνσεις: https://pki.ermis.gov.gr/repository.html, http://www.yap.gov.gr και http://www.syzefxis.gov.gr.

9.10.3 Ανακοίνωση Τροποποιήσεων

Οι ΥπΑΠ ανακοινώνουν τις τροποποιήσεις της ΔΠ στο τμήμα του Χώρου Αποθήκευσης των που προορίζεται για Ενημερώσεις και Ανακοινώσεις στις διευθύνσεις: https://pki.ermis.gov.gr/repository.html, http://www.yap.gov. gr και http://www.syzefxis.gov.gr.

9.11 Επίλυση Διαφορών

Σύμφωνα με τα προβλεπόμενα στην §9.13 της ΠΠ της ΑΠΕΔ.

9.12 Εφαρμοστέο Δίκαιο

Η ερμηνεία, η εγκυρότητα, η ισχύς και η εφαρμογή της παρούσας ΔΠ διέπεται από την κοινοτική και την κείμενη ελληνική νομοθεσία.

9.13 Ανωτέρα Βία

Σύμφωνα με τα προβλεπόμενα στην §9.15 της ΠΠ της ΑΠΕΔ.

Γ. Δήλωση Πρακτικής των Υποκείμενων Αρχών Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΠΠ 7)

1. Εισαγωγή

Η παρούσα Δήλωση Πρακτικής των Υποκείμενων Αρχών Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ), εφεξής ΥπΑΠ, εξειδικεύει την Πολιτική Πιστοποίησης της ΑΠΕΔ για συγκεκριμένες πολιτικές πιστοποιητικών (§1.2.1), και ειδικότερα τους όρους και τις προϋποθέσεις καθώς και τις τεχνικές προδιαγραφές για την έγκριση, έκδοση, χειρισμό, χρήση, ανάκληση και ανανέωση των ψηφιακών πιστοποιητικών τελικών χρηστών σύμφωνα με τις διατάξεις της παραγράφου 2 του Άρθρου 20 του Νόμου 3448/2006 (ΦΕΚ 57/Α).

Η παρούσα δήλωση πρακτικής εφαρμόζει και υλοποιεί την Πολιτική Πιστοποίησης της ΑΠΕΔ εκτός και αν από τις διατάξεις της παρούσας ορίζεται διαφορετικά.

1.1 Περίληψη

Η παρούσα Δήλωση Πρακτικής (ΔΠ) καθορίζει:

- Τις υποχρεώσεις των ΥπΑΠ, των Αρχών Εγγραφής (Registration Authorities), των Τελικών Χρηστών και των Τρίτων Συμμετεχόντων.
- Τα θέματα που αφορούν στους Όρους Χρήσης Πιστοποιητικών (ΟΧΠ) Τελικού Χρήστη και τους Όρους Τρίτων Συμμετεχόντων (ΟΤΣ).
- Τις μεθόδους που χρησιμοποιούνται για την επιβεβαίωση της ταυτότητας των Τελικών Χρηστών.
- Τις λειτουργικές διαδικασίες ως προς τις υπηρεσίες κύκλου ζωής Πιστοποιητικού: υποβολή αιτήματος για έκδοση, αποδοχή, ανάκληση και ανανέωση Πιστοποιητικού.
- Το περιεχόμενο των Πιστοποιητικών, των Καταλόγων Ανακληθέντων Πιστοποιητικών (ΚΑΠ), και των Πιστοποιητικών της υπηρεσίας δικτυακού ελέγχου κατάστασης πιστοποιητικών σε πραγματικό χρόνο (Online Certificate Status Protocol - OCSP), όταν διατίθεται.
- Τις λειτουργικές διαδικασίες ασφάλειας ως προς την καταγραφή στοιχείων ελέγχου, την τήρηση αρχείων και την αποκατάσταση καταστροφών.
- Τους κανονισμούς φυσικής ασφάλειας, ασφάλειας προσωπικού, διαχείρισης κλειδιών και λογικής ασφάλειας.
- Τη διαχείριση της ΔΠ, συμπεριλαμβανομένων των μεθόδων τροποποίησης της.

Ο Πίνακας 1 περιλαμβάνει τον κατάλογο των προς δημοσίευση εγγράφων των ΥπΑΠ, καθώς και των τοποθεσιών δημοσίευσης αυτών. Τα έγγραφα που δε διατίθενται προς δημοσίευση αποτελούν εμπιστευτικό υλικό της ΑΠΕΔ.

Πίνακας 1: Διαθέσιμα Έγγραφα Κανονισμών

Έγγραφα	Κατάσταση	Τοποθεσία Δημοσίευσης για το Κοινό
Πολιτική Πιστοποιητικών της ΑΠΕΔ	Δημόσιο	Χώρος Αποθήκευσης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου, σύμφωνα με την §2.2 της ΠΠ της ΑΠΕΔ
Όροι Χρήσης Πιστοποιητικών (ΟΧΠ) Τελικών Χρηστών και Όροι Τρίτου Συμμετέχοντα (ΟΤΣ)	Δημόσιο	Χώρος Αποθήκευσης των ΥπΑΠ, σύμφωνα με την §2.2 της παρούσας ΔΠ

1.2 Όνομα και Ταυτότητα Εγγράφου

Οι ΥπΑΠ έχουν προσαρμόσει την παρούσα ΔΠ στο πρότυπο Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (Πλαίσιο Πολιτικής Πιστοποιητικού Υποδομής Δημόσιου Κλειδιού και Κανονισμών Πιστοποίησης X.509 για το Διαδίκτυο), γνωστό και ως RFC 3647, της Ομάδας Δράσης για την Διαδικτυακή Μηχανική (Internet Engineering Task Force), φορέας ο οποίος είναι υπεύθυνος για τον καθορισμό προτύπων στο Διαδίκτυο, για να διευκολύνει την απεικόνιση της εφαρμοζόμενης πολιτικής πιστοποιητικού.
Μικρές αποκλίσεις από την δομή του RFC 3647 σε επιμέρους λεπτομέρειες, είναι απαραίτητες εξαιτίας της εφαρμογής του λειτουργικού μοντέλου της ΑΠ στο δημόσιο τομέα.

1.2.1 Προσφερόμενες Υπηρεσίες των ΥπΑΠ

Οι ΥπΑΠ που εφαρμόζουν την παρούσα ΔΠ διαχειρίζονται τον κύκλο ζωής των ψηφιακών πιστοποιητικών τελικών χρηστών (έκδοση, ανάκληση, αναστολή και ανανέωση) σύμφωνα με την ΠΠ 7 της Πολιτικής Πιστοποίησης της ΑΠΕΔ.

1.2.2 Τιμές Προσδιοριστή Αντικειμένου

Τα Πιστοποιητικά που εκδίδονται από τις ΥπΑΠ σύμφωνα με την παρούσα ΔΠ περιλαμβάνουν τιμές προσδιοριστή αντικειμένου (Object Identifier) που αντιστοιχούν στην εκάστοτε πολιτική πιστοποιητικού που ακολουθείται. Η τιμή προσδιοριστή αντικειμένου για την:

- ΠΠ 7 είναι: 1.2.300.0.110001.1.7.1.1.7

1.3 Συμμετέχοντες στην Υποδομή Δημοσίου Κλειδιού

Σύμφωνα με τα προβλεπόμενα στην §1.3 της ΠΠ της ΑΠΕΔ.

1.4 Εφαρμογή των Πιστοποιητικών

Σύμφωνα με τα προβλεπόμενα στην §1.4 της ΠΠ της ΑΠΕΔ.

1.5 Διαχείριση Δήλωσης Πρακτικής

1.5.1 Οργανισμός που διαχειρίζεται το έγγραφο

Την παρούσα ΔΠ εκδίδει η Αρχή Πιστοποίησης του Ελληνικού Δημοσίου σύμφωνα με τις διατάξεις της παραγράφου 2 του άρθρου 1 του Ν 3448/2006 (ΦΕΚ 57/Α).
Τυχόν αιτήματα για διευκρινίσεις επί των κεφαλαίων του παρόντος θα απευθύνονται προς την Αρχή Πιστοποίησης του Ελληνικού Δημοσίου.

1.5.2 Στοιχεία επικοινωνίας

Τα στοιχεία επικοινωνίας για τις ΥπΑΠ δημοσιεύονται στις παρακάτω ιστοσελίδες:

- http://www.ermis.gov.gr
- http://www.yap.gov.gr
- http://www.syzefxis.gov.gr

1.6 Ορισμοί και ακρωνύμια

Στο Παράρτημα Α παρατίθεται Πίνακας Ορισμών και Ακρωνυμίων.

2. Δημοσίευση και Χώρος Αποθήκευσης

2.1 Χώροι Αποθήκευσης

Σύμφωνα με τα προβλεπόμενα στην §2.1 της ΠΠ της ΑΠΕΔ.

2.2 Δημοσίευση Πληροφοριών

Σύμφωνα με τα προβλεπόμενα στην §2.2 της ΠΠ της ΑΠΕΔ.

2.2.1 Δημοσίευση της ΔΠ

Η παρούσα ΔΠ δημοσιεύεται σε ηλεκτρονική μορφή στις διευθύνσεις https://pki.ermis.gov.gr/repository.html, http://www.yap.gov.gr, και http://www.syzefxis.gov.gr όπου βρίσκεται διαθέσιμη σε μορφή εγγράφου Adobe Acrobat® pdf ή/και Microsoft Word® ή HTML.

2.2.2 Στοιχεία που δε δημοσιεύονται στη ΔΠ

Τα έγγραφα ασφαλείας που θεωρούνται εμπιστευτικά από τις ΥπΑΠ δεν αποκαλύπτονται σε τρίτους.

