Αρχή Πιστοποίησης Ελληνικού Δημοσίου

Κανονισμός Πιστοποίησης

Όπως τροποποιήθηκε και ισχύει

[ΦΕΚ Β’2403/24-04-2024]

Τελευταία Ενημέρωση: 24-4-2024

ΠΕΡΙΕΧΟΜΕΝΑ

Έχοντας Υπόψη:

1. Τις διατάξεις:
α) Του Κανονισμού (ΕΕ) 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ (L 257/73).
β) Του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 27ης Απριλίου 2016, για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ (Γενικός Κανονισμός για την Προστασία Δεδομένων).
γ) Του ν. 4727/2020 «Ψηφιακή Διακυβέρνηση (Ενσωμάτωση στην Ελληνική Νομοθεσία της Οδηγίας (ΕΕ) 2016/2102 και της Οδηγίας (ΕΕ) 2019/1024) - Ηλεκτρονικές Επικοινωνίες (Ενσωμάτωση στο Ελληνικό Δίκαιο της Οδηγίας (ΕΕ) 2018/1972) και άλλες διατάξεις», και ιδίως του Κεφαλαίου Θ’ και της παρ. 37 του άρθρου 107 του νόμου αυτού (Α΄ 184).
δ) Του ν. 4624/2019 «Αρχή Προστασίας Δεδομένων Προσωπικού Χαρακτήρα, μέτρα εφαρμογής του Κανονισμού (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας δεδομένων προσωπικού χαρακτήρα και ενσωμάτωση στην εθνική νομοθεσία της Οδηγίας (ΕΕ) 2016/680 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 και άλλες διατάξεις (Α’137)».
ε) Του π.δ. 40/2020 «Οργανισμός του Υπουργείου Ψηφιακής Διακυβέρνησης».
στ) Του π.δ. 77/2023 «Σύσταση Υπουργείου και μετονομασία Υπουργείων-Σύσταση, κατάργηση και μετονομασία Γενικών και Ειδικών Γραμματειών-Μεταφορά αρμοδιοτήτων, υπηρεσιακών μονάδων, θέσεων προσωπικού και εποπτευόμενων φορέων» (Α’ 130).
ζ) Του π.δ. 79/2023 «Διορισμός Υπουργών, Αναπληρωτών Υπουργών και Υφυπουργών» (Α΄ 131).
η) Του άρθρου 90 του Κώδικα Νομοθεσίας για την Κυβέρνηση και τα κυβερνητικά όργανα, (π.δ. 63/2005 - Α’ 98), σε συνδυασμό με την παρ. 22 του άρθρου 119 του ν. 4622/2019 (Α' 133).
2. Την υπ΄ αριθμ. 245 ΕΞ 2022/5.1.2022 απόφαση του Υπουργού Επικρατείας «Έναρξη λειτουργίας της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)». (Β΄43)
3. Την υπ΄ αριθμ. 243 ΕΞ 2022/5.1.2022 απόφαση του Υπουργού Επικρατείας «Κανονισμός Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)». (Β΄43)
4. Την υπ΄ αριθμ. 2051 ΕΞ 2022/19.1.2023 απόφαση των Υπουργών Ψηφιακής Διακυβέρνησης και Επικρατείας «Καθορισμός οργανικών μονάδων της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ).» (Β΄ 216)
5. Την υπ’ αριθμ. 837/1Β/30.11.2017 απόφαση της ΕΕΤΤ «Κανονισμός Παροχής Υπηρεσιών Εμπιστοσύνης» (Β’ 4396).
6. Την υπ’ αριθμ. 1012/03/25.10.2021 απόφαση της ΕΕΤΤ «Αξιολόγηση συμμόρφωσης των υπηρεσιών έκδοσης εγκεκριμένων πιστοποιητικών ηλεκτρονικής υπογραφής και εγκεκριμένων ηλεκτρονικών χρονοσφραγίδων της ‘ΑΡΧΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΤΟΥ ΕΛΛΗΝΙΚΟΥ ΔΗΜΟΣΙΟΥ (ΑΠΕΔ)’», σύμφωνα με την οποία διαπιστώνεται η συμμόρφωση της ΑΠΕΔ με τις απαιτήσεις του Κανονισμού ΕΕ 910/2014 (eIDAS)
7. Το γεγονός ότι από τις διατάξεις της παρούσας απόφασης δεν προκαλείται δαπάνη σε βάρος του κρατικού προϋπολογισμού.
8. Την ανάγκη τροποποίησης των όρων και προϋποθέσεων για την παροχή υπηρεσιών εμπιστοσύνης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ) ως εγκεκριμένου παρόχου, σύμφωνα με τις διατάξεις του Κανονισμού ΕΕ 910/2014 (eIDAS), προκειμένου να αναβαθμιστούν οι υπηρεσίες που παρέχει και συγκεκριμένα:

α. Η υπηρεσία της εξ αποστάσεως ταυτοποίησης,

β. Η διασύνδεση με το Μητρώο Πολιτών,

γ. Η ανάκληση του πιστοποιητικού σε περίπτωση αδυναμίας λειτουργίας της εφαρμογής, λόγω αιφνίδιου και απρόβλεπτου γεγονότος και

δ. Η δυνατότητα έκδοσης εγκεκριμένων πιστοποιητικών ηλεκτρονικής υπογραφής μέσω εξ αποστάσεως (απομακρυσμένης) συσκευής (Εγκεκριμένης Διάταξης Δημιουργίας Υπογραφής).

Ιστορικό εκδόσεων

Ημερομηνία	Έκδοση	Μεταβολές
15/12/2021	1.0	Αρχικό έγγραφο
24/4/2024	1.1	Προσθήκη υπηρεσίας εξ αποστάσεως ταυτοποίησης, απομακρυσμένης ΕΔΔΥ, διαλειτουργικότητας με μητρώο πολιτών, διορθώσεις τυπογραφικών λαθών

1. Εισαγωγή

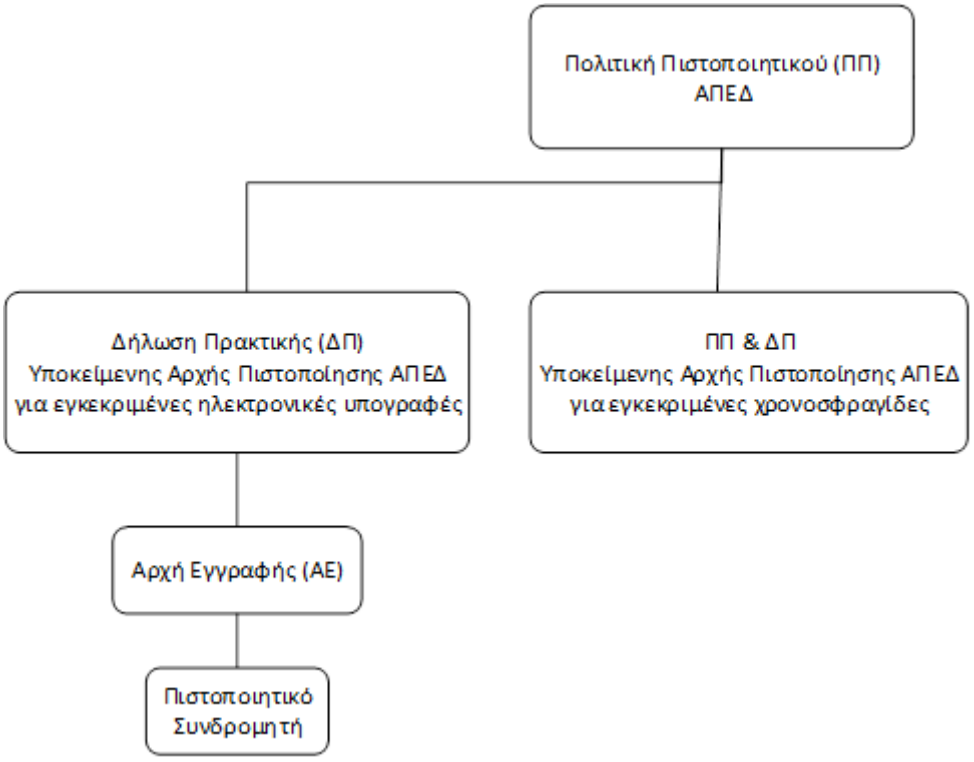
Η παρούσα αποτελεί τον Κανονισμό Πιστοποίησης της ΑΡΧΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ του ΕΛΛΗΝΙΚΟΥ ΔΗΜΟΣΙΟΥ – ΑΠΕΔ, του άρθρου 58 του ν. 4727/2020, όπως τροποποιήθηκε με το άρθρο 164 του ν. 4808/2021, με την οποία καθορίζονται οι όροι και οι προϋποθέσεις για την παροχή των υπηρεσιών εμπιστοσύνης από την ΑΠΕΔ, στη δομή της οποίας περιλαμβάνονται η Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ), οι Υποκείμενες Αρχές Πιστοποίησης (ΥπΑΠ), οι Αρχές Εγγραφής και τα Εντεταλμένα Γραφεία, προς το σκοπό της εν γένει παροχής υπηρεσιών εμπιστοσύνης του Ελληνικού Δημοσίου, μέσω της Υποδομής Δημοσίου Κλειδιού της ΑΠΕΔ, η οποία αναλύεται στα επιμέρους κεφάλαια του παρόντος. Η ΑΠΕΔ είναι αρμόδια για την έκδοση και διαχείριση πιστοποιητικών για την παροχή υπηρεσιών εμπιστοσύνης σε όλους τους φορείς του δημοσίου τομέα, καθώς και σε φυσικά ή νομικά πρόσωπα ή νομικές οντότητες.

Ο Κανονισμός Πιστοποίησης καθορίζει την Πολιτική Πιστοποιητικού της ΑΠΕΔ (Ενότητα Α), τη Δήλωση Πρακτικής των Υποκείμενων Αρχών Πιστοποίησης της ΑΠΕΔ (Ενότητα Β), εξειδικεύει τους όρους και τις προϋποθέσεις για την παροχή Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης σύμφωνα με την Πολιτική Πιστοποιητικού της ΑΠΕΔ και επιπλέον καθορίζει την Πολιτική Πιστοποιητικού και τη Δήλωση Πρακτικής της (Υποκείμενης) Αρχής Χρονοσφραγίδας (Ενότητα Γ).

Ειδικότερα, τα πιστοποιητικά υπηρεσιών εμπιστοσύνης της ΑΠΕΔ αποτελούν ηλεκτρονικές βεβαιώσεις, με τα οποία: α) καθίσταται δυνατή η χρήση υπηρεσιών εμπιστοσύνης από τον κάτοχο αυτού και β) ταυτοποιείται ο κάτοχος του πιστοποιητικού μέσω της επιβεβαίωσης του ονόματος ή του ψευδωνύμου του. Το περιεχόμενο και οι απαιτήσεις των εγκεκριμένων πιστοποιητικών ορίζονται στον Κανονισμό eIDAS και τα Παραρτήματα αυτού, ενώ η ισχύς του πιστοποιητικού άρχεται από την ημερομηνία που αναγράφεται πάνω σε αυτό και σε κάθε περίπτωση όχι νωρίτερα από την καταχώριση των δεδομένων του κατόχου, κατά τη διαδικασία ηλεκτρονικής ταυτοποίησης του άρθρου 57 του ν. 4727/2020, στη βάση δεδομένων που τηρεί ο πάροχος υπηρεσιών εμπιστοσύνης. Τέλος, η ισχύς του πιστοποιητικού λήγει: α) με την παρέλευση της ημερομηνίας λήξης που αναγράφεται πάνω σε αυτό, ή β) κατόπιν ανάκλησης του πιστοποιητικού σύμφωνα με το άρθρο 55 του ιδίου νόμου.

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

Στον παρόντα Κανονισμό ορίζεται η Πολιτική Πιστοποιητικού της ΑΠΕΔ καθώς και η Δήλωση Πρακτικής των Υποκείμενων Αρχών Πιστοποίησης. Η ιεραρχία της ΥΔΚ της ΑΠΕΔ απεικονίζεται στο σχήμα που ακολουθεί.



Σημειώνεται ότι ο όρος ΥπΑΠ και εκδότριες ΑΠ αναφέρεται στις Αρχές Πιστοποίησης που έχουν ως Πρωτεύουσα Αρχή Πιστοποίησης την ΑΠΕΔ

Α. Πολιτική Πιστοποιητικού της ΑΠΕΔ

1. Εισαγωγή

Στην παρούσα Πολιτική Πιστοποιητικού (ΠΠ) καθορίζεται η πολιτική πιστοποιητικών της ΑΠΕΔ, οι όροι και οι προϋποθέσεις για την ανάθεση και υποστήριξη ή παροχή υπηρεσιών εμπιστοσύνης σε φορείς - Παρόχους Υπηρεσιών Εμπιστοσύνης, οι οποίοι υποχρεούνται να εφαρμόζουν το παρόν νομικό, τεχνικό και λειτουργικό πλαίσιο παροχής υπηρεσιών εμπιστοσύνης.
Σε κάθε περίπτωση, η ΑΠΕΔ μεριμνά και λαμβάνει τα αναγκαία μέτρα για την εφαρμογή 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 έκδοση, τη διατήρηση και τη διαχείριση του κύκλου ζωής των εγκεκριμένων πιστοποιητικών ηλεκτρονικής υπογραφής και ηλεκτρονικών χρονοσφραγίδων και την παροχή των σχετικών υπηρεσιών εμπιστοσύνης 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 Συνδρομητών (Τελικών Χρηστών) και των Βασιζόμενων Μερών.
- Τα θέματα που αφορούν στους Γενικούς Όρους και Προϋποθέσεις Χρήσης Πιστοποιητικών.

- Τις μεθόδους που χρησιμοποιούνται για την επιβεβαίωση της ταυτότητας των Συνδρομητών.
- Τις λειτουργικές διαδικασίες ως προς τις υπηρεσίες κύκλου ζωής Πιστοποιητικού Συνδρομητή: υποβολή αιτήματος για έκδοση, αποδοχή και ανάκληση κλειδιών 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 δημοσίευσής τους. Τα έγγραφα που δε διατίθενται προς δημοσίευση αποτελούν εμπιστευτικό υλικό της ΑΠΕΔ.

Πίνακας 1: Διαθέσιμα Έγγραφα Κανονισμών

Έγγραφα	Κατάσταση	Τοποθεσία Δημοσίευσης για το Κοινό
Κανονισμός Πιστοποίησης της ΑΠΕΔ	Δημόσιο	Χώρος Αποθήκευσης της ΑΠΕΔ, σύμφωνα με την §2.2 της ΠΠ
Όροι και Προϋποθέσεις Χρήσης Πιστοποιητικών	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 τη 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 Πολιτική Εγκεκριμένων Πιστοποιητικών Ηλεκτρονικών Υπογραφών

Η συγκεκριμένη Πολιτική Πιστοποιητικού αναφέρεται σε Εγκεκριμένα Πιστοποιητικά ηλεκτρονικών υπογραφών συνδρομητών.
Τα πιστοποιητικά που εκδίδονται βάσει της συγκεκριμένης ΠΠ είναι κατάλληλα για να υποστηρίξουν εγκεκριμένη ηλεκτρονική υπογραφή (σύμφωνα με το στ. 12 του άρθρου 3 του Κανονισμού ΕΕ 910/2014 (eIDAS)), η οποία βασίζεται σε Εγκεκριμένο Πιστοποιητικό και δημιουργείται από Εγκεκριμένη Διάταξη Δημιουργίας Υπογραφής (ΕΔΔΥ), οπότε και επέχει θέση ιδιόχειρης υπογραφής τόσο στο ουσιαστικό όσο και στο δικονομικό δίκαιο, σύμφωνα με το άρθρο 25 του ως άνω Κανονισμού και τα άρθρα 14, 15, 16 και 50 του ν. 4727/2020.
Η ΠΠ αντιστοιχεί στη δημόσια πολιτική πιστοποιητικών "QCP-n-qscd" όπως περιγράφεται στο πρότυπο ETSI *EN 319 411-2 V2.5.1 (2023-10)* του European Telecommunications Standards Institute - ETSI αναφορικά με τις Απαιτήσεις Πολιτικής για Αρχές Πιστοποίησης που εκδίδουν Εγκεκριμένα Πιστοποιητικά. Τα Πιστοποιητικά που εκδίδονται με βάση την ΠΠ πιστοποιούν την αντιστοιχία του φυσικού προσώπου (Συνδρομητή) με τα στοιχεία που αναφέρονται στο έγγραφο ταυτοποίησής του. Το ως άνω πρότυπο χρησιμοποιείται και στην περίπτωση της έκδοσης εγκεκριμένων πιστοποιητικών ηλεκτρονικής υπογραφής μέσω εξ αποστάσεως (απομακρυσμένης) ΕΔΔΥ
Η ταυτοποίηση των Συνδρομητών προϋποθέτει κατ' αρχήν, τη φυσική παρουσία τους ενώπιον αρμόδιων στελεχών σύμφωνα με τα προβλεπόμενα στην παρούσα πράξη, οι οποίοι ελέγχουν τα έγγραφα που τεκμηριώνουν την ταυτότητα του Συνδρομητή (§3.2.2). Εξάλλου, η ταυτοποίηση μπορεί να γίνει και εξ αποστάσεως, εφόσον πληρούνται οι όροι και οι προϋποθέσεις της υπ' αριθμ. 27499 ΕΞ 2021 Απόφασης του Υπουργού Επικρατείας (ΦΕΚ 3682/Β'/10-8-2021)

Τα Εγκεκριμένα Πιστοποιητικά Συνδρομητών αναφέρονται αποκλειστικά και μόνο σε φυσικά πρόσωπα. Σε κάθε περίπτωση το Εγκεκριμένο Πιστοποιητικό συνδέεται κατ` αποκλειστικότητα με ένα φυσικό πρόσωπο, το οποίο και φέρει την αποκλειστική ευθύνη για αυτό το πιστοποιητικό.
Το αναγνωριστικό για την Πολιτική Πιστοποιητικού (Certificate Policy Identifier) που αντιστοιχεί στην Πολιτική Πιστοποιητικού είναι το: 1.2.300.0.110001.2.1.1.

1.3 Συμμετέχοντες στην Υποδομή Δημοσίου Κλειδιού

Η παρούσα ΠΠ διέπει τις υπηρεσίες Υποδομής Δημοσίου Κλειδιού που παρέχονται από την ΑΠΕΔ.

1.3.1 Αρχές Πιστοποίησης

Η ΑΠΕΔ μπορεί να εντάξει στην παρούσα Υποδομή Δημόσιου Κλειδιού άλλες δημόσιες υπηρεσίες ή φορείς του δημόσιου τομέα (Υποκείμενες Αρχές Πιστοποίησης), οι οποίες ακολουθούν την Πολιτική Πιστοποιητικού της ΑΠΕΔ.
Οι Υποκείμενες Αρχές Πιστοποίησης (ΥπΑΠ), εφόσον ορισθούν με ΚΥΑ του ΥΨΗΔ και του αρμόδιου Υπουργού και ενταχθούν στην Υποδομή Δημοσίου Κλειδιού, βάσει του ν. 4727, αρ. 107, παρ. 37 και των διατάξεων του παρόντος, ελέγχονται από τον Οργανισμό Αξιολόγησης Συμμόρφωσης (ΟΑΣ), εγκρίνονται από την ΕΕΤΤ και, εφόσον απαιτείται, εγγράφονται στον Κατάλογο Εμπιστοσύνης της ΕΕΤΤ. Η διαχείριση των πιστοποιητικών που θα εκδίδουν οι ΥπΑΠ θα γίνεται από την ΑΠΕΔ.
Επίσης, με όμοια ΚΥΑ του ΥΨΗΔ και του αρμόδιου Υπουργού ορίζονται μία 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 §1.3.3). Οι ΥπΑΠ μπορούν να ασκήσουν και αρμοδιότητες της Αρχής Εγγραφής και των Εντεταλμένων Γραφείων όπως αυτές ορίζονται στις ενότητες §1.3.2 και §1.3.3.

1.3.2 Αρχές Εγγραφής

Οι Αρχές Εγγραφής (ΑΕ) προκειμένου για τη χορήγηση των εγκεκριμένων πιστοποιητικών ηλεκτρονικής υπογραφής σύμφωνα με τις διατάξεις του παρόντος, είναι αρμόδιες για τον έλεγχο των αιτημάτων και των εγγραφών των Συνδρομητών, και για την επιβεβαίωση των στοιχείων της ταυτότητας των Συνδρομητών. Επιπλέον, οι ΑΕ ελέγχουν και εισηγούνται την έκδοση και ανάκληση κλειδιών Πιστοποιητικών.

1.3.3 Εντεταλμένα Γραφεία (ΕΓ)

Σε κάθε Αρχή Εγγραφής απευθύνεται ένας αριθμός Εντεταλμένων Γραφείων, τα στελέχη των οποίων είναι αρμόδια για την επιβεβαίωση - επαλήθευση των στοιχείων ταυτότητας των Συνδρομητών καθώς και την παραλαβή των αιτημάτων για έκδοση και ανάκληση κλειδιών Πιστοποιητικών και αναφέρονται στην προϊσταμένη Αρχή (ή Αρχές) Εγγραφής.

1.3.4 Συνδρομητές (Τελικοί Χρήστες)

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

1.3.5 Βασιζόμενα Μέρη

Ως Βασιζόμενα Μέρη νοούνται τα φυσικά ή νομικά πρόσωπα που ενεργούν βάσει εμπιστοσύνης σε κάποιο Πιστοποιητικό που έχει εκδοθεί σύμφωνα με τις διατάξεις του παρόντος. Το Βασιζόμενο Μέρος μπορεί να είναι, ή και να μην είναι, Συνδρομητής εντός της ΥΔΚ της ΑΠΕΔ.

1.4 Εφαρμογή των Πιστοποιητικών

1.4.1 Εγκεκριμένες Χρήσεις Πιστοποιητικών

Τα Πιστοποιητικά που ακολουθούν την ΠΠ σύμφωνα με τις διατάξεις της παρούσας, αποτελούν Εγκεκριμένα Πιστοποιητικά Ηλεκτρονικής Υπογραφής κατά την έννοια του στ. 15) του άρθρου 3 του Κανονισμού 910/2014.
Τα Πιστοποιητικά Συνδρομητών που εκδίδονται για φυσικά πρόσωπα είναι αυστηρώς προσωπικά και χρησιμοποιούνται στο πλαίσιο που προβλέπεται από τις Δηλώσεις Πρακτικής των ΥπΑΠ.

Οι εφαρμογές στις οποίες μπορούν να χρησιμοποιηθούν τα Πιστοποιητικά Συνδρομητών που θα παρασχεθούν βάσει της Υποδομής Δημοσίου Κλειδιού του παρόντος και με την χρήση εγκεκριμένης ηλεκτρονικής υπογραφής, όπου απαιτείται, δύνανται να είναι αποκλειστικά μία ή περισσότερες από τις εξής:

- Έλεγχος πρόσβασης
- Ασφαλής προσδιορισμός υπογράφοντος
- Προσδιορισμός του Υπευθύνου για κάθε σχετική ηλεκτρονική επικοινωνία / συναλλαγή
- Υπογραφή ηλεκτρονικών αρχείων (π.χ. αρχεία Adobe Acrobat)

1.4.1.1 Περιορισμοί στη χρήση των πιστοποιητικών

Τα πιστοποιητικά που είναι σύμφωνα με τη ΠΠ έχουν περιορισμούς στη χρήση τους όπως ορίζεται στην §1.4.1 του παρόντος. Σε κάθε περίπτωση οι διατάξεις του παρόντος δεν θίγουν διατάξεις που, αναφορικά με τη σύναψη και την ισχύ συμβάσεων ή εν γένει νομικών υποχρεώσεων, δεν επιβάλλουν τη χρήση ορισμένου τύπου, ούτε θίγουν διατάξεις για την αποδεικτική ή άλλη χρήση εγγράφων ή διατάξεις με τις οποίες απαγορεύεται να διακινούνται και να καθίστανται γνωστά έγγραφα ορισμένων κατηγοριών ή/και δεδομένα προσωπικού χαρακτήρα.

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. 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 στην ιστοσελίδα: http://www.aped.gov.gr.

1.5.3 Έγκριση Καταλληλότητας Δήλωσης Πρακτικής για την Πολιτική Πιστοποιητικών

Η ΑΠΕΔ εξετάζει και εγκρίνει τις Δηλώσεις Πρακτικής των ΥπΑΠ αναφορικά με την καταλληλότητα και συμμόρφωσή 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 τροποποιήσεών τους με την παρούσα ΠΠ.

1.6 Ορισμοί και ακρωνύμια

Στο κεφάλαιο 3 (Παράρτημα Α) παρατίθενται πίνακες Πηγών, 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. Οι εκδότριες ΑΠ διασφαλίζουν επίσης ένα δημοσίως προσβάσιμο ηλεκτρονικό χώρο αποθήκευσης για τις υπηρεσίες ΥΔΚ που προσφέρουν.
Η ΑΠΕΔ διασφαλίζει ότι ο χώρος αποθήκευσής της είναι διαθέσιμος 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα, με ελάχιστη συνολική διαθεσιμότητα 99,00% ανά έτος με τις προγραμματισμένες διακοπές λειτουργίας να μην υπερβαίνουν το ποσοστό του 0,3% ετησίως. Σε περίπτωση βλάβης του συστήματος, εργασιών συντήρησης ή άλλων παραγόντων που δεν υπόκεινται στον έλεγχο της ΑΠΕΔ, θα καταβληθεί κάθε δυνατή προσπάθεια προκειμένου να διασφαλίσει ότι η μη διαθεσιμότητα της συγκεκριμένης υπηρεσίας πληροφοριών δεν θα υπερβαίνει τον ανωτέρω δηλωθέντα χρόνο.

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 στα Βασιζόμενα Μέρη 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 συνδρομητών που έχει εκδώσει.
Με την ανάκληση ενός Πιστοποιητικού ΥπΑΠ η ΑΠΕΔ δημοσιεύει αναγγελία της ανάκλησης αυτής στο χώρο αποθήκευσής τους. Με την ανάκληση ενός Πιστοποιητικού Συνδρομητή, 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 στο δικτυακό της κόμβο την παρούσα ΠΠ, τη Δήλωση Πρακτικής της, τους Όρους και Προϋποθέσεις Χρήσης Πιστοποιητικού (ΟΧΠ).
Τέλος, οι εκδότριες ΑΠ δημοσιεύουν τα Πιστοποιητικά Συνδρομητών 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 στα Βασιζόμενα Μέρη πληροφορίες σχετικά με την τοποθεσία δημοσίευσης και τον τρόπο αναζήτησης των Πιστοποιητικών Συνδρομητών που εκδίδουν.

2.2.1 Δημοσίευση της ΠΠ

Η παρούσα ΠΠ δημοσιεύεται σε ηλεκτρονική μορφή στο Χώρο Αποθήκευσης της ΑΠΕΔ στη διεύθυνση https://pki.aped.gov.gr/repository, όπου βρίσκεται διαθέσιμη σε μορφή εγγράφου Adobe Acrobat®.

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 ένα χρονικό διάστημα 30 ημερών, στο τμήμα του Χώρου Αποθήκευσής της που προορίζεται για Ενημερώσεις και Ανακοινώσεις επί των Πολιτικών, στις διευθύνσεις που αναφέρονται στην ενότητα §2.2.1.
Τα Πιστοποιητικά Συνδρομητών δημοσιεύονται κατά την έκδοση, σύμφωνα με τα αναφερόμενα στην §2.2. 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 και Προϋποθέσεων Χρήσης Πιστοποιητικού, 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 την Πολιτική Πιστοποιητικού της ΑΠΕΔ, επαληθεύονται.

3.1.1 Τύποι Ονομάτων

Τα Πιστοποιητικά που εκδίδει η ΑΠΕΔ για την πιστοποίηση των ΥπΑΠ, περιλαμβάνουν Διακριτικά Ονόματα Χ.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"
Organization (O) - Οργανισμός =	“HELLENIC PUBLIC ADMINISTRATION CERTIFICATION AUTHORITY”
Common Name (CN) – Κοινό Όνομα =	Το χαρακτηριστικό αυτό περιλαμβάνει το Κοινό Όνομα της ΥπΑΠ (CA name): "APED Qualified eSignature Issuing CA".

Τα Πιστοποιητικά Συνδρομητή που εκδίδονται σύμφωνα με τις πολιτικές πιστοποίησης που ορίζονται στην παρούσα ΠΠ περιλαμβάνουν διακριτικό όνομα Χ.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 Συνδρομητή

Χαρακτηριστικό	Τιμή
Country (C) - Χώρα=	"GR"
Common Name (CN)− Κοινό Όνομα =	Τα χαρακτηριστικό αυτό περιλαμβάνει το όνομα και το επώνυμο (ένα ή περισσότερα) του Συνδρομητή
Surname (SN) – Επώνυμο =	Τα χαρακτηριστικό αυτό περιλαμβάνει το επώνυμο (ένα ή περισσότερα) του Συνδρομητή με λατινικούς χαρακτήρες (με χρήση του προτύπου ΕΛΟΤ 743, εκτός και αν αναγράφεται με διαφορετικό τρόπο στο προσκομισθέν κατά την εγγραφή έγγραφο ταυτοποίησης – νομιμοποιητικό έγγραφο).
Given name (G) – Όνομα =	Το χαρακτηριστικό αυτό περιλαμβάνει το όνομα (ή ονόματα) του Συνδρομητή με λατινικούς χαρακτήρες (με χρήση του προτύπου ΕΛΟΤ 743, εκτός και αν αναγράφεται με διαφορετικό τρόπο στο προσκομισθέν κατά την εγγραφή έγγραφο ταυτοποίησης – νομιμοποιητικό έγγραφο).
Serial Number – Σειριακός Αριθμός =	Το χαρακτηριστικό αυτό περιλαμβάνει τον Σειριακό Αριθμό του Πιστοποιητικού του Συνδρομητή σύμφωνα με το πρότυπο ETSI EN 319 412-1

3.1.2 Ανάγκη Κατανόησης των Ονομάτων

Τα ονόματα που περιλαμβάνονται στα Πιστοποιητικά Συνδρομητή βρίσκονται σε μορφή απλή και κατανοητή ώστε να επιτρέπουν τον προσδιορισμό της ταυτότητας του φυσικού προσώπου που αποτελεί το Υποκείμενο του Πιστοποιητικού.
Τα Πιστοποιητικά της ΑΠ της ΑΠΕΔ περιλαμβάνουν ονόματα με ευρέως κατανοητή σημασιολογία δίνοντας τη δυνατότητα να προσδιοριστεί η ταυτότητα της ΑΠ που αποτελεί το Υποκείμενο του Πιστοποιητικού.

3.1.3 Ανωνυμία ή ψευδωνυμία συνδρομητών

Δεν εφαρμόζεται.

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 Συνδρομητών.
Η μοναδικότητα του Διακριτικού Ονόματος για ηλεκτρονικές υπογραφές και έλεγχο ταυτότητας εξασφαλίζεται από την τιμή χαρακτηριστικού γνωρίσματος του Σειριακού Αριθμού στο πεδίο Θέμα του πιστοποιητικού.

3.2 Αρχική Εγγραφή

Η επαλήθευση ταυτότητας αποτελεί μέρος της διαδικασίας αίτησης και έκδοσης πιστοποιητικού.

3.2.1 Μέθοδος Απόδειξης της Κατοχής Ιδιωτικού Κλειδιού

Ο Αιτών Πιστοποιητικό πρέπει να αποδείξει ότι νόμιμα κατέχει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που αναγράφεται στο Πιστοποιητικό. Η μέθοδος απόδειξης της κατοχής του ιδιωτικού κλειδιού είναι σύμφωνα με το PKCS #10 (Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού) ή άλλη ισοδύναμη κρυπτογραφικά μορφή ή άλλη μέθοδος αποδεκτή από την ΑΠΕΔ.

3.2.2 Μέθοδος Απόδειξης της Ταυτότητας Φυσικού Προσώπου

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

- Ο Συνδρομητής είναι το πρόσωπο που προσδιορίζεται στην Ηλεκτρονική Εγγραφή ή Αίτηση για Πιστοποιητικό.

Η πιστοποίηση της ταυτότητας (ταυτοποίηση) του Συνδρομητή γίνεται είτε με την προσωπική (φυσική) του παρουσία ενώπιον στελέχους του Εντεταλμένου Γραφείου, ή όπου αυτό κρίνεται απαραίτητο, ενώπιον της Αρχής Εγγραφής, ή της Εκδότριας ΑΠ, με σκοπό τον έλεγχο των στοιχείων της ταυτότητάς του, είτε εξ αποστάσεως, εφόσον πληρούνται οι όροι και οι προϋποθέσεις της υπ' αριθμ. 27499 ΕΞ 2021 Απόφασης του Υπουργού Επικρατείας (ΦΕΚ 3682/Β'/10-8-2021)

- Αποδεκτά έγγραφα φυσικής ταυτοποίησης είναι:
  i. Δελτίο Αστυνομικής Ταυτότητας (Ελληνικής ή άλλου κράτους της Ευρωπαϊκής Ένωσης)
  ii. Ελληνική Στρατιωτική (ΓΕΣ, ΓΕΝ, ΓΕΑ, Σώματα Ασφαλείας)
  iii. Διαβατήριο.
- Αποδεκτά έγγραφα εξ αποστάσεως ταυτοποίησης είναι τα παρακάτω, εφόσον πληρούν τις προϋποθέσεις του αρ. 4, παρ 1, 2, της υπ' αριθμ. 27499 ΕΞ 2021 Απόφασης του Υπουργού Επικρατείας (ΦΕΚ 3682/Β'/10-8-2021):
  i. Δελτίο Αστυνομικής Ταυτότητας (Ελληνικής ή άλλου κράτους της Ευρωπαϊκής Ένωσης)
  ii. Ελληνική Στρατιωτική (ΓΕΣ, ΓΕΝ, ΓΕΑ, Σώματα Ασφαλείας)
  iii. Διαβατήριο.

  Ειδικά για το διάστημα μέχρι 24/9/2024, γίνονται αποδεκτά το ισχύον αστυνομικό δελτίο ταυτότητας, στο οποίο το ονοματεπώνυμο αναγράφεται και με λατινικούς χαρακτήρες (GRC-BO-01004, GRC-BO-01005, GRC-BO-02001), τα δελτία ταυτότητας των στελεχών των Ενόπλων Δυνάμεων και των Σωμάτων Ασφαλείας.
  Ο αναλυτικός κατάλογος των αποδεκτών εγγράφων εξ αποστάσεως ταυτοποίησης είναι αναρτημένος στη σελίδα της ΑΠΕΔ www.aped.gov.gr

Η διαδικασία ταυτοποίησης περιγράφεται παρακάτω:

- Ο συνδρομητής ενημερώνεται αναλυτικά για τη διαδικασία στο https://www.aped.gov.gr. Εκεί υπάρχουν σύνδεσμοι για δύο αρχικά βήματα:
  - (1) σύνδεσμος στην αίτηση – Υπεύθυνη Δήλωση (ΥΔ) στο gov.gr,
  - (2) σύνδεσμος για το portal https://services.aped.gov.gr/apedcitizen/login
- Ο συνδρομητής μεταβαίνει στο gov.gr στην αίτηση – Υπεύθυνη Δήλωση (ΥΔ) για έκδοση ΨΠ και τη δημιουργεί.
  - Η αίτηση-ΥΔ στο gov.gr έχει τυποποιημένο κείμενο. Ο χρήστης την επιλέγει, αυθεντικοποιείται (έλεγχος ταυτότητας δύο παραγόντων, με χρήση του πιστοποιημένου κινητού τηλεφώνου), συμπληρώνει τα πεδία ταυτοποίησης και τη δημιουργεί.
    - Στην αίτηση περιλαμβάνονται επιπλέον ενότητες (κείμενο μόνο): ενημέρωση για επεξεργασία δεδομένων προσωπικού χαρακτήρα, και ορισμένοι βασικοί όροι χρήσης και παραπομπή στο κείμενο των όρων χρήσης.
- Ο συνδρομητής υποβάλλει το αίτημα στο portal της ΑΠΕΔ.
  - Ο πολίτης αποκτά πρόσβαση στην ηλεκτρονική εφαρμογή στο portal https://services.aped.gov.gr/apedcitizen/login με τη χρήση των κωδικών-διαπιστευτηρίων που διαθέτει μέσω της Γενικής Γραμματείας Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Υπουργείου Ψηφιακής Διακυβέρνησης.
  - Υποβάλλει αίτημα έκδοσης ΨΠ.
    - Τα βασικά πεδία είναι προσυμπληρωμένα (ανάκτηση από το web service της ΑΑΔΕ).
    - Συμπληρώνει προαιρετικά στοιχεία επικοινωνίας: email, διεύθυνση κατοικίας.
    - Συμπληρώνει τον μοναδικό αναγνωριστικό αριθμό επαλήθευσης (κωδικάριθμο) της αίτησης-ΥΔ του gov.gr.
    - Επιλέγει:
      i. Φυσική ταυτοποίηση ή
      ii. Εξ αποστάσεως ταυτοποίηση
    - Καλείται να επιβεβαιώσει (τσεκάρει) ότι έχει διαβάσει τους όρους χρήσης.
    - Υποβάλλει την ηλεκτρονική αίτηση («αίτημα στο portal της ΑΠΕΔ»). Γίνεται αυτόματα έλεγχος στα βασικά πεδία (όνομα, επώνυμο, ΑΦΜ) ανάμεσα σε ανακτηθέντα στοιχεία ΑΑΔΕ και αίτησης-ΥΔ του gov.gr. Η ηλεκτρονική αίτηση και η αίτηση-ΥΔ του gov.gr αποθηκεύονται στη βάση δεδομένων.

Διακρίνονται οι παρακάτω περιπτώσεις:

i. Φυσική ταυτοποίηση
   - Ο συνδρομητής μεταβαίνει σε οποιοδήποτε Εντεταλμένο Γραφείο (ΕΓ) για να γίνει η φυσική ταυτοποίηση.
   - Ο υπάλληλος ΕΓ αυθεντικοποιείται στο portal της ΑΠΕΔ με τη χρήση των κωδικών Δημόσιας Διοίκησης της Γενικής Γραμματείας Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Υπουργείου Ψηφιακής Διακυβέρνησης σύμφωνα με όσα ορίζονται στην υπ' αρ. 29810 ΕΞ/23.10.2020 απόφαση του Υπουργού Επικρατείας, εφόσον πρόκειται για Δημόσιο Υπάλληλο, αλλιώς με τη χρήση των κωδικών-διαπιστευτηρίων που διαθέτει μέσω της Γενικής Γραμματείας Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Υπουργείου Ψηφιακής Διακυβέρνησης (TaxisNet)
   - Ο υπάλληλος ΕΓ αναζητά και εντοπίζει το συνδρομητή. Μεταφέρεται στη σελίδα με τα στοιχεία της αίτησης. Από εκεί μπορεί να δει την αίτηση-ΥΔ του gov.gr.
   - Ο υπάλληλος ΕΓ ταυτοποιεί το συνδρομητή και επιβεβαιώνει την ορθότητα των στοιχείων της αίτησης του gov.gr.
   - Ο υπάλληλος ΕΓ κάνει και αντιπαραβολή ανάμεσα στα ανακτηθέντα στοιχεία από το Φορολογικό Μητρώο της Α.Α.Δ.Ε./ ΓΓΠΣΨΔ (όνομα, επώνυμο, ΑΦΜ) και στα αντίστοιχα στην αίτηση - ΥΔ του gov.gr. Αν δεν υπάρχει ταύτιση ακυρώνεται το αίτημα.
   - Ο υπάλληλος διορθώνει, αν απαιτείται, τα πεδία που μπορεί να επεξεργαστεί (ονοματεπώνυμο (λατινικά), διεύθυνση, email). Η λατινική γραφή του ονοματεπωνύμου θα είναι ίδια με αυτή που αναφέρεται στο έγγραφο ταυτοποίησης.