2.3 Χρόνος ή Συχνότητα Δημοσίευσης

Οι ΥπΑΠ ανακοινώνουν τις τροποποιήσεις της ΔΠ, μέσα σε εύλογο χρονικό διάστημα στο Χώρο Αποθήκευσης τους, στις διευθύνσεις που αναφέρονται στην ενότητα §2.2.1.

Τα Πιστοποιητικά Τελικών Χρηστών δημοσιεύονται κατά την έκδοση. Πληροφορίες αναφορικά με την κατάσταση Πιστοποιητικών δημοσιεύονται σύμφωνα με τις §4.9.6 και §4.9.8 της ΔΠ.

2.4 Έλεγχοι Πρόσβασης σε Χώρους Αποθήκευσης

Σύμφωνα με τα προβλεπόμενα στην §2.4 της ΠΠ της ΑΠΕΔ.

3. Αναγνώριση και Ταυτοποίηση

3.1 Ονοματοδοσία

Σύμφωνα με τα προβλεπόμενα στην §3.1 της ΠΠ της ΑΠΕΔ.

3.1.1 Τύποι Ονομάτων

Σύμφωνα με τα προβλεπόμενα στην §3.1.1 της ΠΠ της ΑΠΕΔ.

3.1.2 Ανάγκη Κατανόησης των Ονομάτων

Σύμφωνα με τα προβλεπόμενα στην §3.1.2 της ΠΠ της ΑΠΕΔ.

3.1.3 Ανωνυμία ή ψευδωνυμία τελικού χρήστη

Οι ΥπΑΠ δεν εκδίδουν πιστοποιητικά όπου στα στοιχεία του Τελικού Χρήστη αναγράφεται ψευδώνυμο.

3.1.4 Μοναδικότητα των Ονομάτων

Σύμφωνα με τα προβλεπόμενα στην §3.1.4 της ΠΠ της ΑΠΕΔ.

3.1.5 Αναγνώριση και Αυθεντικοποίηση

Σύμφωνα με τα προβλεπόμενα στην §3.1.5 της ΠΠ της ΑΠΕΔ.

3.2 Αρχική Εγγραφή

3.2.1 Μέθοδος Απόδειξης της Κατοχής Ιδιωτικού Κλειδιού

Σύμφωνα με τα προβλεπόμενα στην §3.2.1 της ΠΠ της ΑΠΕΔ.

3.2.2 Μέθοδος Απόδειξης της Ταυτότητας Φορέα (ΠΠ 7)

Σύμφωνα με τα προβλεπόμενα στην §3.2.2 της ΠΠ της ΑΠΕΔ.

3.2.3 Μέθοδος Απόδειξης της Ταυτότητας Φυσικού Προσώπου

Σύμφωνα με τα προβλεπόμενα στην §3.2.3 της ΠΠ της ΑΠΕΔ.

3.2.4 Πληροφορίες Τελικού Χρήστη που Δεν Επαληθεύονται

Σύμφωνα με τα προβλεπόμενα στην §3.2.4 της ΠΠ της ΑΠΕΔ.

3.3 Ταυτοποίηση και Αυθεντικοποίηση για Επαναδημιουργία Κλειδιών

3.3.1 Ταυτοποίηση και Αυθεντικοποίηση για Τακτική Επαναδημιουργία Κλειδιών

Για τα Πιστοποιητικά τελικού χρήστη, τα οποία δεν έχουν ανακληθεί και είναι σε ισχύ, είναι δυνατή η ανανέωση τους με ταυτόχρονη επαναδημιουργία κλειδιών δεδομένης της επιβεβαίωσης της ορθότητας των στοιχείων του Τελικού Χρήστη.

3.3.2 Ταυτοποίηση και Αυθεντικοποίηση για Επαναδημιουργία Κλειδιών Μετά την Ανάκληση

Σύμφωνα με τα προβλεπόμενα στην §3.3.2 της ΠΠ της ΑΠΕΔ.

3.4 Ταυτοποίηση και Αυθεντικοποίηση για Αίτηση Ανάκλησης

Για την ανάκληση Πιστοποιητικών Τελικών Χρηστών είναι απαραίτητη η ταυτοποίηση του νόμιμου Εκπροσώπου του Φορέα, του νόμιμου εκπροσώπου του εποπτεύοντος φορέα, ή άλλου νομίμως εξουσιοδοτημένου για το σκοπό αυτό προσώπου, σύμφωνα με τις διαδικασίες που περιγράφονται στην §4.9.3.

4. Λειτουργικές Απαιτήσεις Κύκλου Ζωής Πιστοποιητικών

4.1 Αίτηση για Έκδοση Πιστοποιητικού

4.1.1 Ποιος Μπορεί να Υποβάλλει Αίτηση για Έκδοση Πιστοποιητικού

Σύμφωνα με τα προβλεπόμενα στην §4.1.1 της ΠΠ της ΑΠΕΔ.

4.1.2 Διαδικασίες για τη χορήγηση Πιστοποιητικού

4.1.2.1 Διαδικασίες για τη χορήγηση Πιστοποιητικού Τελικού Χρήστη

Για τη χορήγηση Πιστοποιητικών Τελικού Χρήστη, όλοι οι Τελικοί Χρήστες υποβάλλονται σε διαδικασία εγγραφής και επαλήθευσης της ταυτότητας η οποία συνίσταται σε:

- Υποβολή αιτήματος χορήγησης πιστοποιητικού.
- Φυσική παρουσία του νόμιμου Εκπροσώπου του Φορέα, ή νόμιμου εκπροσώπου του εποπτεύοντος φορέα, ή άλλου νομίμως εξουσιοδοτημένου για το σκοπό αυτό προσώπου, στο αρμόδιο Εντεταλμένο Γραφείο ή, αν αυτό κρίνεται απαραίτητο, σε εκπροσώπους της Αρχής Εγγραφής ή της Αρχής Πιστοποίησης, για επιβεβαίωση της ταυτότητας του Τελικού Χρήστη.
- Γραπτή ή ηλεκτρονική αποδοχή των Όρων Χρήσης Πιστοποιητικού (ΟΧΠ).
- Παραγωγή ή υποβολή αιτήματος για παραγωγή ζεύγους κλειδιών σύμφωνα με την §6.1 της ΠΠ.
- Αποστολή του δημόσιου κλειδιού από το φορέα, στην εκδότρια ΑΠ, σύμφωνα με την §6.1.3 της ΠΠ.
- Ο Τελικός Χρήστης αποδεικνύει στην εκδότρια ΑΠ σύμφωνα με την §3.2.1 της ΠΠ ότι έχει στην κατοχή του το ιδιωτικό κλειδί υπογραφής που αντιστοιχεί στο δημόσιο κλειδί που απέστειλε στην εκδότρια ΑΠ.

Τα αρχεία που διατηρούνται από την ΥπΑΠ περιλαμβάνουν τις πληροφορίες που καταγράφονται στην §5.5.1 της ΠΠ.

Στην περίπτωση μιας αίτησης για ανανέωση ή επανέκδοση:

- οποιεσδήποτε αλλαγές στους ΟΧΠ μετά από την προηγούμενη εγγραφή ή επανεγγραφή είναι σύμφωνες με την §2.2 της ΠΠ και
- τα αρχεία που διατηρούνται σύμφωνα με την §5.5.1 της ΠΠ επίσης περιλαμβάνουν τη συγκατάθεση του νόμιμου Εκπροσώπου του Φορέα, του νόμιμου εκπροσώπου του εποπτεύοντος φορέα, ή άλλου νομίμως εξουσιοδοτημένου για το σκοπό αυτό προσώπου, σε οποιεσδήποτε τέτοιες αλλαγές.

4.2 Επεξεργασία Αίτησης Έκδοσης Πιστοποιητικού

4.2.1 Έκδοση Πιστοποιητικού Τελικού Χρήστη

Σύμφωνα με τα προβλεπόμενα στην §4.2.1 της ΠΠ της ΑΠΕΔ.

4.2.2 Χρόνος Επεξεργασίας Αιτήσεων

Σύμφωνα με τα προβλεπόμενα στην §4.2.3 της ΠΠ της ΑΠΕΔ.

4.3 Έκδοση Πιστοποιητικού

4.3.1 Ενέργειες της εκδότριας ΑΠ κατά τη Διάρκεια Έκδοσης Πιστοποιητικού Τελικού Χρήστη

Σύμφωνα με τα προβλεπόμενα στην §4.3.1 της ΠΠ της ΑΠΕΔ.

4.3.2 Ενημέρωση του Τελικού Χρήστη για την Έκδοση Πιστοποιητικού

Οι ΥπΑΠ ενημερώνουν τον νόμιμο Εκπρόσωπο του Φορέα, ή τον νόμιμο εκπρόσωπο του εποπτεύοντος φορέα, ή το νομίμως εξουσιοδοτημένο για το σκοπό αυτό πρόσωπο, για τη διαδικασία έκδοσης των ψηφιακών πιστοποιητικών, για τη διαθεσιμότητα αυτών και τους τρόπους παραλαβής των μέσα από τη διεύθυνση http://www.ermis. gov.gr. Οι σχετικές πληροφορίες είναι διαθέσιμες στον ενδιαφερόμενο κατόπιν εισόδου του στο σύστημα.

4.4 Αποδοχή Πιστοποιητικού

4.4.1 Ενέργειες που Αποτελούν Αποδοχή Πιστοποιητικού

Σύμφωνα με τα προβλεπόμενα στην §4.4.1 της ΠΠ της ΑΠΕΔ.

4.4.2 Δημοσίευση Πιστοποιητικού από την Αρχή Πιστοποίησης

Σύμφωνα με τα προβλεπόμενα στην §4.4.2 της ΠΠ της ΑΠΕΔ.

Επιπρόσθετα, τα πιστοποιητικά που εκδίδουν οι ΥπΑΠ είναι διαθέσιμα μέσω αναζήτησης στον εξυπηρετητή (server) του καταλόγου LDAP στη διεύθυνση https://pki. ermis.gov.gr/repository.html.

4.5 Ζεύγος κλειδιών και Χρήση Πιστοποιητικών

4.5.1 Χρήση Ιδιωτικού Κλειδιού και Πιστοποιητικού από Τελικό Χρήστη

Σύμφωνα με τα προβλεπόμενα στην §4.5.1 της ΠΠ της ΑΠΕΔ.

4.5.2 Χρήση Δημοσίου Κλειδιού και Πιστοποιητικού από Τρίτο Συμμετέχοντα

Σύμφωνα με τα προβλεπόμενα στην §4.5.2 της ΠΠ της ΑΠΕΔ.

4.6 Ανανέωση Πιστοποιητικού

4.6.1 Συνθήκες για Ανανέωση Πιστοποιητικού

Σύμφωνα με τα προβλεπόμενα στην §4.6.1 της ΠΠ της ΑΠΕΔ. Οι ΥπΑΠ δε προσφέρουν δυνατότητα ανανέωσης πιστοποιητικών χωρίς την επαναδημιουργία κλειδιών.

4.7 Επαναδημιουργία Κλειδιών Πιστοποιητικού

4.7.1 Συνθήκες Επαναδημιουργίας Κλειδιών Πιστοποιητικού

Σύμφωνα με τα προβλεπόμενα στην §4.7.1 της ΠΠ της ΑΠΕΔ.

4.7.2 Ποιος Μπορεί να Αιτηθεί Πιστοποίηση Νέου Κλειδιού

Σύμφωνα με τα προβλεπόμενα στην §4.7.2 της ΠΠ της ΑΠΕΔ.

4.7.3 Επεξεργασία Αιτημάτων Επαναδημιουργίας Κλειδιών Πιστοποιητικού

Σύμφωνα με τα προβλεπόμενα στην §4.7.3 της ΠΠ της ΑΠΕΔ.

4.7.4 Ενημέρωση Χρήστη για την Έκδοση Νέου Πιστοποιητικού.

Η κοινοποίηση έκδοσης Πιστοποιητικού με επαναδημιουργημένα κλειδιά στον νόμιμο Εκπρόσωπο του Φορέα, τον νόμιμο εκπρόσωπο του εποπτεύοντος φορέα, ή το νομίμως εξουσιοδοτημένο για το σκοπό αυτό πρόσωπο, πραγματοποιείται σύμφωνα με τα προβλεπόμενα στην §4.3.2 της ΔΠ.

4.7.5 Ενέργειες που Αποτελούν Αποδοχή Πιστοποιητικού με Νέο Κλειδί

Σύμφωνα με τα προβλεπόμενα στην §4.7.5 της ΠΠ της ΑΠΕΔ.

4.7.6 Δημοσίευση του Νέου Πιστοποιητικού από την Αρχή Πιστοποίησης

Οι εκδότριες ΑΠ δημοσιεύουν τα Πιστοποιητικά με επαναδημιουργημένα κλειδιά σε χώρο πληροφοριών προσβάσιμο από το κοινό, σύμφωνα με την §4.4.2 της ΔΠ.

4.8 Μετατροπή Πιστοποιητικού

Σύμφωνα με τα προβλεπόμενα στην §4.8 της ΠΠ της ΑΠΕΔ.

4.9 Αναστολή και Ανάκληση Πιστοποιητικού

4.9.1 Συνθήκες Ανάκλησης

Σύμφωνα με τα προβλεπόμενα στην §4.9.1 της ΠΠ της ΑΠΕΔ.

4.9.2 Ποιος Μπορεί να Ζητήσει Ανάκληση

Σύμφωνα με τα προβλεπόμενα στην §4.9.2 της ΠΠ της ΑΠΕΔ.

4.9.3 Διαδικασία για Υποβολή Αιτήματος Ανάκλησης Πιστοποιητικού

Ο νόμιμος Εκπρόσωπος του Φορέα, ή νόμιμος εκπρόσωπος του εποπτεύοντος φορέα, ή νομίμως εξουσιοδοτημένο για αυτό το σκοπό φυσικό πρόσωπο που επιθυμεί ανάκληση του Πιστοποιητικού του φορέα πρέπει να υποβάλλει αίτημα ανάκλησης με τους παρακάτω τρόπους:

- Με φυσική παρουσία του σε εκπροσώπους των Εντεταλμένων Γραφείων, ή όπου αυτό κρίνεται απαραίτητο, σε εκπροσώπους της Αρχής Εγγραφής ή της Αρχής Πιστοποίησης.

- Με ενυπόγραφη αίτηση του από όπου να τεκμηριώνεται επαρκώς η νομιμότητα αυτής.

4.9.4 Χρονικό Διάστημα Μέσα στο Οποίο η ΑΠ θα Πρέπει να Επεξεργαστεί το Αίτημα Ανάκλησης.

Σύμφωνα με τα προβλεπόμενα στην §4.9.4 της ΠΠ της ΑΠΕΔ.

4.9.5 Απαιτήσεις Ελέγχου Ανάκλησης για Τρίτους Συμμετέχοντες

Σύμφωνα με τα προβλεπόμενα στην §4.9.5 της ΠΠ της ΑΠΕΔ.
Ειδικότερα, οι ΚΑΠ των ΥπΑΠ είναι διαθέσιμες από τη διεύθυνση https://pki.ermis.gov.gr/repository.html.

4.9.6 Συχνότητα Έκδοσης Καταλόγου Ανακληθέντων Πιστοποιητικών (ΚΑΠ)

Σύμφωνα με τα προβλεπόμενα στην §4.9.6 της ΠΠ της ΑΠΕΔ.

4.9.7 Μέγιστος Χρόνος Αναμονής για ΚΑΠ

Σύμφωνα με τα προβλεπόμενα στην §4.9.7 της ΠΠ της ΑΠΕΔ.

4.9.8 Διαθεσιμότητα Δικτυακού Ελέγχου Ανάκλησης/ Κατάστασης Πιστοποιητικών

Οι πληροφορίες για την κατάσταση Πιστοποιητικών που εκδίδουν οι ΥπΑΠ είναι επίσης διαθέσιμες και μέσω της χρήσης του Πρωτοκόλλου Δικτυακού Ελέγχου Κατάστασης Πιστοποιητικών σε πραγματικό χρόνο (Online Certificate Status Protocol - OCSP).

4.9.9 Απαιτήσεις Δικτυακού Ελέγχου Ανάκλησης

Σύμφωνα με τα προβλεπόμενα στην §4.9.9 της ΠΠ της ΑΠΕΔ.

4.9.10 Άλλες Διαθέσιμες Μορφές Αναγγελίας Ανάκλησης

Σύμφωνα με τα προβλεπόμενα στην §4.9.10 της ΠΠ της ΑΠΕΔ.

4.9.11 Ειδικές Απαιτήσεις Σχετικά με την Έκθεση σε Κίνδυνο του Κλειδιού

Σύμφωνα με τα προβλεπόμενα στην §4.9.11 της ΠΠ της ΑΠΕΔ.

4.9.12 Συνθήκες για Αναστολή Πιστοποιητικού

Οι ΥπΑΠ δε παρέχουν υπηρεσίες αναστολής πιστοποιητικού σε Τελικούς Χρήστες. Η δυνατότητα της αναστολής πιστοποιητικού Τελικού Χρήστη παρέχεται μόνο σε στελέχη της Αρχής Εγγραφής σε περιπτώσεις όπου υπάρχουν ενδείξεις ή σοβαρές υπόνοιες για χρήση του πιστοποιητικού που δεν είναι σύμφωνη με τους ΟΧΠ κάτω από τους οποίους έχει χορηγηθεί το εν λόγω πιστοποιητικό.
Το στέλεχος της ΑΕ που θα προβεί στην αναστολή πιστοποιητικού Τελικού Χρήστη οφείλει να ενημερώσει τον ενδιαφερόμενο σε εύλογο χρονικό διάστημα για αυτήν του την ενέργεια καθώς και για τις ενέργειες που απαιτούνται από πλευράς Τελικού Χρήστη ώστε να αλλάξει η κατάσταση του πιστοποιητικού.

4.10 Υπηρεσίες Κατάστασης Πιστοποιητικού

4.10.1 Λειτουργικά Χαρακτηριστικά

Η κατάσταση των Πιστοποιητικών διατίθεται μέσω των διευθύνσεων που ορίζονται στην §4.9.5 για τον ΚΑΠ και §4.9.8 για τον OCSP Responder.

4.10.2 Διαθεσιμότητα Υπηρεσίας

Σύμφωνα με τα προβλεπόμενα στην §4.10.2 της ΠΠ της ΑΠΕΔ.

4.11 Τερματισμός Εγγραφής

Σύμφωνα με τα προβλεπόμενα στην §4.11 της ΠΠ της ΑΠΕΔ.

4.12 Παρακαταθήκη Κλειδιού και Ανάκτηση

Κανένας συμμετέχοντας στην ΥΔΚ της ΑΠΕΔ δεν μπορεί να παρακαταθέτει τα ιδιωτικά κλειδιά ΑΠ ή ΑΕ.
Η δυνατότητα της παρακαταθήκης κλειδιού (key escrow) και ανάκτησης (key recovery) αυτού για κλειδιά φορέων του δημοσίου, δεν παρέχεται.

4.12.1 Πολιτική και Πρακτικές Παρακαταθήκης Κλειδιού και Ανάκτησης

Σύμφωνα με τα προβλεπόμενα στην §4.12.1 της ΠΠ της ΑΠΕΔ.

5. Φυσικά, Διαδικαστικά Μέτρα Προστασίας και Ασφάλειας Προσωπικού

Σύμφωνα με τα προβλεπόμενα στην §5 της ΠΠ της ΑΠΕΔ.