- Το αναγνωριστικό του εγγράφου ταυτοποίησης (ταυτότητα ή διαβατήριο) εισάγεται αυτόματα από την αίτηση – ΥΔ του gov.gr. Το έγγραφο ταυτοποίησης πρέπει να είναι το ίδιο με αυτό που έχει εισαγάγει στην αίτηση – ΥΔ του gov.gr ο συνδρομητής και είναι είτε αστυνομική ταυτότητα (Ελληνική ή άλλου κράτους της Ευρωπαϊκής Ένωσης) είτε Ελληνική Στρατιωτική είτε διαβατήριο.
- Η αίτηση για ΨΠ έχει ένα μοναδικό αναγνωριστικό (αντίστοιχο του αριθμού πρωτοκόλλου) το οποίο και εμφανίζεται στον υπάλληλο ΕΓ. Δεν τυπώνεται η αίτηση για ΨΠ ούτε αποδεικτικό παραλαβής.
- Ο υπάλληλος ΕΓ επιλέγει υποβολή του αιτήματος. Εάν το έγγραφο ταυτοποίησης είναι Ελληνική Αστυνομική Ταυτότητα ή Ελληνικό Διαβατήριο γίνεται έλεγχος μέσω του Κέντρου Διαλειτουργικότητας στο Μητρώο Δελτίων Αστυνομικών Ταυτοτήτων ή στο Μητρώο Διαβατηρίων, αντίστοιχα, της Ελληνικής Αστυνομίας. Εάν πρόκειται για Ελληνική Στρατιωτική Ταυτότητα (ΓΕΣ, ΓΕΝ, ΓΕΑ, Σώματα Ασφαλείας), εφόσον έχει ενσωματωθεί στην εφαρμογή η σχετική υπηρεσία, γίνεται έλεγχος μέσω του Κέντρου Διαλειτουργικότητας, με το αντίστοιχο μητρώο Στρατιωτικών Ταυτοτήτων
- Εφόσον ολοκληρωθεί επιτυχώς ο έλεγχος ή πρόκειται για άλλο έγγραφο ταυτοποίησης για το οποίο δεν υπάρχει διαθέσιμη υπηρεσία ελέγχου, ο υπάλληλος υπογράφει ψηφιακά τη Βεβαίωση Φυσικής Ταυτοποίησης του συνδρομητή.
- Η διαδικασία φυσικής ταυτοποίησης ολοκληρώνεται εάν και μόνο εάν ο έλεγχος του εγγράφου ταυτοποίησης αποφανθεί ότι το εν λόγω έγγραφο ταυτοποίησης είναι ενεργό (στις κατηγορίες εγγράφων που εμπίπτουν σε αυτόν τον έλεγχο) και υπογραφεί ψηφιακά η σχετική βεβαίωση από το ΕΓ. Αυτόματα αποστέλλεται SMS στο κινητό τηλέφωνο του συνδρομητή που ενημερώνει ότι ολοκληρώθηκε επιτυχώς η φυσική ταυτοποίηση.
- Στη βάση δεδομένων της ΑΠΕΔ αποθηκεύεται η Βεβαίωση ταυτοποίησης. Στην εφαρμογή της ΑΠΕΔ, στην οθόνη διαχείρισης ΨΠ του συνδρομητή, αναγράφεται ότι έχει γίνει η ταυτοποίηση από Εντεταλμένο Γραφείο καθώς και ο μοναδικός αναγνωριστικός αριθμός.
- Σε περίπτωση αποτυχίας της ταυτοποίησης ο υπάλληλος καταγράφει το λόγο της απόρριψης. Ο Συνδρομητής λαμβάνει SMS που τον παραπέμπει στην εφαρμογή της ΑΠΕΔ για να ενημερωθεί για το λόγο απόρριψης

ii. Εξ αποστάσεως ταυτοποίηση (σύμφωνα με Υ.Α 27499 ΕΞ 2021 /10-08-2021 άρθρο 3 παρ.2)

- Ο αρμόδιος υπάλληλος του ΕΓ αυθεντικοποιείται στο portal της ΑΠΕΔ με τη χρήση των κωδικών-διαπιστευτηρίων που διαθέτει μέσω της Γενικής Γραμματείας Πληροφοριακών Συστημάτων και Ψηφιακής Διακυβέρνησης του Υπουργείου Ψηφιακής Διακυβέρνησης (TaxisNet)
- Ο αρμόδιος υπάλληλος του ΕΓ πραγματοποιεί την εξ αποστάσεως ταυτοποίηση.
- Η εφαρμογή ελέγχει μέσω διαλειτουργικότητας, όπως αναφέρεται παραπάνω στη φυσική ταυτοποίηση, την εγκυρότητα του εγγράφου ταυτοποίησης.
- Εφόσον ολοκληρωθεί επιτυχώς η ταυτοποίηση, δημιουργείται Βεβαίωση Ταυτοποίησης στην οποία τοποθετείται η προηγμένη ή εγκεκριμένη ηλεκτρονική σφραγίδα του παρόχου της υπηρεσίας της εξ αποστάσεως ταυτοποίησης ή η εγκεκριμένη ηλεκτρονική υπογραφή του υπαλλήλου που πραγματοποίησε την εξ αποστάσεως ταυτοποίησης. Αυτόματα αποστέλλεται SMS στο κινητό τηλέφωνο του Συνδρομητή που ενημερώνει ότι ολοκληρώθηκε επιτυχώς η ταυτοποίηση
- Στη βάση δεδομένων της ΑΠΕΔ αποθηκεύεται η Βεβαίωση ταυτοποίησης. Στη βάση του παρόχου της υπηρεσίας της εξ αποστάσεως ταυτοποίησης αποθηκεύεται αντίγραφο του εγγράφου ταυτοποίησης και το βίντεο της ταυτοποίησης. Στην εφαρμογή της ΑΠΕΔ, στην οθόνη διαχείρισης ΨΠ του Συνδρομητή, αναγράφεται ότι έχει γίνει η ταυτοποίηση από Εντεταλμένο Γραφείο καθώς και ο μοναδικός αναγνωριστικός αριθμός.
- Σε περίπτωση αποτυχίας της ταυτοποίησης ο υπάλληλος καταγράφει το λόγο της απόρριψης. Ο Συνδρομητής λαμβάνει SMS που τον παραπέμπει στην εφαρμογή της ΑΠΕΔ για να ενημερωθεί για το λόγο απόρριψης

- Το αίτημα εγκρίνεται από την Αρχή Εγγραφής.
  - Το στέλεχος της ΑΕ πλοηγείται στην οθόνη «Αιτήματα Έκδοσης ΨΠ» και επιλέγει το αίτημα.
  - Ελέγχει τα στοιχεία της αίτησης του portal καθώς και την αίτηση – ΥΔ του gov.gr. Εφόσον διαπιστώσει ότι όλα είναι σωστά, εγκρίνει το αίτημα.

- Αν διαπιστώσει παρατυπία απορρίπτει το αίτημα και ο συνδρομητής ενημερώνεται με SMS. Στο portal ο συνδρομητής βλέπει την αιτιολογία απόρριψης, και ενημερώνεται για τις διορθωτικές ενέργειες που πρέπει να κάνει προκειμένου να υποβάλει εκ νέου το αίτημα.

  - Ο συνδρομητής ενημερώνεται με SMS στο κινητό τηλέφωνό του ότι εγκρίθηκε το αίτημα. Το μήνυμα περιέχει τον οκταψήφιο κωδικό έκδοσης/ανάκλησης.

- Ο συνδρομητής ακολουθώντας τις οδηγίες προχωρά σε έκδοση του εγκεκριμένου πιστοποιητικού.

Η αίτηση του πολίτη παραμένει ενεργή και σε εκκρεμότητα, για χρονικό διάστημα ενενήντα (90) ημερών από την υποβολή της, προκειμένου να ακολουθήσει εντός του ως άνω διαστήματος η ταυτοποίηση του αιτούντος εγκεκριμένο πιστοποιητικό είτε ενώπιον υπαλλήλου ΕΓ (φυσική ταυτοποίηση), είτε με την μέθοδο της εξ αποστάσεως ταυτοποίησης. Μετά την παρέλευση της ως άνω προθεσμίας άπρακτης, χωρίς δηλαδή, να ακολουθήσει η ταυτοποίηση του αιτούντος, σύμφωνα με τα ανωτέρω, η αίτηση αυτή διαγράφεται χωρίς να παράγει έννομα αποτελέσματα.

Καθ' όλη την διάρκεια της διαδικασίας για την έκδοση του ΨΠ, από την υποβολή της αίτησης έως την έγκρισή της από την ΑΕ, ελέγχεται αυτεπαγγέλτως το αν ο αιτών βρίσκεται στη ζωή, μέσω διαλειτουργικότητας με το Μητρώο Πολιτών. Σε περίπτωση που προκύψει κατά την υποβολή της αίτησης ότι ο αιτών δεν βρίσκεται στη ζωή, η διαδικασία για την έκδοση εγκεκριμένου πιστοποιητικού διακόπτεται και εμφανίζεται σχετικό μήνυμα στην οθόνη του αιτούντος. Το ίδιο συμβαίνει και κατά την εγκατάσταση του εγκεκριμένου πιστοποιητικού στην ΕΔΔΥ. Σε κάθε περίπτωση ο υπάλληλος του ΕΓ ο οποίος διενεργεί την ταυτοποίηση του αιτούντος την έκδοση (ή/και την ανάκληση) του εγκεκριμένου πιστοποιητικού αφού ελέγξει την εγκυρότητα του εγγράφου ταυτοποίησης του αιτούντος, λαμβάνει υπόψη το αποτέλεσμα του ελέγχου μέσω διαλειτουργικότητας με το Μητρώο Πολιτών, σχετικά με τυχόν ένδειξη θανάτου του αιτούντος. Εξάλλου, η ΑΕ διατηρεί το δικαίωμα ακύρωσης του εγκεκριμένου πιστοποιητικού σε περίπτωση κατά την οποία, μέσω διαλειτουργικότητας με το Μητρώο Πολιτών, προκύπτει στοιχείο θανάτου του Τελικού Χρήστη του εγκεκριμένου πιστοποιητικού (Συνδρομητή). Εάν εκ παραδρομής έχει προκύψει ψευδώς στοιχείο θανάτου του αιτούντος/Συνδρομητή, ο αιτών/Συνδρομητής απευθύνεται για τη διόρθωση της ένδειξης στο Μητρώο Πολιτών.

3.2.3 Πληροφορίες Συνδρομητή που Δεν Επαληθεύονται

Δεν υπάρχουν.

3.3 Ταυτοποίηση και Αυθεντικοποίηση για Επαναδημιουργία Κλειδιών

Επαναδημιουργία κλειδιών υποστηρίζεται μόνο για πιστοποιητικά που έχουν λήξει ή ανακληθεί. Η διαδικασία ταυτοποίησης περιγράφεται στην §3.2.2.

3.3.1 Ταυτοποίηση και Αυθεντικοποίηση για Τακτική Επαναδημιουργία Κλειδιών

Δεν εφαρμόζεται

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 Συνδρομητή για Πιστοποιητικά ανακαλύπτει ή έχει λόγο να πιστεύει ότι ορισμένα ουσιώδη στοιχεία στην Ηλεκτρονική Εγγραφή ή Αίτηση για Πιστοποιητικά είναι ψευδή.

- Υπό τους ανωτέρω όρους, τα Πιστοποιητικά Συνδρομητή, τα οποία έχουν ανακληθεί ή έχουν λήξει, είναι δυνατόν να αντικατασταθούν (να ξαναδημιουργηθούν τα ζεύγη κλειδιών), σύμφωνα με την §3.2.2

3.4 Ταυτοποίηση και Αυθεντικοποίηση για Αίτηση Ανάκλησης

Για την ανάκληση Πιστοποιητικών Συνδρομητή 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 (παρ. 4.9.3). Η υπηρεσία ανάκλησης είναι διαθέσιμη 7 ημέρες τη βδομάδα, όλο το εικοσιτετράωρο.

Για την επαλήθευση ταυτότητας αιτήματος ανάκλησης ενός Συνδρομητή ακολουθείται κατά περίπτωση μια από τις ακόλουθες αποδεκτές διαδικασίες:

- Ανάκληση με οκταψήφιο κωδικό
    - Στην περίπτωση αυτή ο ίδιος ο συνδρομητής κάνει την ανάκληση του πιστοποιητικού του χωρίς παρέμβαση / εμπλοκή της Αρχής Εγγραφής.
    - Ο συνδρομητής συνδέεται στο portal της ΑΠΕΔ και επιλέγει την ανάκληση του πιστοποιητικού του. Πρέπει να εισάγει τον μοναδικό οκταψήφιο κωδικό που δημιουργήθηκε όταν εγκρίθηκε το αίτημα έκδοσης και του είχε αποσταλεί με SMS στο κινητό τηλέφωνό του. Με την εισαγωγή του κωδικού και την υποβολή αιτήματος το πιστοποιητικό ακυρώνεται αυτόματα.
    - Αν ο συνδρομητής δεν έχει αποθηκεύσει τον οκταψήφιο κωδικό, μπορεί να γίνει υπενθύμιση. Στην περίπτωση αυτή εισάγει τον ΑΦΜ και την ημερομηνία γέννησής του και εφόσον αυτά τα στοιχεία επαληθευτούν, αποστέλλεται SMS με τον κωδικό στο κινητό τηλέφωνο που καταχωρήθηκε στην έκδοση του πιστοποιητικού. Αν έχει αλλάξει αριθμό κινητού τηλεφώνου, δεν μπορεί να γίνει τροποποίηση του καταχωρημένου κινητού τηλεφώνου και δεν μπορεί να λάβει τον κωδικό υπενθύμισης.
- Ανάκληση με αίτηση στο gov.gr
    - Η επιλογή αυτή χρησιμοποιείται αν ο συνδρομητής δεν έχει τον οκταψήφιο κωδικό και δεν μπορεί να γίνει υπενθύμιση επειδή έχει αλλάξει αριθμό κινητού τηλεφώνου.
    - Ο συνδρομητής πλοηγείται στο gov.gr, εντοπίζει την αίτηση ανάκλησης - Υπεύθυνη Δήλωση (ΥΔ), αυθεντικοποιείται (έλεγχος ταυτότητας δύο παραγόντων, με χρήση πιστοποιημένου κινητού τηλεφώνου) και τη δημιουργεί. Στην αίτηση-ΥΔ καταχωρείται ο νέος πιστοποιημένος αριθμός κινητού τηλεφώνου, με τη διαδικασία πιστοποίησης που διαθέτει ο δικτυακός τόπος του gov.gr
    - Ο συνδρομητής συνδέεται στο portal της ΑΠΕΔ και επιλέγει να προχωρήσει στην ανάκληση εισάγοντας τον κωδικάριθμο της αίτησης – ΥΔ που δημιούργησε στο gov.gr.
    - Με την υποβολή του αιτήματος γίνεται αυτόματα έλεγχος στα βασικά πεδία (ΑΦΜ, όνομα, επώνυμο) και το αίτημα δρομολογείται στην Αρχή Εγγραφής. Η αίτηση-ΥΔ του gov.gr καταχωρείται στη βάση δεδομένων.
    - Η Αρχή Εγγραφής ελέγχει το αίτημα και προχωρά στην ανάκληση του εγκεκριμένου πιστοποιητικού.
    - Ο συνδρομητής ενημερώνεται με SMS για την ανάκληση.

- Ανάκληση σε περίπτωση αδυναμίας λειτουργίας της εφαρμογής:

  https://services.aped.gov.gr/apedcitizen/login

  Σε περίπτωση αδυναμίας λειτουργίας της ως άνω εφαρμογής, λόγω αιφνίδιου και απρόβλεπτου γεγονότος, ο Συνδρομητής δύναται να υποβάλει αίτημα ανάκλησης εκδίδοντας αίτηση/Υπεύθυνη Δήλωση ανάκλησης εγκεκριμένου πιστοποιητικού από την Ενιαία Ψηφιακή Πύλη της Δημόσιας Διοίκησης (gov.gr)και την αποστέλλει μέσω ηλεκτρονικού ταχυδρομείου, στην ηλεκτρονική διεύθυνση aped@mindigital.gr, ή μέσω ταχυδρομείου στο Υπουργείο ψηφιακής Διακυβέρνησης/ΑΠΕΔ, Φραγκούδη 11 και Αλ. Πάντου ΤΚ 17671.

4. Λειτουργικές Απαιτήσεις Κύκλου Ζωής Πιστοποιητικών

4.1 Αίτηση για Έκδοση Πιστοποιητικού

4.1.1 Ποιος Μπορεί να Υποβάλει Αίτηση για Έκδοση Πιστοποιητικού

Για την έκδοση Εγκεκριμένου Πιστοποιητικού Συνδρομητή, το πρόσωπο που μπορεί να υποβάλει αίτηση Πιστοποιητικού είναι το φυσικό πρόσωπο που αποτελεί το Υποκείμενο του Πιστοποιητικού.

4.1.2 Διαδικασία εγγραφής και υποχρεώσεις

Για τη χορήγηση Πιστοποιητικών Συνδρομητή, όλοι οι Συνδρομητές υποβάλλονται σε διαδικασία εγγραφής και επαλήθευσης της ταυτότητάς τους, η οποία περιγράφεται στις Δηλώσεις Πρακτικής των εκδοτριών ΑΠ, και η οποία συνίσταται σε

- Ταυτοποίηση, με τους ακόλουθους δύο τρόπους:
  είτε α) με την φυσική παρουσία του Συνδρομητή,
  είτε β) με την εξ αποστάσεως ταυτοποίησή του, σε/ από αρμόδιο Εντεταλμένο Γραφείο ή, όπου αυτό κρίνεται απαραίτητο, σε/ από εκπροσώπους της Αρχής Εγγραφής ή της Εκδότριας ΑΠ.
- Γραπτή ή ηλεκτρονική αποδοχή των Όρων και Προϋποθέσεων Χρήσης Πιστοποιητικού.
- Στη συμπλήρωση και στην υπογραφή της Αίτησης για Πιστοποιητικό με την παροχή αληθών και ακριβών στοιχείων σύμφωνα με τις απαιτήσεις της παρούσας πολιτικής.
- Στην επίδειξη των σχετικών εγγράφων επικύρωσης.
- Στη δημιουργία ή υποβολή αιτήματος για δημιουργία ζεύγους κλειδιών σύμφωνα με την §6.1 της ΠΠ.
- Στη λήψη του πιστοποιητικού τους.
- Στην αποστολή του δημόσιου κλειδιού από τον Συνδρομητή, στην εκδότρια ΑΠ, σύμφωνα με την §6.1.3 της ΠΠ.
- Στην απόδειξη εκ μέρους του Συνδρομητή 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.

4.2 Επεξεργασία Αίτησης Έκδοσης Πιστοποιητικού

4.2.1 Έγκριση ή Απόρριψη Αίτησης για Έκδοση Πιστοποιητικού Συνδρομητή

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 της ΠΠ. Με την επιτυχή τέλεση όλων των απαιτούμενων διαδικασιών ταυτοποίησης, η ΑΕ θα προχωρήσει στην έγκριση του αιτήματος για την έκδοση του Πιστοποιητικού. Εφόσον η ταυτοποίηση δεν είναι επιτυχής, αντίστοιχα θα την απορρίψει.
Τα Πιστοποιητικά Συνδρομητή δημιουργούνται και εκδίδονται μετά την έγκριση από την ΑΕ της Αίτησης που υποβάλλεται από το Συνδρομητή. Πιο συγκεκριμένα, αφού ο Συνδρομητής ενημερωθεί ότι εγκρίθηκε το αίτημα, πρέπει να συνδεθεί στην ηλεκτρονική εφαρμογή διαχείρισης εγκεκριμένων πιστοποιητικών και να ακολουθήσει τη διαδικασία για την έκδοση του Πιστοποιητικού, όπως περιγράφεται στη Δήλωση Πρακτικής της εκδότριας ΑΠ.
Η ΑΠΕΔ απορρίπτει μια αίτηση για πιστοποιητικό εάν:

- η ταυτοποίηση και η επαλήθευση της ταυτότητας όλων των απαιτούμενων στοιχείων του Συνδρομητή δεν μπορεί να ολοκληρωθεί ή
- ο Συνδρομητής αδυνατεί να υποβάλει τη σχετική τεκμηρίωση που του ζητείται ή
- ο Συνδρομητής αδυνατεί να ανταποκριθεί στις ειδοποιήσεις εντός του καθορισμένου χρόνου

4.2.2 Έγκριση ή Απόρριψη Αίτησης για Έκδοση Πιστοποιητικού ΥπΑΠ

Η ΑΠΕΔ ως Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ) πιστοποιεί Υποκείμενες Αρχές Πιστοποίησης και υπογράφει τα αντίστοιχα Πιστοποιητικά ΥπΑΠ σύμφωνα με τα αναφερόμενα στην §1.3.1 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 στους σχετικούς Γενικούς Όρους και Προϋποθέσεις Χρήσης Πιστοποιητικού ή στη Δήλωση Πρακτικής της εκδότριας ΑΠ. Οι αιτήσεις για Πιστοποιητικό παραμένουν σε ισχύ μέχρι ένα μήνα ή μέχρι την απόρριψή τους.

4.3 Έκδοση Πιστοποιητικού

4.3.1 Ενέργειες της εκδότριας ΑΠ κατά την Έκδοση Πιστοποιητικού Συνδρομητή

Το Πιστοποιητικό δημιουργείται και εκδίδεται από το Συνδρομητή μέσα στην ΕΔΔΥ, μετά τη διαβίβαση αιτήματος έκδοσης πιστοποιητικού από το Εντεταλμένο Γραφείο και τη σχετική έγκριση από την ΑΕ. Το Πιστοποιητικό Συνδρομητή δημιουργείται βάσει των στοιχείων της Αίτησης για Πιστοποιητικό και εφόσον έχει εγκριθεί η Αίτηση αυτή από την ΑΕ. Για την έγκριση της Αίτησης απαιτείται η προσκόμιση εγγράφων ταυτοποίησης από το Συνδρομητή που ορίζονται στο Έντυπο Αίτησης για έκδοση Πιστοποιητικού.
Ο Συνδρομητής οφείλει να προχωρήσει σε έκδοση του Εγκεκριμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής σε διάστημα δεκαπέντε (15) ημερών από την έγκριση της αίτησής του από την Αρχή Εγγραφής. Μετά την πάροδο αυτού του διαστήματος η αίτησή του ακυρώνεται και πρέπει να υποβάλει νέα αίτηση.

4.3.2 Ενημέρωση του Συνδρομητή για την Έκδοση Πιστοποιητικού

Οι εκδότριες ΑΠ που εκδίδουν Πιστοποιητικά σε Συνδρομητές ενημερώνουν τους Συνδρομητές, είτε απευθείας είτε μέσω μιας ΑΕ, ότι το αίτημα έκδοσης πιστοποιητικού έχει εγκριθεί, προκειμένου να προχωρήσει στη διαδικασία έκδοσής του.
Τα Πιστοποιητικά καθίστανται διαθέσιμα στους Συνδρομητές από την ηλεκτρονική εφαρμογή (ιστοσελίδα) διαχείρισης πιστοποιητικών, όπως ορίζεται στη ΔΠ της εκδότριας ΑΠ.

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 (συγκεκριμένα: ονοματεπώνυμο, ημερομηνία έναρξης/ λήξης) από το Συνδρομητή μέσα σε 24 ώρες από την έκδοση, συνιστούν την αποδοχή του Πιστοποιητικού από τον Συνδρομητή.

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	Διαθέσιμο στα Βασιζόμενα Μέρη διαδικτυακά, μέσω του χώρου αποθήκευσης της ΑΠΕΔ, καθώς και ως μέρος της Αλυσίδας Πιστοποιητικού, η οποία ενσωματώνεται στο Πιστοποιητικό Συνδρομητή.
Πιστοποιητικά ΥπΑΠ	Διαθέσιμα στα Βασιζόμενα Μέρη διαδικτυακά, μέσω των χώρων αποθήκευσης της ΑΠΕΔ και των εκδοτριών ΑΠ, καθώς και ως μέρος της Αλυσίδας Πιστοποιητικού, η οποία ενσωματώνεται στο Πιστοποιητικό Συνδρομητή.

Οι εκδότριες ΑΠ δημοσιεύουν τα Πιστοποιητικά που εκδίδουν σε δημοσίως προσβάσιμο διαδικτυακό χώρο αποθήκευσης.