6. Τεχνικά Μέτρα Ασφαλείας

Σύμφωνα με τα προβλεπόμενα στην §6 της ΠΠ της ΑΠΕΔ.
Επιπρόσθετα, ο φορέας οφείλει να λάβει όλα τα απαραίτητα τεχνικά και διαδικαστικά μέτρα ώστε να εξασφαλίσει την προστασία του ιδιωτικού κλειδιού από μη εξουσιοδοτημένη χρήση καθόλη τη διάρκεια του κύκλου ζωής του.

7. Προφίλ Πιστοποιητικού, Καταλόγου Ανακληθέντων Πιστοποιητικών (ΚΑΠ) και OCSP

Σύμφωνα με τα προβλεπόμενα στην §7 της ΠΠ της ΑΠΕΔ.

8. Έλεγχος Συμμόρφωσης και Άλλες Αξιολογήσεις

Σύμφωνα με τα προβλεπόμενα στην §8 της ΠΠ της ΑΠΕΔ.

9. Άλλα Επιχειρησιακά και Νομικά Ζητήματα

9.1 Τέλη Παροχής Υπηρεσιών Πιστοποίησης

9.1.1 Τέλη Έκδοσης ή Ανανέωσης Πιστοποιητικού

Οι ΥπΑΠ δύνανται να χρεώνουν τους τελικούς χρήστες για την έκδοση, το χειρισμό και την ανανέωση Πιστοποιητικών Τελικών Χρηστών καθώς και για τις Ασφαλείς Διατάξεις Δημιουργίας Υπογραφών, αν αυτές απαιτούνται.

9.1.2 Τέλη για την Πρόσβαση σε Πιστοποιητικό

Σύμφωνα με τα προβλεπόμενα στην §9.1.2 της ΠΠ της ΑΠΕΔ.

9.1.3 Τέλη Πρόσβασης σε Πληροφορίες Ανάκλησης ή Κατάστασης

Σύμφωνα με τα προβλεπόμενα στην §9.1.3 της ΠΠ της ΑΠΕΔ.

9.1.4 Τέλη για Άλλες Υπηρεσίες

Οι ΥπΑΠ δε χρεώνουν τέλη για την πρόσβαση στην παρούσα πράξη.
Οποιαδήποτε χρήση γίνεται για σκοπούς διαφορετικούς από την απλή ανάγνωση αυτών των εγγράφων, όπως είναι η αναπαραγωγή, αναδιανομή, τροποποίηση ή δημιουργία αντιγράφων απαιτεί έγκριση ύστερα από αίτηση, σύμφωνα με όσα προβλέπονται στο άρθρο 5 του Νόμου 3448/2006, προς την ΥπΑΠ, η οποία κατέχει και τα δικαιώματα πνευματικής ιδιοκτησίας.

9.2 Εμπιστευτικότητα Πληροφοριών

Σύμφωνα με τα προβλεπόμενα στην §9.2 της ΠΠ της ΑΠΕΔ.

9.3 Προστασία Δεδομένων Προσωπικού Χαρακτήρα

Σύμφωνα με τα προβλεπόμενα στην §9.4 της ΠΠ της ΑΠΕΔ.

9.4 Δικαιώματα Πνευματικής Ιδιοκτησίας

Σύμφωνα με τα προβλεπόμενα στην §9.5 της ΠΠ της ΑΠΕΔ.

9.5 Δηλώσεις και Εγγυήσεις

Σύμφωνα με τα προβλεπόμενα στην §9.6 της ΠΠ της ΑΠΕΔ.

9.6 Αποποιήσεις Εγγυήσεων

Σύμφωνα με τα προβλεπόμενα στην §9.7 της ΠΠ της ΑΠΕΔ.

9.7 Περιορισμοί Ευθύνης

Οι ΥπΑΠ δε φέρουν καμία ευθύνη για τις όποιες έμμεσες, εξαιρετικές, θετικές, τυχαίες, συνεπαγόμενες και αποθετικές ζημιές.

9.8 Διάρκεια Ισχύος και Τερματισμός

9.8.1 Έναρξη Ισχύος

Η ισχύς της παρούσας άρχεται με την δημοσίευση της στο Φύλλο της Εφημερίδας της Κυβέρνησης. Κατόπιν, η παρούσα ΔΠ δημοσιεύεται άμεσα στον δικτυακό αποθηκευτικό χώρο της ΥπΑΠ.

9.8.2 Λήξη Ισχύος

Η παρούσα ΔΠ θα παραμείνει εν ισχύ έως την αντικατάσταση της από τυχόν νέα, τροποποιημένη έκδοση, σύμφωνα με τα αναφερόμενα στην παρ. §9.11 της παρούσας.

9.8.3 Συνέπειες Λήξης Ισχύος

Με την κατάργηση της παρούσας ΔΠ, οι ΥπΑΠ, οι Τελικοί Χρήστες και οι Τρίτοι Συμμετέχοντες της Υποδομής Δημοσίου Κλειδιού της ΑΠΕΔ, εξακολουθούν να δεσμεύονται από τους όρους της, ως προς όλα τα πιστοποιητικά που έχουν εκδοθεί κατά τη διάρκεια ισχύος της παρούσας, και για το υπόλοιπο της περιόδου ισχύος τους.

9.9 Ειδοποίηση Προσώπων και Επικοινωνία με τους Συμμετέχοντες

Σύμφωνα με τα προβλεπόμενα στην §9.10 της ΠΠ της ΑΠΕΔ.

9.10 Τροποποιήσεις

Τροποποιήσεις της παρούσας ΔΠ επιτρέπονται ύστερα από πρόταση της ΥπΑΠ και με τη σύμφωνη γνώμη της ΑΠΕΔ. Οι τροποποιήσεις θα είναι είτε υπό μορφή εγγράφου που περιέχει τις τροποποιήσεις της ΔΠ ή με νέα έκδοση της ΔΠ. Οι τροποποιημένες ή νέες εκδόσεις παρατίθενται στο τμήμα του Χώρου Αποθήκευσης της ΥπΑΠ στις διευθύνσεις: http://www.yap.gov.gr, http://www.ermis.gov. gr, και http://www.syzefxis.gov.gr. Οι νέες εκδόσεις της ΔΠ υπερισχύουν έναντι οποιωνδήποτε προηγούμενων.

9.10.1 Στοιχεία που Μπορούν να Τροποποιηθούν Χωρίς Προειδοποίηση

Οι ΥπΑΠ δύνανται να προτείνουν τροποποιήσεις του παρόντος χωρίς προειδοποίηση των Τελικών Χρηστών και Τρίτων Συμμετεχόντων, για μεταβολές που δεν είναι ουσιώδους σημασίας, περιλαμβανομένων ενδεικτικά, διορθώσεων τυπογραφικών λαθών, αλλαγών των δικτυακών κόμβων (URL) και μεταβολών των στοιχείων επικοινωνίας.

9.10.2 Στοιχεία που Μπορούν να Τροποποιηθούν Με Προειδοποίηση

Οι ΥπΑΠ δύνανται να προβούν σε ουσιώδεις τροποποιήσεις της ΔΠ ύστερα από προειδοποίηση των Τελικών Χρηστών τουλάχιστον με σχετική ανακοίνωση στον Χώρο Αποθήκευσης της στις διευθύνσεις: https://pki.ermis.gov.gr/repository.html, http://www.yap.gov.gr και http://www.syzefxis.gov.gr.

9.10.3 Ανακοίνωση Τροποποιήσεων

Οι ΥπΑΠ ανακοινώνουν τις τροποποιήσεις της ΔΠ στο τμήμα του Χώρου Αποθήκευσης των που προορίζεται για Ενημερώσεις και Ανακοινώσεις στις διευθύνσεις:
https://pki.ermis.gov.gr/repository.html, http://www.yap.gov.gr και http://www.syzefxis.gov.gr.

9.11 Επίλυση Διαφορών

Σύμφωνα με τα προβλεπόμενα στην §9.13 της ΠΠ της ΑΠΕΔ.

9.12 Εφαρμοστέο Δίκαιο

Η ερμηνεία, η εγκυρότητα, η ισχύς και η εφαρμογή της παρούσας ΔΠ διέπεται από την κοινοτική και την κείμενη ελληνική νομοθεσία.

9.13 Ανωτέρα Βία

Σύμφωνα με τα προβλεπόμενα στην §9.15 της ΠΠ της ΑΠΕΔ.

3. ΠΑΡΑΡΤΗΜΑ Α - Ακρωνύμια και Ορισμοί

Πίνακας 1: Πίνακας Ορισμών

Όρος	Ορισμός
OCSP (Online Certificate Status Protocol) /Πρωτόκολλο Δικτυακού Ελέγχου Κατάστασης Πιστοποιητικών	Το πρωτόκολλο που χρησιμοποιείται για την παροχή σε Τρίτους Συμμετέχοντες πληροφοριών σε πραγματικό χρόνο σχετικά με την κατάσταση των Πιστοποιητικών.
PKCS # 10	Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού (Public−Key Cryptography Standard) #10, που έχει αναπτυχθεί από τη RSA Security Inc., το οποίο καθορίζει τη δομή του Αιτήματος Υπογραφής Πιστοποιητικού.
PKCS # 12	Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού (Public−Key Cryptography Standard) #12, που έχει αναπτυχθεί από τη RSA Security Inc., το οποίο καθορίζει το ασφαλές μέσο για τη μεταβίβαση των ιδιωτικών κλειδιών
RSA	Το κρυπτογραφικό σύστημα δημοσίου κλειδιού που επινοήθηκε από τους Rivest, Shamir, και Adelman.
Secure Sockets Layer (SSL)/ (Επίπεδα Ασφαλών Συνδέσεων)	Η καθιερωμένη (βιομηχανικά) μέθοδος για την προστασία των επικοινωνιών Δικτύου που αναπτύχθηκε από τη Netscape Communications Corporation. Το πρωτόκολλο ασφαλείας SSL παρέχει κρυπτογράφηση δεδομένων, ταυτοποίηση εξυπηρετητή (server), αρτιότητα μηνύματος, και προαιρετικά ταυτοποίηση χρήστη (client) για μία σύνδεση Transmission Control Protocol/Internet Protocol (Πρωτοκόλλου Ελέγχου Μετάδοσης/ Πρωτοκόλλου Διαδικτύου).
Αίτημα Υπογραφής Πιστοποιητικού (Certificate Signing Request	Μήνυμα που μεταφέρει το αίτημα για την έκδοση ενός Πιστοποιητικού.
Αναγνωρισμένο Πιστοποιητικό	Πιστοποιητικό που πληρεί τους όρους του Παραρτήματος Ι του ΠΔ 150/2001 και εκδίδεται από πάροχο υπηρεσιών πιστοποίησης ο οποίος πληρεί τους όρους του παραρτήματος ΙΙ του ΠΔ 150/2001.
Αρχή Εγγραφής (ΑΕ)	Ο φορέας ή υπηρεσία που έχει εγκριθεί από μια ΑΠ και υποβοηθά τους ενδιαφερόμενους για Πιστοποιητικά κατά την υποβολή των αιτήσεών τους, εγκρίνει ή απορρίπτει τις εγγραφές / αιτήσεις καθώς επίσης αιτείται στην Αρχή Πιστοποίησης την ανάκληση, ανανέωση, αναστολή ή ανάκτηση Πιστοποιητικών.
Αρχή Πιστοποίησης (ΑΠ)	Ο Φορέας που έχει πιστοποιηθεί να εκδίδει, να χειρίζεται, να ανακαλεί, να αναστέλλει και να ανανεώνει Πιστοποιητικά βάση των διατάξεων του παρόντος και του άρθρου 20 του Ν, 3448/2006 (ΦΕΚ 57 Α').
Ασφαλής Διάταξη Δημιουργίας Υπογραφής (ΑΔΔΥ –SSCD)	Διάταξη δημιουργίας υπογραφής που πληρεί τους όρους του Παραρτήματος ΙΙΙ του ΠΔ 150/2001.
Ασφαλής Κρυπτογραφική Μονάδα (ΑΚΜ –HSM)	Το χρησιμοποιούμενο από τους Παρόχους Υπηρεσιών Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών, Προϊόν Ηλεκτρονικής Υπογραφής που προστατεύεται έναντι τροποποίησης και διασφαλίζει τεχνική και κρυπτογραφική ασφάλεια, σύμφωνα με το Παράρτημα ΙΙ του ΠΔ 150/2001 και πληρεί τις απαιτήσεις της παραγράφου 2 του άρθρου 3 της υπ' αριθ. 295/64/2003 Απόφασης της ΕΕΤΤ «Κανονισμός για τον Έλεγχο Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και Ασφαλών Κρυπτογραφικών Μονάδων».
Δικαιώματα Πνευματικής Ιδιοκτησίας	Δικαιώματα επί ενός ή περισσοτέρων από τα ακόλουθα: κάθε είδους δικαιώματος δημιουργού, εμπορικού μυστικού, εμπορικού σήματος, καθώς και κάθε άλλου δικαιώματος πνευματικής ιδιοκτησίας
Εκδότρια Αρχή Πιστοποίησης	Η Αρχή Πιστοποίησης που εκδίδει Πιστοποιητικά σε Τελικούς Χρήστες ακολουθώντας τουλάχιστον μία εκ των πολιτικών πιστοποιητικών της ΑΠΕΔ. Στην έννοια των Εκδοτριών Αρχών Πιστοποίησης περιλαμβάνονται και οι ΥπΑΠ.
Έκθεση σε Κίνδυνο	Η παραβίαση (ή υποτιθέμενη παραβίαση) μιας πολιτικής ασφαλείας, κατά την οποία μπορεί να έχει συμβεί μη−εξουσιοδοτημένη αποκάλυψη, ή απώλεια του ελέγχου επί, διαβαθμισμένων πληροφοριών. Όσον αφορά τα ιδιωτικά κλειδιά, Έκθεση σε Κίνδυνο αποτελεί η απώλεια, κλοπή, αποκάλυψη, τροποποίηση, μη−εξουσιοδοτημένη χρήση, ή κάθε άλλη έκθεση σε κίνδυνο της ασφάλειας του ιδιωτικού αυτού κλειδιού.
Εμπιστευτικές/ Προσωπικές	Οι πληροφορίες που είναι απαραίτητο να παραμείνουν εμπιστευτικές και

Πληροφορίες	προσωπικές.
Ηλεκτρονική Εγγραφή ή Αίτηση	Η ηλεκτρονική διαδικασία που περιγράφεται στους Κανονισμούς Πιστοποίησης των ΥπΑΠ και που αφορά στα βήματα που πρέπει να προβεί ο Τελικός Χρήστης προκειμένου να αποκτήσει ψηφιακό πιστοποιητικό
Δήλωση Πρακτικής Κανονισμός Πιστοποίησης (ΚΠ)	Πράξεις των εκδοτριών ΑΠ με τις οποίες καθορίζονται οι όροι και οι προϋποθέσεις για την παροχή υπηρεσιών πιστοποίησης που προσφέρουν. Η Δήλωση Πρακτικής συχνά αναφέρεται και ως Κανονισμός Πιστοποίησης.
Κατάλογος Ανακληθέντων Πιστοποιητικών (ΚΑΠ)	Ο περιοδικός (ή έκτακτος) κατάλογος που εκδίδεται ηλεκτρονικά και είναι υπογεγραμμένος από μια ΑΠ, των Πιστοποιητικών που έχουν ανακληθεί πριν από την ημερομηνία λήξης τους. Ο ΚΑΠ αναφέρει το όνομα του εκδότη της ΚΑΠ, την ημερομηνία έκδοσης, την ημερομηνία της επόμενης προγραμματισμένης έκδοσης ΚΑΠ, τους αριθμούς σειράς των ανακληθέντων Πιστοποιητικών, καθώς και τους συγκεκριμένους χρόνους και λόγους ανάκλησής τους.
Κέντρο Επεξεργασίας	Μια ασφαλής λογική και φυσική υποδομή στην οποία φυλάσσονται οι Ασφαλείς Κρυπτογραφικές Μονάδες (ΑΚΜ) και μέσω της οποίας διενεργείται το σύνολο των υπηρεσιών διαχείρισης του κύκλου ζωής πιστοποιητικών (έκδοσης, ανάκλησης, αναστολής και ανανέωσης)
Κωδικός Διαχείρισης Πιστοποιητικού	Μοναδικό αλφαριθμητικό που αποδίδεται στον τελικό χρήστη από την Αρχή Πιστοποίησης και εξασφαλίζει τη μοναδικότητα του Διακριτικού Ονόματος του. Είναι το ίδιο για όλα τα Πιστοποιητικά που εκδίδονται στον συγκεκριμένο χρήστη από την Αρχή Πιστοποίησης.
Λειτουργική Περίοδος	Το χρονικό διάστημα το οποίο ξεκινά την ημερομηνία και το χρόνο έκδοσης ενός Πιστοποιητικού και λήγει την ημερομηνία και το χρόνο λήξης ή πρόωρης ανάκλησης του Πιστοποιητικού.
Πιστοποιητικό	Ηλεκτρονική βεβαίωση η οποία συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο και επιβεβαιώνει την ταυτότητά του.
Πιστοποιητικό Υπευθύνου	Το Πιστοποιητικό που εκδίδεται προς έναν Υπεύθυνο ΑΕ και το οποίο μπορεί να χρησιμοποιηθεί αποκλειστικά για την τέλεση αρμοδιοτήτων ΑΕ.
Προϊόν Ηλεκτρονικής Υπογραφής	Υλικό ή λογισμικό ή συναφή συστατικά στοιχεία τους, που προορίζονται προς χρήση από τον πάροχο υπηρεσιών πιστοποίησης για την προσφορά υπηρεσιών ηλεκτρονικής υπογραφής ή προορίζονται να χρησιμοποιηθούν για τη δημιουργία ή επαλήθευση ηλεκτρονικών υπογραφών.
Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ)	Μια ΑΠ η οποία ενεργεί ως Πρωτεύουσα ΑΠ (Root) και εκδίδει πιστοποιητικά προς υποκείμενες ΑΠ. Στην παρούσα υποδομή η ΑΠΕΔ λειτουργεί ως Πρωτεύουσα Αρχή Πιστοποίησης.
Όροι Τρίτου Συμμετέχοντα	Οι όροι και οι προϋποθέσεις βάση των οποίων ένα φυσικό πρόσωπο ενεργεί ως Τρίτος Συμμετέχων.
Όροι Χρήσης Πιστοποιητικών	Οι όροι και οι προϋποθέσεις χορήγησης και χρήσης πιστοποιητικών βάσει των οποίων ένα φυσικό πρόσωπο ενεργεί ως «αιτών» το πιστοποιητικό (Subscriber).
Τελικός Χρήστης	Το πρόσωπο που αποτελεί το Υποκείμενο (Subject), στο όνομα του οποίου έχει εκδοθεί ένα Πιστοποιητικό. Σε κάποιες περιπτώσεις το φυσικό πρόσωπο που αιτείται το πιστοποιητικό διαφέρει από τον Τελικό Χρήστη (π.χ. πιστοποιητικά που εκδίδονται σύμφωνα με την ΠΠ 7). Ο Τελικός Χρήστης, ή ο αιτών το πιστοποιητικό, είναι εξουσιοδοτημένος να χρησιμοποιεί το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που αναγράφεται στο Πιστοποιητικό και φέρει την ευθύνη για την ορθή χρήση του πιστοποιητικού σύμφωνα με τους ΟΧΠ.
Τρίτος Συμμετέχων	Το φυσικό πρόσωπο ή φορέας που ενεργεί βασιζόμενος σε κάποιο πιστοποιητικά ή/και ηλεκτρονική υπογραφή.
Υπεύθυνος ΑΕ	Ένα Έμπιστο Πρόσωπο το οποίο έχει πρόσβαση στο Κέντρο Ελέγχου της ΑΕ και διενεργεί διαδικασίες του κύκλου ζωής ενός Πιστοποιητικού (π.χ. αποδοχής, ανάκλησης, αναστολής, ανάκτησης ενός Πιστοποιητικού) καθώς και άλλες αρμοδιότητες μιας ΑΕ.
Υποδομή Δημόσιου Κλειδιού (ΥΔΚ)/ Public Key Infrastructure (PKI)	Η αρχιτεκτονική, η οργανωτική δομή, οι τεχνικές, οι κανονισμοί, και οι διαδικασίες που στο σύνολό τους υποστηρίζουν την εφαρμογή και λειτουργία κρυπτογραφικού συστήματος δημοσίου κλειδιού που βασίζεται σε Πιστοποιητικό
Υποκείμενο	Ο κάτοχος ενός ιδιωτικού κλειδιού που αντιστοιχεί σε ένα δημόσιο κλειδί. Το ταυτοποιημένο όνομα ενός Υποκειμένου Πιστοποιητικού είναι συνδεδεμένο με το δημόσιο κλειδί που περιλαμβάνεται στο Πιστοποιητικό.
Ψηφιακή Υπογραφή ή Προηγμένη Ηλεκτρονική Υπογραφή	Ηλεκτρονική υπογραφή που πληρεί τους εξής όρους: • Συνδέεται μονοσήμαντα με τον υπογράφοντα • Είναι ικανή να καθορίσει ειδικά και αποκλειστικά την