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 Συνδρομητή

Η χρήση του Ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί που περιλαμβάνεται στο Πιστοποιητικό θα επιτρέπεται μόνο εφόσον ο Συνδρομητής έχει συμφωνήσει με τους Γενικούς Όρους και Προϋποθέσεις και έχει αποδεχθεί το Πιστοποιητικό. Το Πιστοποιητικό θα χρησιμοποιείται σύμφωνα με τους Γενικούς Όρους και Προϋποθέσεις, τους όρους της παρούσας ΠΠ και της εφαρμοστέας Δήλωσης Πρακτικής της εκδότριας ΑΠ. Επιπλέον, η χρήση του Πιστοποιητικού πρέπει να συμμορφώνεται με τις επεκτάσεις του πεδίου «Χρήση Κλειδιού» (KeyUsage) του Πιστοποιητικού.
Οι Συνδρομητές υποχρεούνται να προστατεύουν τα ιδιωτικά κλειδιά τους από μη εξουσιοδοτημένη χρήση και να διακόπτουν τη χρήση τους μετά τη λήξη ή την ανάκληση του Πιστοποιητικού.

4.5.2 Χρήση Δημοσίου Κλειδιού και Πιστοποιητικού από Βασιζόμενο Μέρος

Τα Βασιζόμενα Μέρη πρέπει να συναινούν στους Γενικούς Όρους και Προϋποθέσεις Χρήσης ως προϋπόθεση για να εμπιστευθούν το Πιστοποιητικό. Η εμπιστοσύνη σε ένα Πιστοποιητικό πρέπει να είναι εύλογη σύμφωνα με τις περιστάσεις. Εάν οι συνθήκες υποδεικνύουν την ανάγκη για πρόσθετες διαβεβαιώσεις, το Βασιζόμενο Μέρος πρέπει να αποκτήσει αυτές τις διαβεβαιώσεις ώστε η εμπιστοσύνη σε ένα Πιστοποιητικό να θεωρηθεί εύλογη.
Πριν από οποιαδήποτε ενέργεια, η οποία θα έχει ως αποτέλεσμα να εμπιστευτούν κάποιο Πιστοποιητικό, τα Βασιζόμενα Μέρη θα αξιολογούν ανεξάρτητα και με δική τους ευθύνη:

- Την καταλληλότητα της χρήσης του Πιστοποιητικού για το δεδομένο σκοπό, ότι η χρήση του Πιστοποιητικού δεν αντίκειται στην ΠΠ και ότι το Πιστοποιητικό χρησιμοποιείται σύμφωνα με τις επεκτάσεις του πεδίου «Χρήση Κλειδιού» (Key Usage) 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, το Βασιζόμενο Μέρος φέρει αποκλειστικά την ευθύνη διερεύνησης του κατά πόσον είναι εύλογο να βασιστεί σε μια ηλεκτρονική υπογραφή που πραγματοποιήθηκε από έναν Συνδρομητή πριν την ανάκληση του Πιστοποιητικού της Αλυσίδας Πιστοποιητικών. Σε αυτή την περίπτωση, η ευθύνη της εμπιστοσύνης στο Πιστοποιητικό βαρύνει αποκλειστικά το Βασιζόμενο Μέρος.

Εφόσον η χρήση του Πιστοποιητικού είναι η κατάλληλη, τα Βασιζόμενα Μέρη πρέπει να χρησιμοποιούν το κατάλληλο λογισμικό ή/και εξοπλισμό για να εμπιστευθούν κάποιο Πιστοποιητικό και να επιτύχουν επαλήθευση της εγκεκριμένης υπογραφής.
Η ΑΠΕΔ και οι εκδότριες ΑΠ δε φέρουν ευθύνη για την αξιολόγηση της καταλληλότητας χρήσης των Πιστοποιητικών.

4.6 Ανανέωση Πιστοποιητικού

Δεν εφαρμόζεται.

4.7 Επαναδημιουργία Κλειδιών Πιστοποιητικού

4.7.1 Συνθήκες Επαναδημιουργίας Κλειδιών Πιστοποιητικού

Επαναδημιουργία κλειδιών Συνδρομητή μπορεί να γίνει μετά την ανάκληση του υφιστάμενου πιστοποιητικού ή μετά τη λήξη του.
Ο Πίνακας 6 κατωτέρω περιγράφει τις απαιτήσεις της ΑΠΕΔ για την επαναδημιουργία κλειδιών.

Πίνακας 6: Απαιτήσεις Επαναδημιουργίας Κλειδιών

Μορφή Πιστοποιητικού	Απαιτήσεις Ανανέωσης
Πιστοποιητικά Συνδρομητή	Ουσιαστικός όρος για την αποδοχή της επαναδημιουργίας κλειδιών ενός Πιστοποιητικού Συνδρομητή είναι ο έλεγχος των πληροφοριών που διενεργείται από την εκδότρια ΑΠ για να επιβεβαιωθεί ότι η ταυτότητα του Συνδρομητή είναι ακόμα έγκυρη. Αυτή η διαδικασία γίνεται με σκοπό να επιβεβαιωθεί ότι το πρόσωπο που επιδιώκει να εκδώσει ένα Πιστοποιητικό Συνδρομητή είναι στην πραγματικότητα ο Συνδρομητής του Πιστοποιητικού, όπως αναφέρεται στην §3.2.2 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 Συνδρομητής.

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 Συνδρομητή είναι στην πραγματικότητα το Υποκείμενο του Πιστοποιητικού.

4.7.4 Ενημέρωση Χρήστη για την Έκδοση Νέου Πιστοποιητικού.

Η κοινοποίηση έκδοσης Πιστοποιητικού με επαναδημιουργημένα κλειδιά στο Συνδρομητή, 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 Ανάκληση Πιστοποιητικού

4.9.1 Λόγοι Ανάκλησης

4.9.1.1 Λόγοι για Ανάκληση Πιστοποιητικών Συνδρομητή

Ένα Πιστοποιητικό Συνδρομητή ανακαλείται:

1. Κατόπιν αίτησης του κατόχου του εγκεκριμένου πιστοποιητικού.
2. Εφόσον διαπιστωθεί από την Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (Ε.Ε.Τ.Τ.) ότι το εγκεκριμένο πιστοποιητικό περιέχει ψευδείς ή ανακριβείς πληροφορίες ως προς τις απαιτήσεις του Κανονισμού (ΕΕ) 910/2014.
3. Σε περίπτωση εγκεκριμένου πιστοποιητικού η έκδοση του οποίου βασίστηκε σε ψευδείς ή ανακριβείς πληροφορίες.
4. Σε περίπτωση τερματισμού των εργασιών του παρόχου υπηρεσιών εμπιστοσύνης, εκτός εάν, πριν την ημερομηνία παύσης των εργασιών, άλλος εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης αναλάβει τη συνέχιση της λειτουργίας του μέρους της υπηρεσίας που απαιτείται.
5. Σε περίπτωση απώλειας της δικαιοπρακτικής ικανότητας, κήρυξης σε αφάνεια ή σε περίπτωση θανάτου του κατόχου του εγκεκριμένου πιστοποιητικού, εάν πρόκειται για φυσικό πρόσωπο.
6. Σε περίπτωση που τελεσίδικη δικαστική απόφαση διατάσσει την ανάκληση, ύστερα από κοινοποίηση της σχετικής απόφασης στον πάροχο υπηρεσιών εμπιστοσύνης.

7. Αν από τη σύμβαση μεταξύ του παρόχου υπηρεσιών εμπιστοσύνης και του κατόχου του εγκεκριμένου πιστοποιητικού απορρέει σχετική προς τούτο υποχρέωση ή δικαίωμα ενός εκ των συμβαλλομένων μερών.
8. Σε περίπτωση που υφίστανται σοβαρές ενδείξεις ότι τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής του κατόχου του εγκεκριμένου πιστοποιητικού έχουν γίνει γνωστά ή χρησιμοποιούνται από τρίτους.
9. Σε περίπτωση κατά την οποία τα δεδομένα δημιουργίας ηλεκτρονικής υπογραφής του παρόχου υπηρεσιών εμπιστοσύνης έχουν γίνει γνωστά σε τρίτους.
10. Σε κάθε περίπτωση κατά την οποία στοιχεία που περιλαμβάνονται στο εγκεκριμένο πιστοποιητικό τροποποιηθούν.

Οι Γενικοί Όροι και Προϋποθέσεις των εκδοτριών ΑΠ απαιτούν από τους Συνδρομητές 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.

4.9.1.2 Λόγοι 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.
- Υπάρξει σχετικό τεκμηριωμένο αίτημα από την ΕΕΤΤ.
- 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 Συνδρομητή

Η ΑΠΕΔ ή η εκδότρια ΑΠ υποχρεούται να ανακαλέσει οποιοδήποτε Πιστοποιητικό Συνδρομητή που έχει εκδώσει, σύμφωνα με τα αναφερόμενα στην §4.9.1.1 της ΠΠ.
Οι Συνδρομητές δύνανται να ζητήσουν ανάκληση των δικών τους Πιστοποιητικών.
Η ΑΠΕΔ, μέσω της Εφαρμογής Διαχείρισης Ψηφιακών Πιστοποιητικών, εκτελεί περιοδικό έλεγχο χρηστών που τα εγκεκριμένα πιστοποιητικά τους είναι σε ισχύ προκειμένου να επιβεβαιωθεί ότι είναι εν ζωή, μέσα από την υπηρεσία ένδειξης ζωής/θανάτου από το Μητρώο Πολιτών. Σε περίπτωση που εντοπιστεί περίπτωση θανάτου του χρήστη εγκεκριμένου πιστοποιητικού η εφαρμογή ανακαλεί αυτόματα το πιστοποιητικό.

4.9.2.2 Ποιος Μπορεί να Ζητήσει Ανάκληση Πιστοποιητικού ΥπΑΠ

Η ΑΠΕΔ, η ΥπΑΠ και η ΕΕΤΤ έχουν δικαίωμα να ζητήσουν την ανάκληση πιστοποιητικού ΥπΑΠ που έχει εκδοθεί για την τελευταία.

4.9.3 Διαδικασία για Υποβολή Αιτήματος Ανάκλησης Πιστοποιητικού

Ένας Συνδρομητής που επιθυμεί ανάκληση του Πιστοποιητικού του πρέπει να υποβάλει 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 πράγματι το υποκείμενο του Πιστοποιητικού, σύμφωνα με την ενότητα §4.9.2 ανωτέρω. Το αίτημα αυτό διαβιβάζεται στην υπεύθυνη ΑΕ που έχει ελέγξει την Ηλεκτρονική Εγγραφή ή Αίτηση του Συνδρομητή για Πιστοποιητικά και η οποία είναι αρμόδια να το ανακαλέσει άμεσα.

4.9.4 Χρονικό Διάστημα μέσα στο οποίο η ΑΠ 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 Εγκεκριμένων Πιστοποιητικών, τυγχάνουν άμεσης επεξεργασίας από τις ΑΕ, οι οποίες εντός 24 ωρών διεκπεραιώνουν το αίτημα.
Αμέσως μετά την ανάκληση του Πιστοποιητικού, η εκδότρια ΑΠ ενημερώνει το Συνδρομητή για το γεγονός αυτό, μέσω μηνύματος ηλεκτρονικού ταχυδρομείου στη διεύθυνση που έχει δηλωθεί στην ηλεκτρονική αίτηση έκδοσης

του πιστοποιητικού («αίτημα στο portal της ΑΠΕΔ») ή μέσω γραπτού μηνύματος (SMS). Η εκδότρια ΑΠ τηρεί σχετικά αρχεία που αποδεικνύουν ότι έχει πραγματοποιηθεί η σχετική ενημέρωση.

4.9.5 Απαιτήσεις Ελέγχου Ανάκλησης για Βασιζόμενα Μέρη

Τα Βασιζόμενα Μέρη 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, το Βασιζόμενο Μέρος 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 αποθήκευσής της στη διεύθυνση: https://pki.aped.gov.gr/repository/gr/CRL/. Επιπλέον, ένας "Πίνακας αναφοράς ΚΑΠ" ανακοινώνεται στο Χώρο Αποθήκευσης στη διεύθυνση: https://pki.aped.gov.gr/repository/gr/CRL/, ώστε να επιτρέπει στα Βασιζόμενα Μέρη να προσδιορίσουν για κάθε ΥπΑΠ την ακριβή τοποθεσία αποθήκευσης του ΚΑΠ. Η τοποθεσία αυτή περιλαμβάνεται και στο ίδιο το πιστοποιητικό και είναι σωστή για όλο το διάστημα της ισχύος του.
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 εκδότριες 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 Συνδρομητών που εκδίδουν οι εκδότριες ΑΠ δημοσιεύονται καθημερινά. Οι ΚΑΠ για πιστοποιητικά ΥπΑΠ που εκδίδει η ΑΠΕΔ δημοσιεύονται κάθε έτος καθώς επίσης και κάθε φορά που ανακαλείται κάποιο Πιστοποιητικό.
Οι πληροφορίες σχετικά με την κατάσταση ανάκλησης καθίστανται διαθέσιμες και μετά την περίοδο ισχύος του πιστοποιητικού, μέσω του πρωτοκόλλου OCSP.
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 στο χώρο πληροφοριών, γίνεται εντός εύλογου χρονικού διαστήματος 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. Η πληροφορία αυτή περιλαμβάνεται και στα ίδια τα πιστοποιητικά και είναι σωστή για όλη τη διάρκεια της ισχύος τους.

4.9.9 Απαιτήσεις Δικτυακού Ελέγχου Ανάκλησης

Κάθε Βασιζόμενο Μέρος 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

Δεν εφαρμόζεται.

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 τα δυνητικά Βασιζόμενα Μέρη με σχετική ανακοίνωση στις ηλεκτρονικές διευθύνσεις

https://pki.aped.gov.gr και https://www.aped.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, ενώ παράλληλα ενημερώνει και την ΕΕΤΤ.

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 και των OCSP responders.

4.10.2 Διαθεσιμότητα Υπηρεσίας

Οι Υπηρεσίες Κατάστασης Πιστοποιητικών είναι διαθέσιμες 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα, με ελάχιστη συνολική διαθεσιμότητα 99% ανά έτος με τις προγραμματισμένες διακοπές λειτουργίας να μην υπερβαίνουν το ποσοστό του 0,4% ετησίως.

4.11 Τερματισμός Εγγραφής

Οι Συνδρομητές μπορούν να διακόψουν τη χρήση των Πιστοποιητικών που κατέχουν είτε αφήνοντας το Πιστοποιητικό τους να λήξει, είτε ανακαλώντας το Πιστοποιητικό τους πριν από τη λήξη του χωρίς να το αντικαταστήσουν.

5. Φυσικά, Διαδικαστικά Μέτρα Προστασίας και Ασφάλειας

Η ΑΠΕΔ εφαρμόζει υψηλές προδιαγραφές ασφαλείας οι οποίες ανταποκρίνονται στην παρούσα ΠΠ. Η ΥΔΚ της ΑΠΕΔ φιλοξενείται σε υποδομές Εγκεκριμένου Παρόχου Υπηρεσιών Εμπιστοσύνης στις οποίες εφαρμόζονται όλα τα απαιτούμενα φυσικά μέτρα προστασίας και ασφάλειας όπως περιγράφονται στην παρούσα ενότητα, και σύμφωνα με την Πολιτική Ασφάλειας που έχει εκπονηθεί.

5.1 Φυσικά Μέτρα Προστασίας

5.1.1 Χώρος Εγκατάστασης και Κατασκευή

Οι υπηρεσίες εμπιστοσύνης των ΑΠ 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. Η ΑΠΕΔ διατηρεί εγκαταστάσεις Αποκατάστασης Καταστροφών όσον αφορά τις λειτουργίες ΑΠ. Οι εγκαταστάσεις Αποκατάστασης Καταστροφών της ΑΠΕΔ προστατεύονται από πολλαπλά επίπεδα φυσικής ασφάλειας.

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 εμπιστοσύνης 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 Διάθεση αποβλήτων

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. Τα εφεδρικά αντίγραφα αποθηκεύονται εκτός του κυρίου χώρου εγκατάστασης με κατάλληλα μέσα προστασίας.

5.2 Διαδικαστικά Μέτρα Ελέγχου

5.2.1 Έμπιστοι Ρόλοι

Ως Έμπιστα Πρόσωπα θεωρούνται όλοι οι υπάλληλοι οι οποίοι έχουν πρόσβαση ή ελέγχουν τις λειτουργίες επαλήθευσης ταυτότητας ή τις κρυπτογραφικές λειτουργίες και οι οποίοι θα μπορούσαν να επηρεάσουν σε σημαντικό βαθμό τα εξής:

- την επικύρωση των στοιχείων στις Αιτήσεις για Πιστοποιητικό,
- την αποδοχή, την απόρριψη ή άλλη επεξεργασία των Αιτήσεων για Πιστοποιητικό, των αιτημάτων για ανάκληση ή των πληροφοριών εγγραφής,
- την έκδοση ή την ανάκληση Πιστοποιητικών, συμπεριλαμβανομένου του προσωπικού που έχει πρόσβαση στα τμήματα περιορισμένης πρόσβασης του χώρου αποθήκευσής της,
- τον χειρισμό των στοιχείων ή των αιτημάτων των Συνδρομητών.

Ως Έμπιστα Πρόσωπα θεωρούνται ενδεικτικά:

- το προσωπικό της ΑΠΕΔ,
- το προσωπικό που εμπλέκεται στις διαδικασίες κρυπτογράφησης,
- το προσωπικό ασφαλείας,
- το προσωπικό διαχείρισης συστημάτων,
- οι εξουσιοδοτημένοι μηχανικοί και
- τα στελέχη στα οποία έχει ανατεθεί η διαχείριση της αξιοπιστίας της υποδομής.

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 εγκεκριμένα 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.
- Την πρόσβαση σε εξ αποστάσεως ΕΔΔΥ.

5.3 Μέτρα Ελέγχου Προσωπικού

Η ΑΠΕΔ εγγυάται για το προσωπικό που πρόκειται να αποκτήσει την ιδιότητα του Έμπιστου Προσώπου ως προς τα τυπικά του προσόντα και την εμπειρία που απαιτούνται για την εκτέλεση των καθηκόντων της επιδιωκόμενης θέσης με επαρκή και ικανοποιητικό τρόπο. Για το προσωπικό που κατέχει Θέσεις Εμπιστοσύνης, οι έλεγχοι ιστορικού επαναλαμβάνονται τουλάχιστον κάθε πέντε (5) έτη.

5.3.1 Απαιτήσεις Προσόντων, Εμπειρίας και Εξουσιοδότησης

Οι υπάλληλοι της ΑΠΕΔ με ιδιότητα Έμπιστου Προσώπου έχουν την υποχρέωση διατήρησης του απορρήτου των εμπιστευτικών πληροφοριών των οποίων έχουν λάβει γνώση κατά την εκτέλεση των καθηκόντων τους, και δεν επιτρέπεται να αναλαμβάνουν πρωτοβουλίες ή καθήκοντα ασυμβίβαστα με τον έμπιστο ρόλο που τους έχει ανατεθεί, ή καταστρατηγώντας την αρχή της αμεροληψίας της διοίκησης.
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

Η ΑΠΕΔ εγγυάται την καταλληλότητα των υπαλλήλων της για την εκτέλεση της παρούσας ΠΠ και μεριμνά για την εφαρμογή του δημοσιοϋπαλληλικού κώδικα και των σχετικών διατάξεων, όπως ισχύουν, ιδίως του Πειθαρχικού Δικαίου.
Πριν από την ανάθεση καθηκόντων Ρόλου Εμπιστοσύνης, η ΑΠΕΔ διενεργεί έλεγχο του φακέλου του υπαλλήλου, προκειμένου να διαπιστώσει τυχόν πειθαρχική ή άλλη καταδίκη. Η ως άνω ανάθεση τελεί υπό την προϋπόθεση ότι δεν προκύπτει πειθαρχική ή άλλη καταδίκη του υπαλλήλου που θα αναλάβει τον έμπιστο ρόλο.
Η χρήση των πληροφοριών που αποκαλύπτονται κατά τον έλεγχο του ιστορικού ώστε να ληφθούν οι σχετικές ενέργειες, υπόκειται στην ισχύουσα νομοθεσία περί απορρήτου και εμπιστευτικότητας.

5.3.3 Απαιτήσεις Εκπαίδευσης

Η ΑΠΕΔ παρέχει στο προσωπικό της εκπαίδευση η οποία κρίνεται απαραίτητη για την εκτέλεση των εργασιακών καθηκόντων τους με επαρκή και ικανοποιητικό τρόπο. Η εκπαίδευση που εφαρμόζει η ΑΠΕΔ περιλαμβάνει τα ακόλουθα:

- τις βασικές έννοιες της ΥΔΚ,
- τις αρμοδιότητες των θέσεων εργασίας,
- την πολιτική και τις διαδικασίες ασφάλειας και λειτουργίας της ΑΠΕΔ,
- τη χρήση και λειτουργία του εξοπλισμού και λογισμικού που έχει αναπτυχθεί,
- την αναφορά και αντιμετώπιση περιστατικών και της Έκθεσης σε Κίνδυνο και την αποκατάσταση καταστροφών και τις διαδικασίες συνέχισης επιχειρηματικής δραστηριότητας.

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

Στην περίπτωση μη εξουσιοδοτημένων ενεργειών ή άλλων παραβάσεων των πολιτικών και των διαδικασιών της ΑΠΕΔ λαμβάνονται τα κατάλληλα πειθαρχικά μέτρα. Τα εν λόγω πειθαρχικά μέτρα προσδιορίζονται ανάλογα με τη συχνότητα και τη σοβαρότητα των μη εξουσιοδοτημένων ενεργειών και είναι σύμφωνα με τον δημοσιοϋπαλληλικό κώδικα, όπως ισχύει.

5.3.6 Απαιτήσεις Ανεξάρτητου Αναδόχου

Η πλήρωση Θέσεων Εμπιστοσύνης γίνεται και από ανεξάρτητους ανάδοχους οι οποίοι υπόκεινται στα ίδια λειτουργικά κριτήρια και κριτήρια ασφαλείας που ισχύουν και για τους εργαζομένους της ΑΠΕΔ. Η πρόσβαση στις ασφαλείς εγκαταστάσεις που φιλοξενείται η ΑΠΕΔ επιτρέπεται μόνον από Έμπιστα Πρόσωπα, τα οποία είναι είτε εργαζόμενοι της ΑΠΕΔ, είτε ανήκουν σε ανεξάρτητο ανάδοχο. Οι εκδότριες ΑΠ και οι ΑΕ δύνανται να επιτρέψουν σε ανεξάρτητους εργολήπτες 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. Θα πρέπει να υπάρχει σχετική σύμβαση η οποία θα έχει ελεγχθεί από Οργανισμό Αξιολόγησης Συμμόρφωσης και να έχει προηγηθεί σχετική ενημέρωση και έγκριση από την ΕΕΤΤ.

5.3.7 Έντυπα που Διατίθενται στο Προσωπικό

Το προσωπικό που αναλαμβάνει την εφαρμογή των υπηρεσιών εμπιστοσύνης της ΥΔΚ βάσει των διατάξεων του παρόντος, λαμβάνει πλήρη γνώση αυτής της Πολιτικής και της εκάστοτε εφαρμοστέας Δήλωσης Πρακτικής, καθώς και την απαιτούμενη εκπαιδευτική και άλλη τεκμηρίωση, 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 Συνδρομητών, συμπεριλαμβανομένων:

- Στοιχείων Εγγραφής,

- Επιτυχούς ή μη επεξεργασίας των Ηλεκτρονικών Εγγραφών ή Αιτήσεων για Πιστοποιητικά, 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 Συνδρομητή.
- Τον αριθμό εγγράφου ταυτοποίησης
- Το περιεχόμενο του εγγράφου ταυτοποίησης (επώνυμο, όνομα, αρχή έκδοσης κλπ), εφόσον υπάρχει διαλειτουργικότητα με το αντίστοιχο ηλεκτρονικό μητρώο του εγγράφου.
- Για την εξ αποστάσεως ταυτοποίηση, αντίγραφο του εγγράφου ταυτοποίησης και το βίντεο της τηλεδιάσκεψης
- Ονοματεπώνυμο του προσώπου που διενεργεί την ταυτοποίηση.
- Τη 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 παράγονται κάθε μία ώρα. Στα αρχεία τοποθετείται προηγμένη ηλεκτρονική υπογραφή και χρονοσφραγίδα. Πλήρη αντίγραφα ασφαλείας παράγονται σε εβδομαδιαία βάση.

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 συμβάντος από το σύστημα συλλογής ελέγχων, δεν είναι απαραίτητη η ειδοποίηση του φυσικού προσώπου, του οργανισμού, της διάταξης ή της εφαρμογής που προκάλεσε το συμβάν, εκτός και εάν η σχετική ειδοποίηση είναι υποχρεωτική βάσει νόμου.
Εάν τα αρχεία αφορούν στη λειτουργία των υπηρεσιών, που απαιτούνται για τους σκοπούς της παροχής αποδεικτικών στοιχείων για την ορθή λειτουργία των υπηρεσιών και για τους σκοπούς των νομικών διαδικασιών, καθίστανται διαθέσιμα στις δικαστικές αρχές και/ή στα άτομα που έχουν το νόμιμο δικαίωμα πρόσβασης.

5.4.8 Αξιολόγηση Ευπάθειας

Τα περιστατικά που λαμβάνουν χώρα κατά τη διαδικασία ελέγχου καταγράφονται, ώστε να είναι δυνατή η παρακολούθηση των ευπαθειών του συστήματος.
Οι αξιολογήσεις ευπαθειών συστήματος διενεργούνται, ελέγχονται και αναθεωρούνται. Η ετήσια Αξιολόγηση Ευπαθειών θα αποτελεί σημείο αναφοράς όσον αφορά τον ετήσιο έλεγχο της ΑΠΕΔ.

5.5 Τήρηση 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 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 Γενικούς Όρους και Προϋποθέσεις Χρήσης.
- Κάθε μεταβολή που έχει επέλθει στους Γενικούς Όρους και Προϋποθέσεις Χρήσης.
- Την ταυτότητα του Συνδρομητή 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 Συνδρομητών περιλαμβάνουν σε ηλεκτρονική μορφή:

- Αίτηση-ΥΔ του gov.gr, που περιέχει αριθμό ταυτότητας ή διαβατηρίου
- Αίτηση στην ΑΠΕΔ
- Βεβαίωση Φυσικής ή Εξ Αποστάσεως Ταυτοποίησης Συνδρομητή, ψηφιακά υπογεγραμμένη, με χρήση εγκεκριμένης ηλεκτρονικής υπογραφής από τον υπάλληλο που πραγματοποίησε την ταυτοποίηση (φυσικής ή εξ αποστάσεως) ή προηγμένη ή εγκεκριμένη ηλεκτρονική σφραγίδα του παρόχου της υπηρεσίας της εξ αποστάσεως 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 φυσικά ή ψηφιακά αρχεία σχετικά με τις αιτήσεις για πιστοποιητικά, τις πληροφορίες εγγραφής και τα αιτήματα ή τις αιτήσεις για ανάκληση φυλάσσονται για τουλάχιστον επτά (7) έτη μετά τη λήξη ισχύος οποιουδήποτε πιστοποιητικού βάσει των εν λόγω αρχείων.

Σε περίπτωση τερματισμού της λειτουργίας της ΑΠ, τα αρχεία καταγραφής και τα αρχεία της ΑΠΕΔ φυλάσσονται και είναι προσβάσιμα έως την ανωτέρω αναφερόμενη περίοδο διατήρησης σύμφωνα με την ενότητα §5.8.

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 προσπέλασής 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, μαζί με το back-up όλης της Βάσης Δεδομένων, μέσω της αποθήκευσης των επιπρόσθετων πληροφοριών (incremental backup), ενώ παράγει πλήρη εφεδρικά αντίγραφα (full backup) σε εβδομαδιαία βάση.
Οι εκδότριες ΑΠ εφαρμόζουν μέτρα ανάλογου επιπέδου ασφαλείας.

5.5.5 Απαιτήσεις για τη χρονοσήμανση των αρχείων

Τα Πιστοποιητικά, οι ΚΑΠ καθώς και οι άλλες καταχωρίσεις ανάκλησης στη βάση δεδομένων περιλαμβάνουν πληροφορίες σχετικά με την ώρα και την ημερομηνία. Τα εν λόγω στοιχεία χρονοσήμανσης δεν είναι κρυπτογραφημένα.

5.5.6 Διαδικασίες για την Πρόσβαση και την Επαλήθευση Πληροφοριών Αρχείου

Βλ. ΠΠ §5.5.3.

5.6 Αντικατάσταση Κλειδιών

Τα ζεύγη κλειδιών που πιστοποιούν τις ΑΠ αποσύρονται με το πέρας του αντίστοιχου ανώτατου χρόνου ζωής τους όπως ορίζεται στην §6.3.2 της ΠΠ.
Πριν από τη λήξη του Πιστοποιητικού της ΑΠ για μια ιεραρχικά Ανώτερη ΑΠ, εφαρμόζονται διαδικασίες αντικατάστασης των κλειδιών ώστε να διευκολυνθεί η ομαλή μετάβαση όσον αφορά οντότητες εντός της ιεραρχίας της Ανώτερης ΑΠ, από το παλαιό ζεύγος κλειδιών στο νέο ζεύγος κλειδιών. Η διαδικασία αντικατάστασης κλειδιών της ΑΠ προϋποθέτει ότι:

- Η ιεραρχικά Ανώτερη ΑΠ διακόπτει την έκδοση νέων Πιστοποιητικών των ιεραρχικά Υφιστάμενων ΑΠ το αργότερο έως τις 60 ημέρες πριν από το χρονικό σημείο (εφεξής «Ημερομηνία Διακοπής Έκδοσης») όπου ο εναπομένων χρόνος ζωής του ζεύγους κλειδιών της ιεραρχικά Ανώτερης ΑΠ είναι ίσος με την Περίοδο Ισχύος του εγκριθέντος Πιστοποιητικού για τη συγκεκριμένη μορφή Πιστοποιητικών που εκδίδονται από τις Υφιστάμενες ΑΠ στην ιεραρχία της Ανώτερης ΑΠ.
- Τα Πιστοποιητικά, κατά την αποδοχή Αιτήματος για Πιστοποιητικό Υφιστάμενης ΑΠ (ή Συνδρομητή τελικού χρήστη) που λαμβάνεται μετά την «Ημερομηνία Διακοπής Έκδοσης», θα υπογράφονται με το νέο ζεύγος κλειδιών της ΑΠ.

Η ιεραρχικά Ανώτερη ΑΠ συνεχίζει να εκδίδει ΚΑΠ υπογεγραμμένες με το αρχικό ιδιωτικό κλειδί της Ανώτερης ΑΠ έως 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

5.7.1 Διαδικασίες χειρισμού περιστατικών και έκθεσης σε κίνδυνο

Αντίγραφα ασφαλείας των ακόλουθων πληροφοριών της ΑΠ φυλάσσονται σε αποθήκη εκτός του κύριου χώρου εγκαταστάσεων και καθίστανται διαθέσιμα σε περίπτωση Έκθεσης σε κίνδυνο ή καταστροφής: Δεδομένα των

Αιτήσεων για Πιστοποιητικό, δεδομένα ελέγχων και αρχεία της βάσης δεδομένων για όλα τα εκδοθέντα Πιστοποιητικά. Αντίγραφα ασφαλείας των ιδιωτικών κλειδιών της ΑΠ δημιουργούνται και διατηρούνται σύμφωνα με την παρούσα ΔΠΠ.

Η ΑΠΕΔ ενημερώνει, χωρίς αδικαιολόγητη καθυστέρηση και, σε κάθε περίπτωση, εντός 24 ωρών αφότου έλαβε γνώση σχετικά, τον εποπτικό φορέα Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ), τη Γενική Διεύθυνση Κυβερνοασφάλειας του ΥΨηΔ και κατά περίπτωση την Εθνική Αρχή Αντιμετώπισης Ηλεκτρονικών Επιθέσεων (Εθνικό CERT) και τον DPO του ΥΨηΔ, για οποιαδήποτε παραβίαση της ασφάλειας ή απώλεια της ακεραιότητας που έχει σημαντικό αντίκτυπο στην παρεχόμενη υπηρεσία εμπιστοσύνης ή στα σχετικά δεδομένα προσωπικού χαρακτήρα (επίπεδο επίδρασης συμβάντος 3 ή μεγαλύτερο, σύμφωνα με την κατάταξη που ορίζεται στον Κανονισμό Παροχής Υπηρεσιών Εμπιστοσύνης της ΕΕΤΤ, άρθρο 5).

Όταν η παραβίαση της ασφάλειας ή η απώλεια της ακεραιότητας είναι πιθανόν να επηρεάσει δυσμενώς φυσικό ή νομικό πρόσωπο στο οποίο έχει παρασχεθεί η υπηρεσία εμπιστοσύνης, η ΑΠΕΔ ενημερώνει επίσης, χωρίς αδικαιολόγητη καθυστέρηση, το φυσικό ή νομικό πρόσωπο για την παραβίαση της ασφάλειας ή την απώλεια της ακεραιότητας.

5.7.2 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.

5.7.3 Έκθεση 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:

- Ειδοποιείται η Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων (ΕΕΤΤ).
- Η ΕΕΤΤ μπορεί να αποσύρει το Πιστοποιητικό από τον Κατάλογο Εμπιστοσύνης εποπτευόμενων/ διαπιστευμένων Παροχών Υπηρεσιών Εμπιστοσύνης – TSL.
- Η κατάσταση ανάκλησης του Πιστοποιητικού ΥπΑΠ κοινοποιείται στους Συνδρομητές και στα Βασιζόμενα Μέρη 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 και νέο πιστοποιητικό ΥπΑΠ σύμφωνα με την §5.6 της ΠΠ, εκτός της περίπτωσης όπου διακόπτεται η παροχή των υπηρεσιών πιστοποίησης σύμφωνα με την §5.8 της ΠΠ

5.7.4 Δυνατότητες Συνέχισης Επιχειρησιακών Λειτουργιών Μετά Από Καταστροφή

Για την εξασφάλιση της συνέχισης των επιχειρησιακών 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 εμπιστοσύνης μιας ΥπΑΠ, η εν λόγω ΑΠ υποχρεούται με κάθε πρόσφορο μέσο να ενημερώσει όσους επηρεάζονται άμεσα από την εν λόγω διακοπή, τους

Συνδρομητές, Βασιζόμενα Μέρη, κ.α., για τη διακοπή παροχής των υπηρεσιών εμπιστοσύνης πριν αυτή επέλθει, με σχετική ανακοίνωση της στην ηλεκτρονική διεύθυνση της. Για τη διακοπή παροχής των υπηρεσιών εμπιστοσύνης της ΑΠΕΔ, η σχετική ανακοίνωση της δημοσιεύεται στην ηλεκτρονική διεύθυνση http://www.aped.gov.gr
Ενόψει της διακοπής παροχής των υπηρεσιών εμπιστοσύνης της ΑΠΕΔ ή μιας εκδότριας ΑΠ σύμφωνα με τα παραπάνω, αναπτύσσεται από την εν λόγω ΑΠ Σχέδιο Τερματισμού Εργασιών το οποίο συμμορφώνεται με τον εν ισχύ Κανονισμό Παροχής Υπηρεσιών Εμπιστοσύνης και το στ. θ της παρ. 2 του άρθρου 24 του Κανονισμού ΕΕ 910/2014 (eIDAS), και δύναται να περιλαμβάνει ανάλογα με την περίπτωση, τα ακόλουθα:

- την ειδοποίηση των μερών που επηρεάζονται από τη διακοπή λειτουργίας, όπως είναι οι Συνδρομητές και τα Βασιζόμενα Μέρη, ενημερώνοντάς τους για την κατάσταση της ΑΠ,
- την ανάκληση του Πιστοποιητικού που εκδόθηκε στην ΑΠ από την ΑΠΕΔ,
- τη διατήρηση των αρχείων και των εγγράφων της ΑΠ για τα χρονικά διαστήματα που απαιτούνται από την παρούσα ΔΠΠ,
- τη συνεχή παροχή των υπηρεσιών υποστήριξης Συνδρομητή,
- τη συνεχή παροχή των υπηρεσιών ανάκλησης, όπως είναι η έκδοση των ΚΑΠ ή η υποστήριξη υπηρεσιών δικτυακού ελέγχου κατάστασης Πιστοποιητικών,
- την ανάκληση των Πιστοποιητικών Συνδρομητών και των υφιστάμενων ΑΠ τα οποία δεν έχουν λήξει ή ανακληθεί, εφόσον είναι απαραίτητο,
- την καταστροφή του ιδιωτικού κλειδιού της ΑΠ, συμπεριλαμβανομένου του εφεδρικού κλειδιού και των διακριτικών υλικού που περιλαμβάνουν το εν λόγω ιδιωτικό κλειδί,
- τις απαραίτητες ρυθμίσεις για τη μετάβαση των υπηρεσιών της ΑΠ προς τη διάδοχη ΑΠ, όπου είναι δυνατό,
- την ειδοποίηση της ΕΕΤΤ
- τη μεταφορά των υποχρεώσεων σε αξιόπιστο μέρος όσον αφορά τη διατήρηση των αρχείων και των εγγράφων της ΑΠ για τα χρονικά διαστήματα που απαιτούνται από την παρούσα ΔΠΠ και τον Κανονισμό eIDAS, καθώς και τη συνεχή παροχή των υπηρεσιών ανάκλησης, όπως είναι η έκδοση των ΚΑΠ ή η υποστήριξη υπηρεσιών δικτυακού ελέγχου κατάστασης Πιστοποιητικών
- την υποβολή του αρχείου και των εγγράφων της ΑΠ της ΑΠΕΔ σε άλλον συμβατικό Πάροχο Υπηρεσιών Εμπιστοσύνης όσον αφορά στα Εγκεκριμένα Πιστοποιητικά για τα χρονικά διαστήματα που απαιτούνται βάσει νομοθεσίας.

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 Συνδρομητές διενεργείται με τη χρήση πιστοποιημένης Εγκεκριμένης Διατάξεως Δημιουργίας Υπογραφής (ΕΔΔΥ), η οποία συμμορφώνεται με τις απαιτήσεις του Κανονισμού ΕΕ 910/2014 (eIDAS). Ειδικότερα, κατά τη διαδικασία της Ηλεκτρονικής Εγγραφής ή Αίτησης για Πιστοποιητικά:

- Ο Συνδρομητής χρησιμοποιεί συγκεκριμένο μοντέλο ΕΔΔΥ, όπως αναφέρεται στις οδηγίες που έχει αναρτήσει η ΑΠΕΔ στο www.aped.gov.gr
- Ο Συνδρομητής δημιουργεί ένα ζεύγος δημόσιου - ιδιωτικού κλειδιού υπογραφής μέσα στην ΕΔΔΥ μέσω της Εφαρμογής Διαχείρισης Ψηφιακών Πιστοποιητικών της ΑΠΕΔ, ακολουθώντας τις σχετικές οδηγίες στο www.aped.gov.gr. Η εφαρμογή χρησιμοποιεί το απαραίτητο middleware για να επικοινωνήσει με τον driver της συγκεκριμένης ΕΔΔΥ και να ολοκληρώσει τη διαδικασία με ένα αυτόματο τρόπο. Το ιδιωτικό κλειδί υπογραφής παραμένει στην ΕΔΔΥ.
- Το δημόσιο κλειδί με τα στοιχεία του Συνδρομητή αποστέλλονται στην Αρχή Πιστοποίησης για να υπογραφούν.

Η παραγωγή, αποθήκευση και περαιτέρω χρήση των κλειδιών των εξ αποστάσεως Εγκεκριμένων Ψηφιακών Πιστοποιητικών γίνεται ή ελέγχεται από την ΑΠΕΔ χρησιμοποιώντας αποκλειστικά συσκευές πιστοποιημένες σύμφωνα με τις απαιτήσεις του άρθρου 30.3 του Κανονισμού ΕΕ 910/2014 (eIDAS), οι οποίες εμπεριέχονται στη λίστα εγκεκριμένων συσκευών που τηρεί η Ευρωπαϊκή Επιτροπή σε συμμόρφωση με τα άρθρα 30, 31 και 39 του Κανονισμού eIDAS.

6.1.2 Παράδοση Ιδιωτικού Κλειδιού

Το ζεύγος κλειδιών Συνδρομητή παράγεται σε ΕΔΔΥ από το Συνδρομητή, οπότε δεν ισχύει η παράδοση του ιδιωτικού κλειδιού στον Συνδρομητή.
Όταν τα ζεύγη κλειδιών παράγονται σε εξ αποστάσεως ΕΔΔΥ από τον Συνδρομητή, το ιδιωτικό κλειδί δημιουργείται και αποθηκεύεται εντός της εξ αποστάσεως ΕΔΔΥ.

6.1.3 Παράδοση Δημόσιου Κλειδιού στον Εκδότη του Πιστοποιητικού

Οι Συνδρομητές υποβάλλουν ηλεκτρονικά το δημόσιο κλειδί τους στην εκδότρια ΑΠ που θα παράσχει τις υπηρεσίες εμπιστοσύνης, 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).

6.1.4 Παράδοση Δημόσιου Κλειδιού ΑΠ σε Βασιζόμενα Μέρη

Η ΑΠΕΔ καθιστά διαθέσιμα τα Πιστοποιητικά των ΥπΑΠ στους Συνδρομητές και στα Βασιζόμενα Μέρη από το χώρο αποθήκευσής της (https://pki.aped.gov.gr/repository).
Οι εκδότριες ΑΠ καθιστούν διαθέσιμη την πλήρη αλυσίδα πιστοποιητικών στο Συνδρομητή κατά την έκδοση ενός Πιστοποιητικού.

6.1.5 Μέγεθος Κλειδιού

Τα ζεύγη κλειδιών πρέπει να διαθέτουν ικανοποιητικό μέγεθος ώστε να αποτρέπουν τρίτους να καθορίσουν το ιδιωτικό κλειδί του ζεύγους κλειδιών χρησιμοποιώντας την κρυπτανάλυση κατά την αναμενόμενη διάρκεια χρήσης των κλειδιών αυτών. Το πρότυπο της ΑΠΕΔ όσον αφορά στο ελάχιστο μέγεθος κλειδιών είναι η χρήση ενός ζεύγους κλειδιών ισχύος τουλάχιστον με 2048 bit RSA για τα πιστοποιητικά των ΑΠ και του Συνδρομητή.
Όλα τα πιστοποιητικά των ΑΠ και του Συνδρομητή χρησιμοποιούν τον SHA-256 αλγόριθμο κατακερματισμού (hash) για τις ψηφιακές υπογραφές.

6.1.6 Δημιουργία παραμέτρων και έλεγχος ποιότητας δημόσιων κλειδιών

Η ποιότητα των δημοσίων κλειδιών εξασφαλίζεται με τη χρήση ασφαλών μηχανισμών παραγωγής τυχαίων αριθμών που είναι ενσωματωμένοι στην ΕΔΔΥ.

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 Συνδρομητές 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 και έλεγχοι για τις Κρυπτογραφικές Μονάδες

Για τη δημιουργία και αποθήκευση ιδιωτικών κλειδιών της ΑΠΕΔ και των εκδοτριών ΑΠ χρησιμοποιούνται κρυπτογραφικές μονάδες οι οποίες είναι πιστοποιημένες κατά eIDAS (QSCDs) για τις εγκεκριμένες υπηρεσίες. Τα ιδιωτικά κλειδιά του Συνδρομητή παράγονται σε ΕΔΔΥ που συμμορφώνεται με τις απαιτήσεις του κανονισμού eIDAS.