	ταυτότητα του υπογράφοντος • Δημιουργείται με μέσα τα οποία ο υπογράφων μπορεί να διατηρήσει υπό τον αποκλειστικό του έλεγχο και • Συνδέεται με τα δεδομένα στα οποία αναφέρεται, κατά τρόπο ώστε να μπορεί να εντοπιστεί οποιαδήποτε μεταγενέστερη αλλοίωση των εν λόγω δεδομένων.
Χώρος Αποθήκευσης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου	Η δικτυακά προσπελάσιμη βάση δεδομένων της Αρχής Πιστοποίησης Ελληνικού Δημοσίου στην οποία περιέχονται τα στοιχεία των Πιστοποιητικών καθώς και άλλες πληροφορίες σχετικές με την Υποδομή Δημοσίου Κλειδιού της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ).

Πίνακας 2: Πίνακας Ακρωνυμίων

Ακρωνύμιο		Όρος (στα Ελληνικά και στα Αγγλικά)
(Ελληνικά)	(Αγγλικά)	
	CC	Common Criteria
	EAL	Evaluation Assurance Level. (Επίπεδο αξιολόγησης εγγυήσεων, σύμφωνα με τα Common Criteria).
	OCSP	Online Certificate Status Protocol (Πρωτόκολλο Δικτυακής Κατάστασης Πιστοποιητικών)
	PIN	Personal identification Number (Προσωπικός αριθμός ταυτότητας)
	PKCS	Public−Key Cryptography Standard (Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού)
	PUK	Personal Unblocking Key (Προσωπικό Κλειδί που χρησιμοποιείται για απεμπλοκή της έξυπνης κάρτας μετά από συνεχή εσφαλμένη εισαγωγή PIN)
	RFC	Request For Comment (Αίτημα για σχολιασμό)
	S/MIME	Secure Multipurpose Internet Mail Extensions
	SSL	Secure Sockets Layer (Επίπεδο Ασφαλών Συνδέσεων)
ΑΕ	RA	Αρχή Εγγραφής. (Registration Authority
ΑΠ	CA	Αρχή Πιστοποίησης (Certification Authority)
ΑΤΛΑ	LSVA	Αξιολόγηση Τρωτότητας της Λογικής Ασφάλειας (Logical security vulnerability assessment.)
ΔΠ	CPS	Δήλωση Πρακτικής (Certification Practice Statement)
ΚΑΠ	CRL	Κατάλογος Ανακληθέντων Πιστοποιητικών (Certificate Revocation List)
ΚΠ		Κανονισμός Πιστοποίησης
ΟΤΣ		Όροι Τρίτου Συμμετέχοντα
ΟΧΠ		Όροι Χρήσης Πιστοποιητικών
ΠΑ	OID	Προσδιοριστής Αντικειμένου (Object Identifier)
ΠΑΠ	RCA	Πρωτεύουσα Αρχή Πιστοποίησης (Root Certification Authority)
ΠΠ	CP	Πολιτική Πιστοποιητικών
ΥΔΚ	PKI	Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure)

4. ΠΑΡΑΡΤΗΜΑ Β` - Πολιτική/ Δήλωση Πρακτικής Χρονοσήμανσης της ΑΠΕΔ

Σύμφωνα με τις διατάξεις της υπ` αριθ. ΥΑΠ/ Φ.60/38/232/2010 (ΦΕΚ 799/Β`/09-06-2010) κοινής απόφασης των υπουργών Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και Υποδομών, Μεταφορών και Δικτύων «Κύρωση του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)», καθορίζονται οι όροι, οι προϋποθέσεις και οι διαδικασίες για την παροχή υπηρεσιών πιστοποίησης από την Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ), σύμφωνα με τις διατάξεις του άρθρου 20 του Ν3448/2006 (ΦΕΚ 57/Α/2006). Εξάλλου, με την υπουργική απόφαση ΥΑΠ/Φ.60/76/984/9-4-2012 (ΦΕΚ 1162/Β`/2012) καθορίστηκαν οι οργανικές μονάδες για την παροχή υπηρεσιών πιστοποίησης της ΑΠΕΔ.

Με την Υπουργική Απόφαση Υ ΑΠ/Φ .40.4/163 (ΦΕΚ 401/ Β/22-02-2013) καθορίζονται οι διαδικασίες και ο τρόπος ηλεκτρονικής επιβεβαίωσης της λήψης εγγράφων και της ασφαλούς χρονοσήμανσης, οι προδιαγραφές και τα πρότυπα του συστήματος για τη γνωστοποίηση εγγράφων σε φυσικά πρόσωπα ή Ν.Π.Ι.Δ. με χρήση ΤΠΕ και η ηλεκτρονική διακίνηση εγγράφων μεταξύ φορέων του δημόσιου τομέα και των φυσικών προσώπων ή ΝΠΙΔ.

Η ΑΠΕΔ παρέχει υπηρεσίες χρονοσήμανσης με σκοπό τη δημιουργία των απαραίτητων τεκμηρίων για την ύπαρξη ενός συνόλου ψηφιακών δεδομένων σε μία συγκεκριμένη χρονική στιγμή. Η Πολιτική Χρονοσήμανσης και η

Δήλωση Πρακτικής Χρονοσήμανσης της ΑΠΕΔ έχουν συγχωνευτεί σε ένα ενιαίο παράρτημα με την ονομασία Πολιτική/ Δήλωση Πρακτικής Χρονοσήμανσης (ΠΔΠΧ). Με τις διατάξεις του παρόντος παραρτήματος καθορίζονται οι πολιτικές και πρακτικές που εφαρμόζονται για την παροχή υπηρεσιών χρονοσήμανσης από την ΑΠΕΔ, ως Πάροχος Υπηρεσιών Χρονοσήμανσης (ΠΥΧ). Η παρούσα ΠΔΠΧ αποσκοπεί στον καθορισμό των σχετικών διαδικασιών της ΑΠΕΔ ως ΠΥΧ.

Η ΑΠΕΔ εφαρμόζει ένα έμπιστο και αξιόπιστο σύστημα ακριβούς χρόνου για την παροχή υπηρεσιών χρονοσήμανσης με χρήση της Υποδομής Δημόσιου Κλειδιού σύμφωνα με τις διατάξεις της κοινής απόφασης των υπουργών Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και Υποδομών, Μεταφορών και Δικτύων (ΦΕΚ 799/ Β709-06-2010) και του προηγουμένου παραρτήματος της παρούσας. Η ΑΠΕΔ λαμβάνει όλα τα αναγκαία μέτρα για τη διασφάλιση της εμπιστευτικότητας και τη διατήρηση της ακεραιότητας των ιδιωτικών κρυπτογραφικών κλειδιών ως ΠΥΧ.