Η ΑΠΕΔ επιβλέπει την κατάσταση του πιστοποιητικού ΕΔΔΥ μέχρι τη λήξη ισχύος του πιστοποιητικού που συνδέεται με την αντίστοιχη ΕΔΔΥ. Σε περίπτωση τροποποίησης της κατάστασης του πιστοποιητικού της ΕΔΔΥ, η ΑΠΕΔ θα παύσει να εκδίδει πιστοποιητικά σε αυτές τις συσκευές.

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. Θα πρέπει να σημειωθεί ότι ο αριθμός των μεριδίων που διανέμονται για τα διακριτικά αποκατάστασης καταστροφής μπορεί να είναι μικρότερος από τον αριθμό μεριδίων που διανεμήθηκαν για τα λειτουργικά διακριτικά (tokens), ενώ ο κατώτατος αριθμός των απαιτούμενων μεριδίων παραμένει ο ίδιος. Τα Μερίδια Απορρήτου προστατεύονται σύμφωνα με την παρούσα ΔΠΠ.
Κανένας έλεγχος πολλαπλών προσώπων δεν εφαρμόζεται στα ιδιωτικά κλειδιά του Συνδρομητή.

6.2.3 Παρακαταθήκη Ιδιωτικού Κλειδιού

Η ΑΠΕΔ και οι εκδότριες ΑΠ δεν τηρούν ιδιωτικά κλειδιά ΑΠ ή Συνδρομητή.

6.2.4 Δημιουργία Εφεδρικού Αντιγράφου Ιδιωτικού Κλειδιού

Δημιουργούνται εφεδρικά αντίγραφα των ιδιωτικών κλειδιών ΑΠ και των ιδιωτικών κλειδιών των Συνδρομητών που δημιουργούνται και αποθηκεύονται από μία εξ αποστάσεως ΕΔΔΥ, για την περίπτωση ανάκτησης (τακτικής ή έκτακτης). Τα κλειδιά αυτά αποθηκεύονται σε κρυπτογραφημένη μορφή εντός κρυπτογραφικών μονάδων οι οποίες πληρούν τις προδιαγραφές της §6.2.1 της ΠΠ. Τα ιδιωτικά κλειδιά ΑΠ αντιγράφονται σε εφεδρικές κρυπτογραφικές μονάδες σύμφωνα με την §6.2.5 της ΠΠ. Τα ιδιωτικά κλειδιά του Συνδρομητή που αποθηκεύονται σε ΕΔΔΥ δεν μπορούν να εξαχθούν ή να αποκατασταθούν από την ΕΔΔΥ και δεν δημιουργούνται αντίγραφα ασφαλείας τους.

6.2.5 Αρχειοθέτηση Ιδιωτικών Κλειδιών

Με το τέλος της περιόδου ισχύος τους το ζεύγος κλειδιών της ΑΠΕΔ και των εκδοτριών ΑΠ αρχειοθετείται για χρονικό διάστημα τουλάχιστον 5 ετών. Το αρχειοθετημένο ζεύγος κλειδιών ΑΠ αποθηκεύεται με ασφαλή τρόπο με τη χρήση 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.
Η ΑΠΕΔ και οι εκδότριες ΑΠ δεν αρχειοθετούν αντίγραφα των ιδιωτικών κλειδιών Συνδρομητή.

6.2.6 Μεταφορά Ιδιωτικού Κλειδιού Από και Προς Μια Κρυπτογραφική Μονάδα

Όταν απαιτείται η μεταφορά ενός εφεδρικού αντιγράφου ζεύγους κλειδιών ΑΠ σε άλλη κρυπτογραφική μονάδα, 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.
Όταν για τα ζεύγη κλειδιών του Συνδρομητή δημιουργούνται αντίγραφα ασφάλειας σε άλλες κρυπτογραφικές μονάδες υλικού, η μεταφορά τους μεταξύ των μονάδων πραγματοποιείται σε κρυπτογραφημένη μορφή.

6.2.7 Αποθήκευση Ιδιωτικού Κλειδιού σε Κρυπτογραφική Μονάδα

Τα ιδιωτικά κλειδιά που βρίσκονται σε κρυπτογραφικές μονάδες υλικού, τηρούνται σε κρυπτογραφημένη μορφή.

6.2.8 Μέθοδος Ενεργοποίησης Ιδιωτικού Κλειδιού

Οι Συνδρομητές που αποκτούν Πιστοποιητικά σύμφωνα με την ΠΠ ή/και στις περιπτώσεις που το απαιτεί η εκδότρια ΑΠ, πρέπει να ακολουθούν της οδηγίες έκδοσης Πιστοποιητικού που είναι αναρτημένες στη διεύθυνση www.aped.gov.gr. Παράλληλα θεωρείται υποχρεωτική από τους Συνδρομητές:

- Η χρήση του συνθηματικού πρόσβασης στην ΕΔΔΥ 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 ταυτότητάς 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.

Ένα ιδιωτικό κλειδί της ΑΠ σε σύνδεση (online) ενεργοποιείται από έναν ορισμένο αριθμό Κατόχων Μεριδίων, όπως ορίζεται στην ενότητα 6.2.2, παρέχοντας τα δεδομένα ενεργοποίησης (τα οποία είναι αποθηκευμένα σε ασφαλή μέσα). Μόλις ενεργοποιηθεί το ιδιωτικό κλειδί, μπορεί να παραμείνει ενεργό για απεριόριστο χρονικό διάστημα έως ότου απενεργοποιηθεί όταν η ΑΠ βρεθεί εκτός σύνδεσης (offline). Παρομοίως, ένας ορισμένος αριθμός Κατόχων Μεριδίων πρέπει να παράσχει τα δεδομένα ενεργοποίησής τους προκειμένου να ενεργοποιηθεί το ιδιωτικό κλειδί της ΑΠ που βρίσκεται εκτός σύνδεσης (offline). Μόλις ενεργοποιηθεί το ιδιωτικό κλειδί, παραμένει ενεργό μόνο για μία μόνο σύνδεση.

6.2.9 Μέθοδος Απενεργοποίησης Ιδιωτικού Κλειδιού

Τα ιδιωτικά κλειδιά ΑΠ απενεργοποιούνται με την αφαίρεση τους από τη συσκευή ανάγνωσης.
Τα ιδιωτικά κλειδιά Συνδρομητών μπορούν να απενεργοποιηθούν με την αφαίρεση της ΕΔΔΥ από το σταθμό εργασίας ή κατά την αποσύνδεση από την εξ αποστάσεως ΕΔΔΥ. Σε κάθε περίπτωση οι Συνδρομητές έχουν υποχρέωση να προστατεύουν επαρκώς τα ιδιωτικά κλειδιά τους σύμφωνα με την §6.4 της ΠΠ.

6.2.10 Μέθοδος Καταστροφής Ιδιωτικού Κλειδιού

Όταν απαιτείται, η ΑΠΕΔ καταστρέφει τα ιδιωτικά κλειδιά της ΑΠ και των Συνδρομητών κατά τρόπο που εύλογα να διασφαλίζεται ότι δεν θα παραμείνουν μέρη του κλειδιού τα οποία θα μπορούσαν να οδηγήσουν στην ανασύνθεσή του. Η ΑΠΕΔ χρησιμοποιεί τη λειτουργία διαγραφής ευαίσθητων παραμέτρων των κρυπτογραφικών μονάδων υλικού της καθώς και άλλα κατάλληλα μέσα ώστε να εξασφαλίσει την ολοκληρωτική καταστροφή των ιδιωτικών κλειδιών. Οι ενέργειες καταστροφής κλειδιών της ΑΠ καταγράφονται κατά την εκτέλεσή τους.
Τα ιδιωτικά κλειδιά των Συνδρομητών που βρίσκονται σε τοπική ΕΔΔΥ μπορούν να καταστραφούν με αρχικοποίηση της ΕΔΔΥ ή με φυσική καταστροφή ή πρόκληση φθοράς της ΕΔΔΥ.

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 Συνδρομητών δημιουργούνται αντίγραφα ασφαλείας τα οποία αρχειοθετούνται ως μέρος της τακτικής διαδικασίας δημιουργίας αντιγράφων.
Όλα τα δημόσια κλειδιά των Συνδρομητών φυλάσσονται στη βάση δεδομένων της ΑΠΕΔ και μπορούν να αρχειοθετηθούν για τουλάχιστον επτά (7) έτη μετά τη λήξη του εκάστοτε πιστοποιητικού του Συνδρομητή.

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)	Μέχρι 20 έτη
Εκδότριας ΑΠ	Μέχρι 10 έτη
Συνδρομητή	Μέχρι 3 έτη

Η ΑΠΕΔ και οι εκδότριες ΑΠ παύουν να χρησιμοποιούν τα ζεύγη κλειδιών ΑΠ μετά τη λήξη της περιόδου χρήσης τους.
Οι Συνδρομητές παύουν τη χρήση των ζευγών κλειδιών τους μετά τη λήξη των περιόδων χρήσης τους.
Εάν ένας αλγόριθμος ή το ανάλογο μήκος κλειδιού δεν προσφέρει επαρκή ασφάλεια κατά την περίοδο ισχύος του πιστοποιητικού, το εν λόγω πιστοποιητικό θα ανακαλείται και θα δρομολογείται μια νέα αίτηση για πιστοποιητικό.
Η εφαρμοσιμότητα των κρυπτογραφικών αλγορίθμων και παραμέτρων εποπτεύεται συνεχώς από την ΑΠΕΔ.

6.4 Δεδομένα Ενεργοποίησης

6.4.1 Δημιουργία και Εγκατάσταση Δεδομένων Ενεργοποίησης

Τα δεδομένα ενεργοποίησης που χρησιμοποιούνται (PIN) για την προστασία των τοπικών ΕΔΔΥ που περιέχουν τα ιδιωτικά κλειδιά του Υποκειμένου, παράγονται σύμφωνα με το αντίστοιχο εγχειρίδιο της ΕΔΔΥ.
Τα προκαθορισμένα δεδομένα ενεργοποίησης πρέπει να αλλάζουν αμέσως πριν από την παραγωγή κλειδιών από τους Συνδρομητές. Τα δεδομένα ενεργοποίησης (κωδικός χρήστη, κωδικός πρόσβασης και κωδικός μιας χρήσης) για την προστασία των εξ αποστάσεως ΕΔΔΥ, που περιέχουν τα ιδιωτικά κλειδιά του Υποκειμένου, δημιουργούνται σύμφωνα με τις απαιτήσεις συμμόρφωσης της ΕΔΔΥ για την επίτευξη αποκλειστικού ελέγχου από τον υπογράφοντα με υψηλό επίπεδο διασφάλισης, κατά τα οριζόμενα στον Κανονισμό eIDAS, Άρθρο 26, παρ.γ.

6.4.2 Προστασία Δεδομένων Ενεργοποίησης

Οι Συνδρομητές οφείλουν να λαμβάνουν κάθε απαραίτητο μέτρο για τη διαφύλαξη και μη γνωστοποίηση των δεδομένων ενεργοποίησης των ιδιωτικών τους κλειδιών. Απομνημονεύουν τους κωδικούς ενεργοποίησης, (PIN, PUK, κωδικός χρήστη, κωδικός πρόσβασης και κωδικός μιας χρήσης) και δεν τους κοινοποιούν σε κανέναν άλλον.

6.4.3 Άλλα θέματα για τα δεδομένα ενεργοποίησης

6.4.3.1 Μετάδοση δεδομένων ενεργοποίησης

Στην περίπτωση μετάδοσης των δεδομένων ενεργοποίησης των ιδιωτικών κλειδιών, οι Συμμετέχοντες προστατεύουν τη μετάδοση χρησιμοποιώντας μεθόδους που παρέχουν προστασία από απώλεια, κλοπή, τροποποίηση, μη εξουσιοδοτημένη γνωστοποίηση ή χρήση των εν λόγω ιδιωτικών κλειδιών.

6.4.3.2 Καταστροφή των δεδομένων ενεργοποίησης

Τα δεδομένα ενεργοποίησης των ιδιωτικών κλειδιών τίθενται εκτός λειτουργίας χρησιμοποιώντας μεθόδους που παρέχουν προστασία από απώλεια, κλοπή, τροποποίηση, μη εξουσιοδοτημένη γνωστοποίηση ή χρήση των ιδιωτικών κλειδιών που προστατεύονται από τα εν λόγω δεδομένα ενεργοποίησης. Μετά το πέρας των περιόδων διατήρησης των αρχείων σύμφωνα με την ενότητα 5.5.2, η ΑΠΕΔ καταστρέφει τα δεδομένα ενεργοποίησης αντικαθιστώντας τα με καινούργια και/ή μέσω της φυσικής καταστροφής τους.

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.
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 Αξιολόγηση Ασφαλείας Υπολογιστών

Καμία διατύπωση.

6.6 Τεχνικοί Έλεγχοι κατά τον Κύκλο Ζωής Πιστοποιητικού

6.6.1 Έλεγχοι Ανάπτυξης Συστήματος

Νέες εκδόσεις λογισμικού αναπτύσσονται και εφαρμόζονται σύμφωνα με τη διαδικασία διαχείρισης αλλαγών.
Καινούριο ή ενημερωμένο λογισμικό το οποίο όταν φορτώνεται για πρώτη φορά παρέχει μια μέθοδο επαλήθευσης ότι το λογισμικό στο σύστημα προέρχεται από έμπιστη πηγή, δεν έχει τροποποιηθεί πριν από την εγκατάσταση και αποτελεί την έκδοση που προορίζεται για τη σχετική χρήση.

6.6.2 Έλεγχοι 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.

6.6.3 Έλεγχοι ασφάλειας κατά τον κύκλο ζωής του πιστοποιητικού

Οι πολιτικές και τα υλικά στοιχεία της ΑΠΕΔ ελέγχονται σε προγραμματισμένα χρονικά διαστήματα ή όταν συντελούνται σημαντικές αλλαγές προκειμένου να διασφαλιστεί η συνέχιση της καταλληλότητας, επάρκειας και αποτελεσματικότητάς τους. Οι διαμορφώσεις των συστημάτων ελέγχονται τουλάχιστον ετησίως για αλλαγές που παραβιάζουν τις πολιτικές ασφαλείας της ΑΠΕΔ.
Η ΑΠΕΔ διαθέτει διαδικασίες για να διασφαλίζει ότι οι ενημερώσεις κώδικα ασφαλείας εφαρμόζονται στο σύστημα πιστοποίησης σε εύλογο χρονικό διάστημα αφού καταστούν διαθέσιμες αλλά το αργότερο εντός έξι μηνών μετά τη διαθεσιμότητα των ενημερώσεων κώδικα ασφαλείας. Οι λόγοι για τη μη εφαρμογή κάποιας ενημέρωσης κώδικα ασφαλείας θα τεκμηριώνονται.

6.7 Έλεγχοι Ασφάλειας Δικτύου

Όλες οι υπηρεσίες εμπιστοσύνης 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 εγκεκριμένων υπογραφών.

6.8 Χρονοσήμανση

Τα αρχεία καταγραφής, τα Πιστοποιητικά, οι ΚΑΠ και άλλες εγγραφές ανάκλησης περιλαμβάνουν πληροφορίες ημερομηνίας και ώρας.

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 (2005): Information Technology – Open Systems Interconnection – The Directory: Authentication Framework, August 2005 και (β) το RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008 ("RFC5280") [Προφίλ Πιστοποιητικού Υποδομής Δημοσίου Κλειδιού Δια-δικτύου X.509 και ΚΑΠ]. Επίσης τα βασικά πεδία των Πιστοποιητικών βρίσκονται σε συμμόρφωση με τον Κανονισμό ΕΕ 910/2014. Αυτό σημαίνει ότι στα Πιστοποιητικά που ακολουθούν την ΠΠ 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 Εγκεκριμένη Ηλεκτρονική Υπογραφή του παρόχου υπηρεσιών εμπιστοσύνης που εκδίδει το πιστοποιητικό.

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 Υποκειμένου (Subject 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.
Key Size (Μέγεθος Κλειδιού)	4096

7.1.1 Αριθμός (-οί) έκδοσης

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

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, των εκδοτριών ΑΠ και Συνδρομητών είναι σύμφωνα με το RFC 5280: InternetX.509 Public Key Infrastructure Certificate and CRL Profile (Προφίλ Πιστοποιητικού Υποδομής Δημοσίου Κλειδιού Διαδικτύου X.509 και ΚΑΠ). Το πεδίο criticality (Κρισιμότητα) της επέκτασης KeyUsage γενικά παίρνει την τιμή True (Αληθές).

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

		Αρχές Πιστοποίησης
Criticality (κρισιμότητα)		**ΑΛΗΘΕΣ (TRUE)**
1	keyCertSign (Κλειδί Υπογραφής Πιστοποιητικού)	Ορίζεται (set)

2	CRLSign (Υπογραφή ΚΑΠ)	Ορίζεται (set)
3	Off-line CRL	Ορίζεται (set)

		Πιστοποιητικό Υπογραφής – Αυθεντικοποίησης Συνδρομητή
Criticality (κρισιμότητα)		**ΑΛΗΘΕΣ (TRUE)**
1	Digital Signature (Ψηφιακή Υπογραφή)	Ορίζεται (set)
2	Non-Repudiation (Μη-Αποποίηση)	Ορίζεται (set)

7.1.2.2 Επέκταση Πολιτικών Πιστοποιητικού (Certificate Policies extension)

Τα Πιστοποιητικά Συνδρομητή X.509 Έκδοσης 3 χρησιμοποιούν την επέκταση «Certificate Policies» (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 “Subject Altetnative Name” υποστηρίζεται για τα πιστοποιητικά X.509 έκδοσης 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 RFC822 Name περιλαμβάνεται προαιρετικά η διεύθυνση ηλεκτρονικής αλληλογραφίας του κατόχου του Πιστοποιητικού.

7.1.2.4 Βασικοί Περιορισμοί (Basic Constraints)

Η ΑΠΕΔ αναγράφει στα Πιστοποιητικά ΥπΑΠ X.509 Έκδοσης 3 την επέκταση Basic Constraints (Βασικοί Περιορισμοί) όπου το πεδίο CA (ΑΠ) έχει οριστεί ως ΑΛΗΘΕΣ (TRUE).
Στα Πιστοποιητικά Συνδρομητή που εκδίδουν οι εκδότριες ΑΠ το πεδίο της επέκτασης “Basic Constraints” (Βασικοί Περιορισμοί) παραμένει κενό υποδηλώνοντας πως έχει οριστεί ως EndEntity (Τελικό Πρόσωπο). Το πεδίο κρισιμότητας (criticality) της επέκτασης “Basic Constraints” ορίζεται ως ΑΛΗΘΕΣ (TRUE) για τα Πιστοποιητικά εκδοτριών ΑΠ και Συνδρομητών.
Τα Πιστοποιητικά εκδοτριών ΑΠ X.509 έκδοσης 3 εκδίδονται ορίζοντας στο πεδίο “Maximum Path Length” 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 “Maximum Path Length” (περιορισμός Μήκους Διαδρομής) την τιμή "0" υποδεικνύοντας ότι μόνο ένα Πιστοποιητικό Συνδρομητή μπορεί να ακολουθήσει τη διαδρομή πιστοποίησης.

7.1.2.5 Ενισχυμένη Χρήση Κλειδιού (Enhanced Key Usage)

Η επέκταση “Enhanced Key Usage” (Εκτεταμένη Χρήση Κλειδιού) χρησιμοποιείται από τις εκδότριες ΑΠ για τα Πιστοποιητικά Συνδρομητών που εκδίδει (X.509`Έκδοσης 3) στις ακόλουθες περιπτώσεις (Πίνακας 10).

Πίνακας 10: Ρυθμίσεις για την Επέκταση - Εκτεταμένη Χρήση Κλειδιού

		Πιστοποιητικό Ηλεκτρονικής Υπογραφής
Criticality (κρισιμότητα)		**ΨΕΥΔΗΣ (FALSE)**
1	ClientAuth (Ταυτοποίηση Χρήστη)	Ορίζεται

2	Document Signing	Ορίζεται
3	Secure email (Προστασία Email)	Ορίζεται

7.1.2.6 Σημεία Διανομής ΚΑΠ (CRL Distribution Points)

Στα Πιστοποιητικά Συνδρομητή περιλαμβάνεται η επέκταση CRL Distribution Points (Σημεία Διανομής ΚΑΠ) η οποία παραπέμπει στο δικτυακό κόμβο (URL) από όπου κάποιο Βασιζόμενο Μέρος 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 έχει τιμή Root SKI, ενώ για τα Πιστοποιητικά των Συνδρομητών έχει τον SKI του εκδότη.

7.1.2.8 Προσδιοριστής Κλειδιού Υποκειμένου (Subject Key Identifier)

Η δυνατότητα χρήσης της επέκτασης Subject Key Identifier (Προσδιοριστής Κλειδιού Υποκειμένου) παρέχεται για το αυτοϋπογραφόμενο Πιστοποιητικό της ΑΠΕΔ, τα Πιστοποιητικά εκδοτριών ΑΠ, και τα Πιστοποιητικά Συνδρομητών. Η μέθοδος δημιουργίας του keyIdentifier (Προσδιοριστής Κλειδιού) υπολογίζεται τουλάχιστον σύμφωνα με τις μεθόδους που περιγράφονται στο RFC 5280 (ασφαλέστερες μέθοδοι δεν αποκλείονται).