1. Ορισμοί:

- Χρονοσήμανση: Αλληλουχία χαρακτήρων ή στοιχεία που δηλώνουν με ασφάλεια την ημερομηνία και ώρα που έχει λάβει χώρα μία πράξη ή ενέργεια και εκδίδεται από πάροχο υπηρεσιών χρονοσήμανσης.
- Υπηρεσία χρονοσήμανσης: Η δημιουργία των απαραίτητων τεκμηρίων για ένα σύνολο δεδομένων σε ψηφιακή μορφή, έτσι ώστε να μπορεί να αποδειχθεί ότι τα δεδομένα αυτά υπήρχαν σε μία συγκεκριμένη χρονική στιγμή.
- Πάροχος Υπηρεσιών Χρονοσήμανσης: Ο φορέας που εκδίδει χρονοσημάνσεις κατ` εφαρμογή του θεσμικού πλαισίου διαπίστευσης της ΕΕΤΤ και περιλαμβάνεται στον κατάλογο εμπίστευσης της ΕΕΤΤ (Κατάλογος Εμπίστευσης εποπτευόμενων/ διαπιστευμένων Παροχών Υπηρεσιών Πιστοποίησης - TSL).
- Ακριβής χρόνος: Η αναφορά στοιχείων με τα οποία προσδιορίζεται το έτος, ο μήνας, η ημερομηνία, η ώρα, τα λεπτά και τα δευτερόλεπτα. Για τους φορείς του Δημόσιου Τομέα, σύμφωνα με τις διατάξεις της παρούσας, ο ακριβής χρόνος προσδιορίζεται με βάση την Εθνική ώρα Ελλάδας.
- Ηλεκτρονικό έγγραφο: Κάθε μέσο, το οποίο χρησιμοποιείται από υπολογιστικό - πληροφοριακό σύστημα, με ηλεκτρονικό, μαγνητικό ή άλλο τρόπο, για εγγραφή, αποθήκευση, παραγωγή ή αναπαραγωγή στοιχείων που δεν μπορούν να αναγνωστούν άμεσα, όπως και κάθε μαγνητικό, ηλεκτρονικό ή άλλο υλικό, στο οποίο εγγράφεται οποιαδήποτε πληροφορία, εικόνα, σύμβολο ή ήχος, αυτοτελώς ή σε συνδυασμό, εφόσον το εν λόγω περιεχόμενο επιφέρει έννομες συνέπειες ή προορίζεται ή είναι πρόσφορο να αποδείξει γεγονότα που μπορούν να έχουν έννομες συνέπειες.
- Μεταφόρτωση ηλεκτρονικού εγγράφου: Η μεταφορά του συνόλου του περιεχομένου ενός ηλεκτρονικού εγγράφου από το διαδικτυακό τόπο στον οποίο αυτό έχει αναρτηθεί σε αποθηκευτικό χώρο της επιλογής του παραλήπτη.
- Συντονισμένος Παγκόσμιος Χρόνος (Coordinated Universal Time -UTC): Χρονική κλίμακα με βάση το δευτερόλεπτο όπως ορίζεται στη σύσταση ITU-R TF.460-5.
- UTC(x): Ο Συντονισμένος Παγκόσμιος Χρόνος που παράγεται από το εργαστήριο χ.

2. Πολιτική Χρονοσήμανσης:

Η Πολιτική Χρονοσήμανσης είναι ένα σύνολο κανόνων που αφορά την έκδοση και διαχείριση των χρονοσημάνσεων που παράγονται από την ΑΠΕΔ ως ΠΥΧ για τους τελικούς χρήστες. Οι υπηρεσίες χρονοσήμανσης περιλαμβάνουν την οργάνωση της υποδομής και την έκδοση χρονοσημάνσεων. Οι συγκεκριμένες υπηρεσίες παρέχονται από την ΑΠΕΔ στους τελικούς χρήστες στο πλαίσιο λειτουργίας της υποδομής δημοσίου κλειδιού της ΑΠΕΔ. Οι υπηρεσίες παρέχονται κυρίως για την υποστήριξη ψηφιακών υπογραφών αλλά και για οποιαδήποτε εφαρμογή απαιτεί αποδεικτικά στοιχεία για την ύπαρξη κάποιων δεδομένων μία συγκεκριμένη χρονική στιγμή. Η ΑΠΕΔ διασφαλίζει την χρήση αξιόπιστης πηγής ώρας και την κατάλληλη διαχείριση των συστημάτων χρονοσήμανσης. Ειδικότερα, οι υπηρεσίες χρονοσήμανσης περιλαμβάνουν:

- Λειτουργία αντιστοίχισης υπηρεσίας χρονοσήμανσης: Η υπηρεσία χρονοσήμανσης αντιστοιχίζει ένα ηλεκτρονικό αρχείο με μια συγκεκριμένη χρονική στιγμή και εγγυάται την ακρίβεια της χρονικής στιγμής και της αντιστοίχισης
- Ανάκτηση ακριβούς χρόνου: Η διαδικασία χρονοσήμανσης χρησιμοποιεί τον επίσημο χρόνο Coordinated Universal Time (UTC), μέσα από τέτοιες πηγές χρόνου που παρέχουν ασφαλή και ιχνηλάσιμα κανάλια επικοινωνίας. Η μέγιστη απόκλιση από το ρολόι της πηγής είναι ένα (1) δευτερόλεπτο. Η παρεχόμενη προς τους τελικούς χρήστες χρονοσήμανση περιλαμβάνει την απαραίτητη προσαύξηση κατά 2 ώρες έτσι ώστε να είναι σύμφωνα με τη χρονική ζώνη της Ελλάδας.
- Παραγωγή χρονοσημάνσεων: Το σύστημα παράγει χρονοσημάνσεις σύμφωνα με την τεχνική προδιαγραφή ETSI TS 102 023 V1.2.2 (2008-10) "Electronic Signatures and Infrastructures (ESI), Policy requirements for time-

stamping authorities" και το RFC 3628 για τις απαιτήσεις που πρέπει να πληρούν οι ΠΥΧ, καθώς και με την τεχνική προδιαγραφή ETSI TS 101 861 V1.4.1 (2011-07) "Electronic Signatures and Infrastructures (ESI), Time stamping profile" και το RFC 3161 για την έκδοση και τη λήψη ασφαλών χρονοσημάνσεων.

- Επαλήθευση υπογραφών και πιστοποιητικών χρονοσήμανσης: Το κλειδί επαλήθευσης της ψηφιακά υπογεγραμμένης χρονοσήμανσης παρέχεται μέσω ψηφιακού πιστοποιητικού. Τα πιστοποιητικά των συστημάτων της χρονοσήμανσης είναι δημοσιευμένα από την ΑΠΕΔ στον σχετικό κατάλογο της ΥΔΚ της ΑΠΕΔ (https://pki.ermis. gov.gr/repositoryhtml) και η εγκυρότητα τους μπορεί να επαληθευτεί σε σχέση με την παραχθείσα χρονοσήμανση του ηλεκτρονικού εγγράφου.
- Πιστοποιητικό ΠΥΧ: Το πιστοποιητικό παράγεται σύμφωνα με το πρότυπο X.509 v3.

Οι χρονοσφραγίδες παράγονται από την ΑΠΕΔ μέσω του παρακάτω συνδέσμου. TSA uri: http://timestamp.ermis. gov.gr/TSS/HttpTspServer

Προσδιοριστής Αντικειμένου - OID Policy 1.3.6.1.4.1.60110.3.1

Το προφίλ των βασικών πεδίων του πιστοποιητικού χρονοσήμανσης της ΑΠΕΔ περιγράφονται στον Πίνακα 1.

Πίνακας 1. Προφίλ των Βασικών Πεδίων του Πιστοποιητικού Χρονοσήμανσης

Πεδίο	Τιμή ή Περιορισμός Τιμής
Version (Έκδοση)	V3
Serial Number (Αριθμός Σειράς)	Μοναδική τιμή ανά Διακριτικό Όνομα Εκδότη (Issuer DN)
Signature Algorithm (Αλγόριθμος Υπογραφής)	SHA1 RSA
Issuer DN (Διακριτικό Όνομα Εκδότη)	cn=HPARCA Time Stamping Services ou=HPARCA o=Hellenic Public Administration Certification Services c=GR
Valid From (Ισχύει Από)	Βάσει του Universal Coordinate Time. Κωδικοποίηση σύμφωνα με το RFC 5280.
Valid To (Ισχύει Μέχρι)	Βάσει του Universal Coordinate Time. Κωδικοποίηση σύμφωνα με το RFC 5280. Η περίοδος ισχύος δεν υπερβαίνει τη διάρκεια ισχύος του πιστοποιητικού της Πρωτεύουσας Αρχής Πιστοποίησης.
Subject DN (Διακριτικό Όνομα Υποκειμένου)	cn=HPARCA Time Stamping Services ou=HPARCA o=Hellenic Public Administration Certification Services c=GR
Μέγεθος Κλειδιού	2048 bits
Χρήση κλειδιού	Ψηφιακή υπογραφή, Κρυπτογράφηση κλειδιού
Βελτιωμένη χρήση κλειδιού	Χρονική σήμανση

Η υπηρεσία χρονοσήμανσης παρέχεται σύμφωνα με τις διατάξεις της υπ` αριθ. πρωτ.: ΥΑΠ/Φ.40.4/163 «Ρυθμίσεις για α) τη διαδικασία και τον τρόπο ηλεκτρονικής επιβεβαίωσης της λήψης και της ασφαλούς χρονοσήμανσης, β) τις προδιαγραφές και τα πρότυπα του συστήματος για τη γνωστοποίηση εγγράφων σε φυσικά πρόσωπα ή Ν.Π.Ι.Δ. με χρήση ΤΠΕ και γ) την ηλεκτρονική διακίνηση εγγράφων μεταξύ φορέων του δημόσιου τομέα και των φυσικών προσώπων ή ΝΠΙΔ» (ΦΕΚ 401/Β`/22-02-2013).

3. Υποχρεώσεις

Η ΑΠΕΔ εγγυάται και διασφαλίζει την εφαρμογή της Πολιτικής Χρονοσήμανσης σύμφωνα με τις διατάξεις της παραγράφου 2 του παραρτήματος Β` της παρούσας, καθώς και των απαιτήσεων της παραγράφου 4 του παραρτήματος Β` «Δήλωση Πρακτικής».
Ειδικότερα, ως προς τους τελικούς χρήστες και τους τρίτους συμμετέχοντες η ΑΠΕΔ διασφαλίζει ότι η μέγιστη απόκλιση από το UTC ρολόι της πηγής είναι ένα (1) δευτερόλεπτο.
Οι τελικοί χρήστες και οι τρίτοι συμμετέχοντες οφείλουν να επαληθεύουν την εγκυρότητα και την ορθότητα της χρονοσήμανσης.