7.1.3 Προσδιοριστές Αντικειμένου Αλγορίθμου Υπογραφής (Algorithm Object Identifiers)

Τα Πιστοποιητικά X.509 της ΑΠΕΔ και των εκδοτριών ΑΠ υπογράφονται με sha256WithRSAEncryption σύμφωνα με το RFC 3279.

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.

7.1.5 Προσδιοριστής Αντικειμένου Πολιτικής Πιστοποιητικού (Certificate Policy Object Identifier)

Τα Πιστοποιητικά των Συνδρομητών θα περιλαμβάνουν αναγνωριστικό για την Πολιτική Πιστοποιητικού (Certificate Policy Identifier) που θα ακολουθούν, σύμφωνα με την §1.2.1 της ΠΠ. Τα Πιστοποιητικά ΥπΑΠ της ΑΠΕΔ θα περιλαμβάνουν προσδιοριστή αντικειμένου για την πολιτική πιστοποιητικού (Certificate Policy Identifier), ήτοι 1.2.300.0.110001.2.1.1.

7.2 Προφίλ Καταλόγου Ανακληθέντων Πιστοποιητικών (ΚΑΠ)

Η ΑΠΕΔ και οι εκδότριες ΑΠ εκδίδουν ΚΑΠ οι οποίοι είναι σύμφωνοι με το RFC 3647. 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 sha256WithRSAEncryption σύμφωνα με το RFC 3279
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.
EffectiveDate (Ημερομηνία Ισχύος)	Ημερομηνία έκδοσης του ΚΑΠ. Οι ΚΑΠ της ΑΠΕΔ, και των εκδοτριών ΑΠ ισχύουν με την έκδοσή τους.
NextUpdate (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.
RevokedCertificates (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.509 Έκδοσης 2.

7.3 Προφίλ OCSP

Οι εκδότριες ΑΠ παρέχουν υπηρεσίες OCSP (Πρωτόκολλο Κατάστασης Πιστοποιητικών Δικτύου). Τα Συστήματα Απόκρισης (Responders) OCSP συμμορφώνονται προς το πρότυπο RFC 6960.

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

Πίνακας 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
Validity Start (Ισχύει Από)	Βάσει του Universal Coordinate Time. Κωδικοποίηση σύμφωνα με το RFC 5280.
Validity End (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 CommonName
Public Key Algorithm (Αλγόριθμος Δημόσιου Κλειδιού 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.

7.3.1 Αριθμός(-οι) Έκδοσης

Οι εκδότριες ΑΠ που παρέχουν υπηρεσίες OCSP, εκδίδουν Πιστοποιητικά Έκδοσης 1, όπως προδιαγράφονται στο RFC 6960.

8. Έλεγχος Συμμόρφωσης και Άλλες Αξιολογήσεις

Η ΑΠΕΔ για τις υπηρεσίες εμπιστοσύνης και διαχείρισης κλειδιών που παρέχει, αξιολογείται από ένα ανεξάρτητο φορέα αξιολόγησης συμμόρφωσης σύμφωνα με τον Κανονισμό ΕΕ 910/2014 (eIDAS), την αντίστοιχη νομοθεσία και πρότυπα ή όποτε συντελείται μια σημαντική αλλαγή στις λειτουργίες της Υπηρεσίας Εμπιστοσύνης.
Πέρα από τους ελέγχους συμμόρφωσης, η ΑΠΕΔ δικαιούται να διενεργεί και άλλες επιθεωρήσεις και έρευνες ώστε να διασφαλίσει την αξιοπιστία των Υπηρεσιών Εμπιστοσύνης. Η ΑΠΕΔ δικαιούται να αναθέσει την εκτέλεση των εν λόγω ελέγχων, επιθεωρήσεων και ερευνών σε μια εξωτερική ελεγκτική εταιρεία.
Η ΑΠΕΔ δικαιούται να διενεργεί δεύτερο κύκλο ελέγχων σε αναδόχους που έχουν συνάψει σχέση με την ΑΠΕΔ για να λειτουργούν ως Εντεταλμένα Γραφεία.

8.1 Συχνότητα Ελέγχου Συμμόρφωσης Φορέα

Οι Έλεγχοι Συμμόρφωσης της ΑΠΕΔ διενεργούνται τουλάχιστον σε ετήσια βάση. Οι έλεγχοι διενεργούνται στο πλαίσιο μιας συνεχούς ακολουθίας ελεγκτικών περιόδων όπου η καθεμία δεν ξεπερνά σε διάρκεια το ένα έτος.

8.2 Ταυτότητα/Προσόντα Ελεγκτή

Οι έλεγχοι συμμόρφωσης της ΑΠ της ΑΠΕΔ πραγματοποιούνται από τους εξής:

- εσωτερικούς ελεγκτές,
- τον οργανισμό αξιολόγησης της συμμόρφωσης ο οποίος έχει διαπιστευθεί σύμφωνα με τον κανονισμό (ΕΚ) αριθμ. 765/2008 και το πρότυπο ΕΝ 319 403 ως ικανός να αξιολογεί τη συμμόρφωση των Εγκεκριμένων Παρόχων Υπηρεσιών Εμπιστοσύνης και των Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης που παρέχουν,
- τον Εποπτικό Φορέα.

8.3 Σχέση Ελεγκτή με Ελεγχόμενο

Ο ελεγκτής του οργανισμού αξιολόγησης της συμμόρφωσης πρέπει να είναι ανεξάρτητος από την ΑΠΕΔ και από τα συστήματα της ΑΠΕΔ που αξιολογούνται.
Ο εσωτερικός ελεγκτής δεν ελέγχει τους τομείς της αρμοδιότητάς του.

8.4 Θέματα που Καλύπτει ο Έλεγχος

Αντικείμενο του ελέγχου συμμόρφωσης αποτελούν το πληροφοριακό σύστημα, 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 Ενωσιακό και Εθνικό 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 κατόπιν της εισήγησης του ελεγκτή. Η ΑΠΕΔ αξιολογεί τη σπουδαιότητα των ανεπαρκειών και θέτει σε προτεραιότητα τις ανάλογες ενέργειες που πρέπει να ληφθούν τουλάχιστον κατά το χρονικό περιθώριο που έχει ορίσει ο Εποπτικός Φορέας ή εντός εύλογου χρονικού διαστήματος. Η ΑΠΕΔ είναι σε κάθε περίπτωση αρμόδια για την ανάπτυξη και εφαρμογή του επανορθωτικού σχεδίου δράσης εντός εύλογου χρονικού διαστήματος.
Όταν, κατά τον έλεγχο της ΕΕΤΤ, υπάρχουν ενδείξεις ότι έχουν παραβιαστεί οι κανόνες προστασίας των προσωπικών δεδομένων, ο Εποπτικός Φορέας ενημερώνει τις αρχές προστασίας δεδομένων για τα αποτελέσματα των ελέγχων συμμόρφωσης.

8.6 Επικοινωνία των Αποτελεσμάτων

Το(τα) πιστοποιητικό(ά) για την(τις) υπηρεσία(ες) εμπιστοσύνης, τα οποία βασίζονται σε αποτελέσματα ελέγχου του οργανισμού αξιολόγησης της συμμόρφωσης που διενεργείται σύμφωνα με τον Κανονισμό ΕΕ 910/2014 (eIDAS), την αντίστοιχη νομοθεσία και πρότυπα, δύνανται να δημοσιεύονται στον δικτυακό τόπο της ΑΠΕΔ. Επιπλέον, η ΑΠΕΔ υποβάλλει τη σχετική έκθεση για την αξιολόγηση της συμμόρφωσης στον Εποπτικό Φορέα εντός τριών (3) εργάσιμων ημερών μετά τη λήψη της.

9. Άλλα Επιχειρησιακά και Νομικά Ζητήματα

9.1 Τέλη Παροχής Υπηρεσιών Εμπιστοσύνης

9.1.1 Τέλη Έκδοσης ή Ανανέωσης Πιστοποιητικού

Τα τέλη για την έκδοση ή ανανέωση των Πιστοποιητικών καθορίζονται από την τιμολογιακή πολιτική της ΑΠΕΔ, που δημοσιεύεται στη διεύθυνση www.aped.gov.gr

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 Βασιζόμενα Μέρη.

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 Βασιζόμενα Μέρη. Η ΑΠΕΔ και οι ΥπΑΠ δεν επιτρέπουν την πρόσβαση σε πληροφορίες ανάκλησης ή κατάστασης Πιστοποιητικού στο χώρο αποθήκευσής 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 και οι εκδότριες ΑΠ 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 ή δημιουργία υπάγεται στις διατάξεις του νόμου 4305/31-10-2014 (ΦΕΚ 237 Α').

9.1.5 Πολιτική Επιστροφής Χρημάτων

Δεν εφαρμόζεται.

9.2 Ευθύνες

Το Ελληνικό Δημόσιο ευθύνεται για ζημία που προκλήθηκε από πράξεις ή παραλείψεις των οργάνων της ΑΠΕΔ ή των εκδότριων ΑΠ σε οποιοδήποτε φυσικό ή νομικό πρόσωπο, λόγω μη συμμόρφωσης προς τις υποχρεώσεις που προβλέπονται στον παρόντα κανονισμό, σύμφωνα με το άρθρο 105 του Εισαγωγικού Νόμου του Αστικού Κώδικα (ΕισΝΑΚ).

Οι Γενικοί Όροι και Προϋποθέσεις για τη χρήση Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης περιορίζουν την ευθύνη της ΑΠΕΔ. Οι περιορισμοί ευθύνης περιλαμβάνουν αποκλεισμό έμμεσων, ειδικών, παρεπόμενων και επακόλουθων ζημιών. Ειδικότερα, για την ευθύνη του Ελληνικού Δημοσίου λόγω πράξεων ή παραλείψεων των οργάνων της ΑΠΕΔ, ως προς την τήρηση των διατάξεων της παρούσας ισχύουν τα ακόλουθα:

Το Ελληνικό Δημόσιο δεν ευθύνεται για τυχόν δυσλειτουργία των υπηρεσιών της ΑΠΕΔ σε περιπτώσεις ανωτέρας βίας, όπως ενδεικτικά σεισμοί, πλημμύρες, πυρκαγιές κ.λπ., συμπεριλαμβανόμενων των περιπτώσεων διακοπής της παροχής ηλεκτρικού ρεύματος (black-out), προβλημάτων στα τηλεπικοινωνιακά δίκτυα και γενικότερα όλων των εξωτερικών εμποδίων που μπορεί να εμποδίσουν την ομαλή παροχή των υπηρεσιών της και δεν οφείλονται σε υπαιτιότητά της.

Εξάλλου, ισχύουν και εφαρμόζονται εν προκειμένω, οι διατάξεις της παραγράφου 2 του άρθρου 13 «Ευθύνη και βάρος απόδειξης» του Κανονισμού 910/2014, κατ' εφαρμογή της παρ. 3 του ιδίου άρθρου.

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.
- 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 δεν 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 στη νομοθεσία περί προστασίας των δεδομένων προσωπικού χαρακτήρα. Η ΑΠΕΔ εφαρμόζει πολιτική απορρήτου η οποία βρίσκεται στην εξής διεύθυνση: https://www.aped.gov.gr

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 Συνδρομητών 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 Πληροφορίες που δεν Αντιμετωπίζονται ως Προσωπικά Δεδομένα

Με την επιφύλαξη της ισχύουσας νομοθεσίας, κάθε πληροφορία που δημοσιοποιείται σε ένα πιστοποιητικό δεν θεωρείται απόρρητη.

9.4.4 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.

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

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

9.4.6 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 Συνδρομητών που ακολουθούν την ΠΠ δεν αποκαλύπτονται ποτέ σε τρίτο, συμπεριλαμβανομένης και της ΑΠΕΔ.

9.4.7 Γνωστοποίηση κατόπιν αιτήματος κατόχου

Η πολιτική απορρήτου της ΑΠΕΔ περιλαμβάνει διατάξεις σχετικά με τη γνωστοποίηση των ιδιωτικών πληροφοριών στο άτομο που τις γνωστοποιεί προς την ΑΠΕΔ. Η παρούσα ενότητα υπόκειται στην εφαρμοστέα νομοθεσία περί απορρήτου.

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

Γενικούς Όρους και Προϋποθέσεις. Η ΑΠΕΔ και αντίστοιχα οι εκδότριες ΑΠ χορηγούν πληροφορίες ανάκλησης σε κάθε Βασιζόμενο Μέρος σύμφωνα με τους ισχύοντες Γενικούς Όρους και Προϋποθέσεις.

9.5.2 Δικαιώματα Ιδιοκτησίας επί των Κλειδιών και του Υλικού Κλειδιών

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

9.5.3 Διαδικασίες για την προστασία Συνδρομητών ή Βασιζόμενων Μερών

Η ΑΠΕΔ διασφαλίζει το Συνδρομητή ή Βασιζόμενο Μέρος 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 Συνδρομητές και στα Βασιζόμενα Μέρη, 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.

9.6.2 Δηλώσεις και Εγγυήσεις ΑΕ

Οι ΑΕ των ΥπΑΠ εγγυώνται στους Συνδρομητές και στα Βασιζόμενα Μέρη 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 τους υπαλλήλους 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.

9.6.3 Δηλώσεις και Εγγυήσεις του Συνδρομητή

Ο Συνδρομητής δέχεται/ εγγυάται, κατ` ελάχιστον, ότι:

- Κάθε εγκεκριμένη ηλεκτρονική υπογραφή που δημιουργείται χρησιμοποιώντας το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που αναγράφεται στο Πιστοποιητικό, αποτελεί την εγκεκριμένη ηλεκτρονική υπογραφή του Συνδρομητή, ενώ το Πιστοποιητικό έχει γίνει αποδεκτό και είναι σε ισχύ (δεν έχει λήξει ή ανακληθεί) κατά το χρόνο δημιουργίας αυτής της εγκεκριμένης ηλεκτρονικής υπογραφής.
- Το ιδιωτικό του κλειδί προστατεύεται και κανένα μη εξουσιοδοτημένο πρόσωπο δεν είχε ποτέ πρόσβαση σε αυτό.
- Όλες οι παραδοχές και τα στοιχεία του Συνδρομητή στην Αίτηση για Πιστοποιητικό την οποία έχει υποβάλει είναι αληθή.
- Όλες οι πληροφορίες που παρέχονται από το Συνδρομητή 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 Συνδρομητής δεν αποτελεί ΑΠ, και επομένως δεν χρησιμοποιεί το 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 Βασιζόμενου Μέρους

Οι Όροι Βασιζόμενου Μέρους 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 Βασιζόμενου Μέρους σύμφωνα με την παρούσα ΠΠ.

9.7 Αποποιήσεις Εγγυήσεων

Στην έκταση που επιτρέπεται από την ισχύουσα νομοθεσία, οι Γενικοί Όροι και Προϋποθέσεις Χρήσης Πιστοποιητικών των εκδοτριών ΑΠ, μπορούν να περιέχουν αποποίηση των πιθανών εγγυήσεων τους, περιλαμβανομένων κάθε είδους εγγυήσεων ως προς την εμπορευσιμότητα ή καταλληλότητα για συγκεκριμένο σκοπό, με την επιφύλαξη των καθοριζομένων στην παράγραφο 9.2 της παρούσας.

9.8 Περιορισμοί Ευθύνης

Οι Δηλώσεις Πρακτικής, οι Γενικοί Όροι και Προϋποθέσεις Χρήσης Πιστοποιητικών των εκδοτριών ΑΠ δύνανται, μετά από έγκριση της ΑΠΕΔ, να περιορίζουν την ευθύνη τους περιλαμβάνοντας τον αποκλεισμό έμμεσων, εξαιρετικών, τυχαίων και αποθετικών ζημιών.

9.9 Διάρκεια Ισχύος και Τερματισμός

9.9.1 Έναρξη Ισχύος

Η ισχύς της παρούσας ΠΠ της ΑΠΕΔ, άρχεται με τη δημοσίευση της στο Φύλλο της Εφημερίδας της Κυβέρνησης. Κατόπιν, η παρούσα ΠΠ αναρτάται άμεσα στο 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 Συμμετέχοντες και Βασιζόμενα Μέρη 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 τη μεταξύ τους επικοινωνία καθώς και την επικοινωνία με τους Συνδρομητές και Βασιζόμενα Μέρη τους, όταν αυτό απαιτείται, λαμβάνοντας υπόψη την κρισιμότητα και το σκοπό της επικοινωνίας - ενημέρωσης.

9.11 Τροποποιήσεις

Τροποποιήσεις της παρούσας ΠΠ επιτρέπονται ύστερα από εισήγηση της ΑΠΕΔ. Οι τροποποιήσεις θα είναι είτε υπό μορφή εγγράφου που περιέχει τις τροποποιήσεις της ΠΠ ή με νέα έκδοση της ΠΠ. Η ΑΠΕΔ ενημερώνει την ΕΕΤΤ για νέες ή ενημερωμένες εκδόσεις, σύμφωνα με το άρθρο 24, παρ. 2(α) του κανονισμού EIDAS, τις δημοσιεύει στο ΦΕΚκαι στο τμήμα Χώρου Αποθήκευσης της ΑΠΕΔ για Ενημερώσεις και Ανακοινώσεις επί των Κανονισμών στη διεύθυνση: www.aped.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 Συνδρομητών και Βασιζόμενων Μερών, 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, αφού ενημερώσει την ΕΕΤΤ και ύστερα από προειδοποίηση των Συνδρομητών τουλάχιστον με σχετική ανακοίνωση στο Χώρο Αποθήκευσής της που προορίζεται για Ενημερώσεις και Ανακοινώσεις επί των Κανονισμών στη διεύθυνση: www.aped.gov.gr.

9.11.3 Ανακοίνωση Τροποποιήσεων

Η ΑΠΕΔ ανακοινώνει τις τροποποιήσεις της ΠΠ, αφού ενημερώσει την ΕΕΤΤ, στο τμήμα του Χώρου Αποθήκευσής της που προορίζεται για Ενημερώσεις και Ανακοινώσεις επί των Κανονισμών, στη διεύθυνση: www.aped.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 στο ΦΕΚ και αναρτάται σε ηλεκτρονική μορφή στο Χώρο Αποθήκευσης της ΑΠΕΔ στη διεύθυνση http://pki.aped.gov.gr όπου βρίσκεται διαθέσιμος σε μορφή εγγράφου Adobe Acrobat®.

9.13 Επίλυση Διαφορών

Διαφορές ανάμεσα στην ΑΠΕΔ, τις εκδότριες ΑΠ, τους Συνδρομητές και Βασιζόμενα Μέρη θα επιλύονται σύμφωνα με την ισχύουσα νομοθεσία από τα Ελληνικά Δικαστήρια.

9.14 Εφαρμοστέο Δίκαιο

Η ερμηνεία, η εγκυρότητα, η ισχύς και η εφαρμογή της παρούσας ΠΠ διέπεται από την ενωσιακή 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

1. Εισαγωγή

Η παρούσα Δήλωση Πρακτικής (ΔΠ) των Υποκείμενων Αρχών Πιστοποίησης (ΥπΑΠ) της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ), εξειδικεύει την Πολιτική Πιστοποιητικού (ΠΠ) της ΑΠΕΔ για την Πολιτική Πιστοποιητικών (§1.2.1), και ειδικότερα τους όρους και τις προϋποθέσεις καθώς και τις τεχνικές προδιαγραφές για την έγκριση, έκδοση, χειρισμό, χρήση και ανάκληση των εγκεκριμένων πιστοποιητικών ηλεκτρονικής υπογραφής συνδρομητών.
Ενώ η ΠΠ ορίζει τις απαιτήσεις που πρέπει να πληρούν οι συμμετέχοντες στην ΥΔΚ της ΑΠΕΔ, η παρούσα ΔΠ περιγράφει τον τρόπο με τον οποίο η ΑΠΕΔ πληροί τις εν λόγω απαιτήσεις σύμφωνα με τον Κανονισμό ΕΕ 910/2014 (eIDAS). Πιο συγκεκριμένα, η παρούσα ΔΠ περιγράφει τις πρακτικές που η ΑΠΕΔ εφαρμόζει για τα ακόλουθα:

- την ασφαλή διαχείριση της ΥΔΚ και
- την έκδοση, τη διατήρηση και τη διαχείριση του κύκλου ζωής των Εγκεκριμένων Πιστοποιητικών όπως ορίζονται στον Κανονισμό (ΕΕ) αριθμ. 910/2014.

Η παρούσα ΔΠ συμμορφώνεται με το RFC 3647 της Ομάδας Μελέτης του Internet (IETF) όσον αφορά την ερμηνεία της Πολιτικής Πιστοποιητικών και της Δήλωσης Πρακτικών Πιστοποίησης. Τέλος, η παρούσα Δήλωση Πρακτικής εφαρμόζει και υλοποιεί την Πολιτική Πιστοποιητικού της ΑΠΕΔ εκτός και αν από τις διατάξεις της παρούσας ορίζεται διαφορετικά.

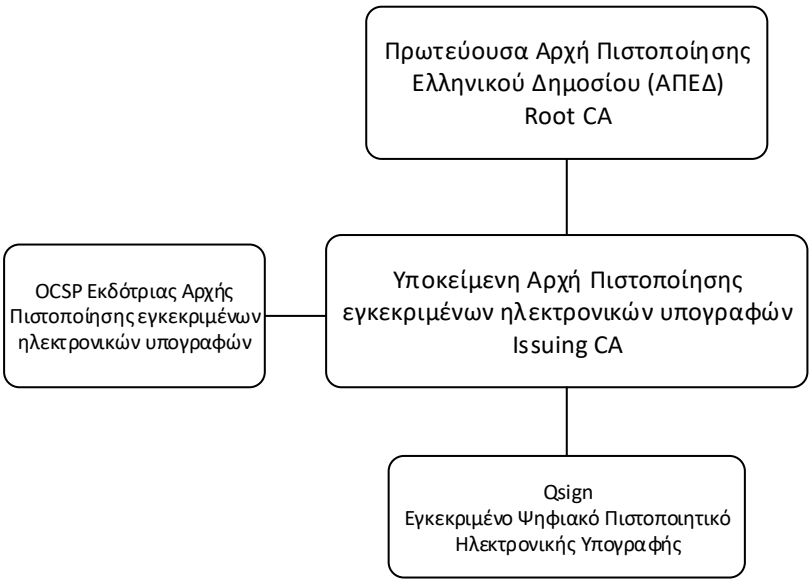
Στη Δήλωση Πρακτικής θα γίνεται ανασκόπηση μία φορά το χρόνο.