4. Δήλωση Πρακτικής

Η Δήλωση Πρακτικής της ΑΠΕΔ περιγράφει τον τρόπο με τον οποίο υλοποιείται η Πολιτική Χρονοσήμανσης, η διαδικασία για τη δημιουργία της Υπηρεσίας Χρονοσήμανσης και η διατήρησης της ακρίβειας του ρολογιού.
Για την υλοποίηση της Υπηρεσίας Χρονοσήμανσης εφαρμόζεται το πρωτόκολλο Time-Stamp Protocol (IETF RFC 3161) και ο Εθνικός Χρόνος UTC (EIM), που παράγεται στο Εργαστήριο Χρόνου και Συχνότητας του Ελληνικού Ινστιτούτου Μετρολογίας (ΕΙΜ), το οποίο αναγνωρίζεται διεθνώς ως ένας αξιόπιστος φορέας στη μέτρηση και τήρηση του χρόνου. Το ΕΙΜ διαθέτει μια υψηλής τεχνολογίας και ακρίβειας συστοιχία πρότυπων ατομικών ρολογιών, που μπορεί να παράγει και να τηρήσει τον εθνικό χρόνο με μεγάλη αξιοπιστία.
Το Εργαστήριο Χρόνου - Συχνότητας υλοποιεί μέσω κβαντικών φαινομένων τις μονάδες του Χρόνου (s) και της Συχνότητας (Hz) με την χρήση τριών πρωτευόντων ατομικών προτύπων-ρολογιών καισίου. Η ακρίβεια τήρησης του χρόνου UTC είναι 1 ns.
Το χρονικό διάστημα για το οποίο διατηρείται όλη η σχετική πληροφορία σχετικά με την λειτουργία χρονοσήμανσης είναι τα δέκα χρόνια. Οι αποδεκτοί Time Stamp Hashes είναι οι: SHA-1, SHA-256, SHA-384, SHA-512.

4.1. Πιστοποιητικά συστημάτων χρονοσήμανσης

Τα κρυπτογραφικά κλειδιά και τα πιστοποιητικά των εξυπηρετητών χρονοσήμανσης (TimeStamping Server) παράγονται, αποθηκεύονται και χρησιμοποιούνται μέσα σε ασφαλείς κρυπτογραφικές μονάδες της ΑΠΕΔ οι οποίες πληρούν τις προϋποθέσεις και τις απαιτήσεις της απόφασης της ΕΕΤΤ 295/64 «Κανονισμός για τον Έλεγχο Συμμόρφωσης Ασφαλών Διατάξεων Δημιουργίας Υπογραφής και Ασφαλών Κρυπτογραφικών Μονάδων» (ΦΕΚ 1730/Β/24-11-2003).
Τα Πιστοποιητικά των Εξυπηρετητών Χρονοσήμανσης (TimeStamping Server) δημοσιεύονται στον σχετικό κατάλογο της ΥΔΚ της ΑΠΕΔ (https://pki.ermis.gov.gr/repositoryhtml).

4.2. Λειτουργικές Απαιτήσεις Κύκλου Ζωής Πιστοποιητικών

Η ΑΠΕΔ, ως Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ), υπογράφει τα Πιστοποιητικά των Εξυπηρετητών Χρονοσήμανσης. Το Πιστοποιητικό της ΑΠΕΔ, καθώς και τα Πιστοποιητικά των Εξυπηρετητών Χρονοσήμανσης είναι διαθέσιμα στους Τρίτους Συμμετέχοντες, διαδικτυακά μέσω των χώρων αποθήκευσης της ΑΠΕΔ, καθώς και ως μέρος της Αλυσίδας Πιστοποιητικού η οποία ενσωματώνεται στο Πιστοποιητικό Εξυπηρετητή Χρονοσήμανσης.
Οι Όροι Τρίτου Συμμετέχοντα απαιτούν από τους τελευταίους τη διαβεβαίωση ότι διαθέτουν επαρκείς πληροφορίες για να αποφασίσουν σε ποιο βαθμό θα βασιστούν στις πληροφορίες που αναγράφονται στο Πιστοποιητικό Εξυπηρετητή Χρονοσήμανσης, ότι είναι αποκλειστικά υπεύθυνοι για το εάν θα βασιστούν ή όχι στις πληροφορίες αυτές και ότι θα υποστούν τις νόμιμες συνέπειες από την αποτυχία τους να εκπληρώσουν τις υποχρεώσεις του Τρίτου Συμμετέχοντα σύμφωνα με την παρούσα Πολιτική/ Δήλωση Πρακτικής Χρονοσήμανσης της ΑΠΕΔ.
Οι Τρίτοι Συμμετέχοντες αποδέχονται τους Όρους Τρίτου Συμμετέχοντα ως προϋπόθεση για να εμπιστευθούν το Πιστοποιητικό Εξυπηρετητή Χρονοσήμανσης. Η εξάρτηση από Πιστοποιητικό πρέπει να είναι εύλογη σύμφωνα με τις περιστάσεις. Η ΑΠΕΔ και οι εκδότριες ΑΠ δε φέρουν ευθύνη για την αξιολόγηση της καταλληλότητας χρήσης των Πιστοποιητικών Εξυπηρετητών Χρονοσήμανσης.
Η επαναδημιουργία κλειδιών των Πιστοποιητικών Εξυπηρετητών Χρονοσήμανσης γίνεται κάτω από αυστηρά μέτρα ελέγχου, σε ειδικές Τελετές Δημιουργίας Κλειδιών σύμφωνα με την §6.1.1 της Πολιτικής Πιστοποιητικών. Πιστοποίηση νέου κλειδιού μπορεί να αιτηθεί μόνο ο Εκπρόσωπος της ΑΠΕΔ. Η ΑΠΕΔ έχει δικαίωμα να ζητήσει την ανάκληση πιστοποιητικού Εξυπηρετητή Χρονοσήμανσης. Η ΑΠΕΔ ανακαλεί Πιστοποιητικά Εξυπηρετητών Χρονοσήμανσης, εφόσον:

- Ανακαλύψει ή έχει λόγο να πιστεύει ότι έχει υπάρξει έκθεση σε κίνδυνο του ιδιωτικού κλειδιού Πιστοποιητικού Εξυπηρετητή Χρονοσήμανσης.
- Ανακαλύψει ή έχει λόγο να πιστεύει ότι το Πιστοποιητικό Εξυπηρετητή Χρονοσήμανσης έχει εκδοθεί με τρόπο που δεν είναι ουσιαστικά σύμφωνος με τις διαδικασίες που απαιτούνται από την παρούσα Πολιτική.
- Διαπιστώσει ότι δεν τηρούνται οι όροι της παρούσας Πολιτικής ή υπάρχει παραίτηση από μια ουσιώδη προϋπόθεση για την Έκδοση Πιστοποιητικού Εξυπηρετητή Χρονοσήμανσης.
- Η ΑΠΕΔ παύσει να λειτουργεί ως ΑΠ.

Σε περίπτωση ανάκλησης του Πιστοποιητικού Εξυπηρετητή Χρονοσήμανσης εφαρμόζονται οι διατάξεις της παραγράφου 5 του κεφαλαίου Α της υπ` αριθ. ΥΑΠ/Φ.60/38/232/2010 (ΦΕΚ 799/Β`/09-06-2010) κοινής απόφασης

των υπουργών Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και Υποδομών, Μεταφορών και Δικτύων «Κύρωση του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)».

4.3. Φυσικά, Διαδικαστικά Μέτρα Προστασίας και Ασφάλειας Προσωπικού

Σύμφωνα με τις διατάξεις της παραγράφου 5 του κεφαλαίου Α της υπ` αριθ. ΥΑΠ/Φ.60/38/232/2010 (ΦΕΚ 799/ Β/09-06-2010) κοινής απόφασης των υπουργών Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και Υποδομών, Μεταφορών και Δικτύων «Κύρωση του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)».

4.4. Τεχνικά Μέτρα Ασφάλειας

Σύμφωνα με τις διατάξεις της παραγράφου 6 του κεφαλαίου Α της υπ` αριθ. ΥΑΠ/Φ.60/38/232/2010 (ΦΕΚ 799/ Β/09-06-2010) κοινής απόφασης των υπουργών Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και Υποδομών, Μεταφορών και Δικτύων «Κύρωση του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)».

4.5 Έλεγχος Συμμόρφωσης και Άλλες Αξιολογήσεις

Σύμφωνα με τις διατάξεις της παραγράφου 8 του κεφαλαίου Α της υπ1 αριθ. ΥΑΠ/Φ.60/38/232/2010 (ΦΕΚ 799/ Β/09-06-2010) κοινής απόφασης των υπουργών Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και Υποδομών, Μεταφορών και Δικτύων «Κύρωση του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)».

4.6 Άλλα Επιχειρησιακά και Νομικά Ζητήματα

Σύμφωνα με τις διατάξεις της παραγράφου 9 του κεφαλαίου Α της υπ` αριθ. ΥΑΠ/Φ.60/38/232/2010 (ΦΕΚ 799/ Β/09-06-2010) κοινής απόφασης των υπουργών Εσωτερικών, Αποκέντρωσης και Ηλεκτρονικής Διακυβέρνησης και Υποδομών, Μεταφορών και Δικτύων «Κύρωση του Κανονισμού Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)».

4.7. Τοποθεσίες δημοσίευσης

Όλα τα δημόσια έγγραφα που αφορούν την ΑΠΕΔ ως ΠΥΧ, είναι διαθέσιμα στην επίσημη ιστοσελίδα της Υπηρεσίας Ανάπτυξης Πληροφορικής του ΥΔΜΗΔ http://www.yap.gov.gr όπως και στην ιστοσελίδα https://pki.ermis.gov.gr/repository.html. Η ΑΠΕΔ είναι υπεύθυνη για την τήρηση, ανανέωση και δημοσίευση όλων των παραπάνω στοιχείων.».

**** Με την ΚΥΑ με αριθμ. ΥΑΠ/Φ.60/3431 (ΦΕΚ Β 3320/27.12.2013) παρ.5 προστέθηκε ως άνω το ΠΑΡΑΡΤΗΜΑ Β..*