1.1 Περίληψη

Η παρούσα Δήλωση Πρακτικής (ΔΠ) καθορίζει:

- Τις υποχρεώσεις των ΥπΑΠ, των Αρχών Εγγραφής (Registration Authorities), των Συνδρομητών και των Βασιζόμενων Μερών.
- Τα θέματα που αφορούν στους Γενικούς Όρους και Προϋποθέσεις Χρήσης Πιστοποιητικών.
- Τις μεθόδους που χρησιμοποιούνται για την επιβεβαίωση της ταυτότητας των Συνδρομητών.
- Τις λειτουργικές διαδικασίες ως προς τις υπηρεσίες κύκλου ζωής Πιστοποιητικού Συνδρομητή: υποβολή αιτήματος για έκδοση, αποδοχή και ανάκληση κλειδιών 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.

Η ΑΠΕΔ εφαρμόζει την ακόλουθη σειρά για την έκδοση εγκεκριμένου πιστοποιητικού ηλεκτρονικής υπογραφής:



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

Πίνακας 1: Διαθέσιμα Έγγραφα Κανονισμών

Έγγραφα	Κατάσταση	Τοποθεσία Δημοσίευσης για το Κοινό
Κανονισμός Πιστοποίησης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ)	Δημόσιο	Χώρος Αποθήκευσης της ΑΠΕΔ, σύμφωνα με την §2.2 της ΠΠ της ΑΠΕΔ
Όροι και Προϋποθέσεις Χρήσης Πιστοποιητικών	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 τη 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 τη 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 πιστοποιητικών ηλεκτρονικής υπογραφής συνδρομητών (έκδοση, ανάκληση, αναστολή και ανανέωση) σύμφωνα με την Πολιτικής Πιστοποίησης της ΑΠΕΔ.

1.2.2 Τιμή Πολιτικής Πιστοποίησης 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 είναι: 1.2.300.0.110001.1.2.1.1.

1.3 Συμμετέχοντες στην Υποδομή Δημοσίου Κλειδιού

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

1.3.1 Αρχές Πιστοποίησης

Αρχή Πιστοποίησης (ΑΠ) είναι η αρχή την οποία εμπιστεύονται οι χρήστες των υπηρεσιών εμπιστοσύνης (δηλαδή οι συνδρομητές, καθώς και τα βασιζόμενα μέρη) για τη δημιουργία και τη χορήγηση πιστοποιητικών. Η ΑΠ έχει τη συνολική ευθύνη για την παροχή των υπηρεσιών εμπιστοσύνης. Ο όρος ΑΠ περιλαμβάνει την υποκατηγορία των εκδοτών που αποκαλούνται ως Πρωτεύουσες Αρχές Πιστοποίησης (ΠΑΠ). Οι ΠΑΠ ενεργούν ως βάσεις (roots). Οι Αρχές Πιστοποίησης της ΑΠΕΔ που εκδίδουν Εγκεκριμένα Πιστοποιητικά σε Συνδρομητές υπάγονται στην ΠΑΠ.
Η ΑΠΕΔ λειτουργεί ως Αρχή Πιστοποίησης που εκδίδει Εγκεκριμένα Πιστοποιητικά βάσει της ακόλουθης ιεραρχικής δομής ΑΠ:

<u>Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ) / ΑΠ Βάσης (Root CA)</u>
CN = APED Global Root CA
O = APED
C = GR
Serial Number = 6780ecc5cd800b2e85773b1a24324287
Thumbprint = 444dae315d00219c6a152f0cc02aae323bf9c6ac

<u>Εκδότρια ΑΠ Εγκεκριμένων Ηλεκτρονικών Υπογραφών (Issuing CA)</u>
CN = APED Qualified eSignature Issuing CA
O = HELLENIC PUBLIC ADMINISTRATION CERTIFICATION AUTHORITY
C = GR
Serial Number = 3be7beb6fa604f85b5a9b7b67beb7756
Thumbprint = 4daf5df29ea6dc58c5c41feafcc7a031f9b2f442

Τα πιστοποιητικά της ΑΠΕΔ εκδίδονται σύμφωνα με τις ακόλουθες πολιτικές πιστοποιητικού:

- OID 1.2.300.0.110001.2.1.1 {iso(1) member-body(2) gr(300) elot(0) ypesdda(110001) APED Trust Services (2) APED Qualified Trust Services (1) Qualified Electronic Signature Policy (1)}
- OID 0.4.0.194112.1.0 {itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural(0)}
- OID 0.4.0.194112.1.2 {itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(194112) policy-identifiers(1) qcp-natural-qscd(2)}
- OID 0.4.0.2042.1.1 {tu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncp(1)}
- OID 0.4.0.2042.1.2 {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus(2)}

1.3.2 Αρχές Εγγραφής

Η Αρχή Εγγραφής είναι η οντότητα που διενεργεί την ταυτοποίηση και επαλήθευση της ταυτότητας των Συνδρομητών για την έκδοση Πιστοποιητικών και προβαίνει σε ή αποδέχεται αιτήσεις ανάκλησης πιστοποιητικών για λογαριασμό της ΑΠ. Η ΑΠΕΔ ενεργεί ως ΑΕ για τα Εγκεκριμένα Πιστοποιητικά που εκδίδει.
Η ΑΠΕΔ έχει την εξουσία να αναθέσει σε τρίτο μέρος την αρμοδιότητα της ταυτοποίησης και επικύρωσης του Συνδρομητή. Στην περίπτωση αυτή, το τρίτο μέρος είναι το Εντεταλμένο Γραφείο (ή Τοπική Αρχή Εγγραφής). Το Εντεταλμένο Γραφείο εκπληρώνει τις αρμοδιότητές του σύμφωνα με την παρούσα ΔΠ.
Η ΑΠΕΔ εκπαιδεύει το εξουσιοδοτημένο προσωπικό όσον αφορά στη διαδικασία επικύρωσης και στις διαδικασίες ασφαλείας πριν από την έναρξη των σχετικών δραστηριοτήτων των Εντεταλμένων Γραφείων. Η ΑΠΕΔ δύναται να διενεργεί ελέγχους στις δραστηριότητες και διαδικασίες των Εντεταλμένων Γραφείων προκειμένου να διασφαλίσει τη συμμόρφωση με την παρούσα ΔΠ.

1.3.3 Εντεταλμένα Γραφεία (ΕΓ)

Ένα Εντεταλμένο Γραφείο (ΕΓ) είναι μια οντότητα που διενεργεί την ταυτοποίηση και την επαλήθευση της ταυτότητας των Συνδρομητών, καθώς και την αρχική εξέταση των σχετικών εγγράφων τους για την έκδοση και την ανάκληση Πιστοποιητικών. Η σχέση μεταξύ του Εντεταλμένου Γραφείου και της ΑΕ περιλαμβάνει, μεταξύ άλλων, τα ακόλουθα:

- τα πλήρη στοιχεία των εξουσιοδοτημένων υπαλλήλων του ΕΓ οι οποίοι θα εκτελούν τα καθήκοντα και τις δραστηριότητες του ΕΓ,
- την υποχρέωση του ΕΓ οι εξουσιοδοτημένοι υπάλληλοί της να λαμβάνουν κατάρτιση από την ΑΠΕΔ αναφορικά με τα καθήκοντα και τις δραστηριότητες του ΕΓ, καθώς και να αποδέχεται τη διενέργεια ελέγχων από την ΑΠΕΔ,
- την υποχρέωση των εξουσιοδοτημένων υπαλλήλων του ΕΓ να χρησιμοποιούν πιστοποιητικά που εκδίδονται από την ΑΠ της ΑΠΕΔ προκειμένου να διασφαλιστεί η ασφαλής επικοινωνία μεταξύ των μερών,
- την υποχρέωση του ΕΓ να διεκπεραιώνει τις αιτήσεις των Συνδρομητών αποκλειστικά μέσω των εξουσιοδοτημένων υπαλλήλων του ΕΓ.

Το Εντεταλμένο Γραφείο υποβάλλει όλες τις αιτήσεις ή τα αιτήματα του Συνδρομητή, συνοδευόμενα με τα σχετικά έγγραφα, στην Αρχή Εγγραφής προς έγκριση ή απόρριψη όσον αφορά την έκδοση ή την ανάκληση Πιστοποιητικών.

1.3.3 Συνδρομητές

Ως Συνδρομητές νοούνται τα φυσικά πρόσωπα, κάτοχοι Πιστοποιητικών σύμφωνα με τις διατάξεις του παρόντος. Ειδικά για τα πιστοποιητικά που εκδίδονται σύμφωνα με την ΠΠ οι Συνδρομητές πρέπει να έχουν δικαιοπρακτική ικανότητα.

1.3.4 Βασιζόμενα Μέρη

Ως Βασιζόμενα Μέρη νοούνται τα φυσικά ή νομικά πρόσωπα που ενεργούν βάσει εμπιστοσύνης σε κάποιο Πιστοποιητικό που έχει εκδοθεί από την ΑΠΕΔ. Το Βασιζόμενο Μέρος μπορεί να είναι, ή και να μην είναι, Συνδρομητής εντός της ΥΔΚ 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 (ΑΠΕΔ). 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 στην παρακάτω ιστοσελίδα:

- www.aped.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

Η ΑΠΕΔ διατηρεί ένα δικτυακά προσπελάσιμο αποθηκευτικό χώρο σε ένα δημόσιο δίκτυο επικοινωνίας δεδομένων (https://pki.aped.gov.gr/repository) που επιτρέπει στα Βασιζόμενα Μέρη να υποβάλουν διαδικτυακά ερωτήματα αναφορικά με την ανάκληση και άλλες πληροφορίες σχετικά με την κατάσταση του Πιστοποιητικού. Η ΑΠΕΔ παρέχει στα Βασιζόμενα Μέρη πληροφορίες σχετικά με τον τρόπο αναζήτησης του κατάλληλου δικτυακού χώρου αποθήκευσης για τον έλεγχο της κατάστασης του Πιστοποιητικού, καθώς και τον τρόπο αναζήτησης του αποκριτή OCSP (OCSP responder).

Η ΑΠΕΔ δημοσιεύει στον δημόσιο αποθηκευτικό χώρο πληροφοριών τουλάχιστον τις ακόλουθες πληροφορίες:

- Επισκόπηση της ιεραρχίας πιστοποίησης
- Πολιτικές πιστοποίησης και Δήλωση Πρακτικών Πιστοποίησης
- Αποτελέσματα ελέγχου
- Πιστοποιητικά, συμπεριλαμβανομένων των ΑΠ βάσης και των εκδοτριών ΑΠ.
- Προφίλ
- Γενικοί Όροι και Προϋποθέσεις για τη χρήση εγκεκριμένων υπηρεσιών εμπιστοσύνης
- Κατάλογοι Ανακληθέντων Πιστοποιητικών
- Αναζήτηση πιστοποιητικού
- Πολιτικές Απορρήτου

2.2.1 Δημοσίευση της ΔΠ

Η παρούσα ΔΠ δημοσιεύεται σε ηλεκτρονική μορφή στο δημόσιο χώρο αποθήκευσης πληροφοριών (https://pki.aped.gov.gr/repository) όπου βρίσκεται διαθέσιμη σε μορφή εγγράφου Adobe Acrobat®.

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 Συνδρομητών 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

Η ονοματοδοσία των πιστοποιητικών πραγματοποιείται όπως προβλέπεται στη Σύσταση ITU-T X.509 [6] ή στο RFC 5280 [7] της Ομάδας Μελέτης του Internet και στο σχετικό μέρος του προτύπου ETSI EN 319 412.

3.1.1 Τύποι Ονομάτων

Ο τύπος των ονομάτων που αποδίδονται στην ΑΠ και τους Συνδρομητές περιγράφεται στη σχετική δημοσίευση της τεκμηρίωσης του Προφίλ Πιστοποιητικού στο χώρο αποθήκευσης της ΑΠΕΔ. Τα Πιστοποιητικά της ΑΠ της ΑΠΕΔ και του Συνδρομητή περιλαμβάνουν τα Διακριτικά Ονόματα X.501 στα πεδία Εκδότη και Υποκειμένου.

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 Συνδρομητή

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

3.1.4 Μοναδικότητα των Ονομάτων

Σύμφωνα με τα προβλεπόμενα στην §3.1.4 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 §3.2.2 της ΠΠ της ΑΠΕΔ.

3.2.3 Πληροφορίες Συνδρομητή που Δεν Επαληθεύονται

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

3.3 Ταυτοποίηση και Αυθεντικοποίηση για Επαναδημιουργία Κλειδιών

3.3.1 Ταυτοποίηση και Αυθεντικοποίηση για Τακτική Επαναδημιουργία Κλειδιών

Δεν εφαρμόζεται

3.3.1 Ταυτοποίηση και Αυθεντικοποίηση για Επαναδημιουργία Κλειδιών Μετά την Ανάκληση

Σύμφωνα με τα προβλεπόμενα στην §3.3.1 της ΠΠ της ΑΠΕΔ.

3.3 Ταυτοποίηση και Αυθεντικοποίηση για Αίτηση Ανάκλησης

Για την ανάκληση Πιστοποιητικών Συνδρομητών είναι απαραίτητη η ταυτοποίηση του Συνδρομητή σύμφωνα με τις διαδικασίες που περιγράφονται στην §4.9.3. Συγκεκριμένα, για την επαλήθευση ταυτότητας αιτήματος ανάκλησης ενός Συνδρομητή ακολουθείται κατά περίπτωση μια από τις ακόλουθες αποδεκτές διαδικασίες:

- Είσοδος και αυθεντικοποίηση του Συνδρομητή στην ηλεκτρονική διεύθυνση https://services.aped.gov.gr/apedcitizen/login, και εισαγωγή του προσωπικού κωδικού έκδοσης / ανάκλησης εγκεκριμένου πιστοποιητικού στο αντίστοιχο πεδίο της αίτησης ανάκλησης.
    - Αν ο Συνδρομητής δεν έχει αποθηκεύσει ή δεν θυμάται τον προσωπικό κωδικό έκδοσης / ανάκλησης, μπορεί να γίνει υπενθύμιση. Στην περίπτωση αυτή εισάγει τον ΑΦΜ και την ημερομηνία γέννησής του και εφόσον αυτά τα στοιχεία επαληθευτούν, αποστέλλεται SMS με τον κωδικό στο κινητό τηλέφωνο που καταχωρήθηκε στην έκδοση του πιστοποιητικού. Αν έχει αλλάξει αριθμό κινητού τηλεφώνου, δεν μπορεί να γίνει τροποποίηση του καταχωρημένου κινητού τηλεφώνου και δεν μπορεί να λάβει τον κωδικό υπενθύμισης.
- Καταχώρηση αίτησης - Υπεύθυνης Δήλωσης ανάκλησης στο gov.gr. Στη συνέχεια ο Συνδρομητής πραγματοποιεί είσοδο και αυθεντικοποίηση στην ηλεκτρονική διεύθυνση https://services.aped.gov.gr/apedcitizen/login και υποβάλλει αίτημα ανάκλησης χρησιμοποιώντας τον κωδικάριθμο της ΥΔ στο gov.gr. Το αίτημα δρομολογείται στην Αρχή Εγγραφής για έγκριση.
- Ανάκληση σε περίπτωση αδυναμίας λειτουργίας της εφαρμογής:

  https://services.aped.gov.gr/apedcitizen/login

Σε περίπτωση αδυναμίας λειτουργίας της ως άνω εφαρμογής, λόγω αιφνίδιου και απρόβλεπτου γεγονότος, ο Συνδρομητής εκδίδει αίτηση/Υπεύθυνη Δήλωση ανάκλησης εγκεκριμένου πιστοποιητικού από την Ενιαία Ψηφιακή Πύλη της Δημόσιας Διοίκησης (gov.gr) και την αποστέλλει μέσω ηλεκτρονικού ταχυδρομείου, στην ηλεκτρονική διεύθυνση aped@mindigital.gr, ή μέσω ταχυδρομείου στο Υπουργείο ψηφιακής Διακυβέρνησης/ΑΠΕΔ, Φραγκούδη 11 και Αλ. Πάντου ΤΚ 17671.

4. Λειτουργικές Απαιτήσεις Κύκλου Ζωής Πιστοποιητικών

4.1 Αίτηση για Έκδοση Πιστοποιητικού

4.1.1 Ποιος Μπορεί να Υποβάλει Αίτηση για Έκδοση Πιστοποιητικού

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

4.1.2 Διαδικασία εγγραφής και υποχρεώσεις

Για τη χορήγηση Πιστοποιητικών Συνδρομητή, όλοι οι Συνδρομητές υποβάλλονται σε διαδικασία εγγραφής και επαλήθευσης της ταυτότητας, η οποία συνίσταται σε:

- Αυθεντικοποίηση και είσοδος στην ηλεκτρονική εφαρμογή διαχείρισης ψηφιακών πιστοποιητικών (https://services.aped.gov.gr/apedcitizen/login), και υποβολή ηλεκτρονικού αιτήματος για την έκδοση πιστοποιητικού συμπληρώνοντας όλα τα υποχρεωτικά πεδία.
- Είτε εξ αποστάσεως ταυτοποίηση είτε φυσική παρουσία του ίδιου του Συνδρομητή στο αρμόδιο Εντεταλμένο Γραφείο ή, αν αυτό κρίνεται απαραίτητο, σε εκπροσώπους της Αρχής Εγγραφής ή της Αρχής Πιστοποίησης, για επιβεβαίωση της ταυτότητας του Συνδρομητή.
- Υποβολή αιτήματος χορήγησης πιστοποιητικού.
- Γραπτή ή ηλεκτρονική αποδοχή των Όρων και Προϋποθέσεων Χρήσης Πιστοποιητικού.
- Παραγωγή ή υποβολή αιτήματος για παραγωγή ζεύγους κλειδιών σύμφωνα με την §6.1 της ΠΠ.
- Αποστολή του δημόσιου κλειδιού από το Συνδρομητή, στην εκδότρια ΑΠ, σύμφωνα με την §6.1.3 της ΠΠ.
- Ο Συνδρομητής 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.

4.2 Επεξεργασία Αίτησης Έκδοσης Πιστοποιητικού

4.2.1 Έγκριση ή Απόρριψη Αίτησης για Έκδοση Πιστοποιητικού Συνδρομητή

Η έγκριση ή απόρριψη αίτησης για έκδοση πιστοποιητικού Συνδρομητή πραγματοποιείται 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

Μετά την έγκριση του αιτήματος έκδοσης εγκεκριμένου πιστοποιητικού ηλεκτρονικής υπογραφής, ο Συνδρομητής λαμβάνει μήνυμα (SMS) από την ΑΕ μέσω αυτοματοποιημένης διαδικασίας για το θετικό αποτέλεσμα της επεξεργασίας της αίτησης που υπέβαλε. Το μήνυμα αποστέλλεται στον αριθμό κινητού τηλεφώνου που συμπληρώθηκε στην αίτηση έκδοσης πιστοποιητικού που υπέβαλλε.

Κατόπιν ο Συνδρομητής πρέπει να συνδεθεί στην ηλεκτρονική εφαρμογή διαχείρισης ψηφιακών πιστοποιητικών και να προχωρήσει στη δημιουργία και έκδοση του εγκεκριμένου πιστοποιητικού ηλεκτρονικής υπογραφής στην ΕΔΔΥ που έχει στην κατοχή του.

4.3.1 Ενέργειες της εκδότριας ΑΠ κατά την Έκδοση Πιστοποιητικού Συνδρομητή

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

4.3.2 Ενημέρωση του Συνδρομητή για την Έκδοση Πιστοποιητικού

Οι ΥπΑΠ ενημερώνουν τους Συνδρομητές για τη διαδικασία έκδοσης των εγκεκριμένων πιστοποιητικών ηλεκτρονικής υπογραφής, για τη διαθεσιμότητα αυτών και τους τρόπους παραλαβής των μέσα από τη διεύθυνση http://www.aped.gov.gr. Οι σχετικές πληροφορίες είναι επίσης διαθέσιμες στον ενδιαφερόμενο κατόπιν εισόδου του στην ηλεκτρονική εφαρμογή διαχείρισης ψηφιακών πιστοποιητικών (https://services.aped.gov.gr/apedcitizen/login).

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.

4.5 Ζεύγος κλειδιών και Χρήση Πιστοποιητικών

4.5.1 Χρήση Ιδιωτικού Κλειδιού και Πιστοποιητικού από Συνδρομητή

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

4.5.2 Χρήση Δημοσίου Κλειδιού και Πιστοποιητικού από Βασιζόμενο Μέρος

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

4.6 Ανανέωση Πιστοποιητικού

Δεν εφαρμόζεται.

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 στο Συνδρομητή 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.

4.7.7 Ενημέρωση Άλλων Οντοτήτων για την Έκδοση Πιστοποιητικού από την Αρχή Πιστοποίησης

Σύμφωνα με τα προβλεπόμενα στην §4.7.7 της ΠΠ της ΑΠΕΔ

4.8 Μετατροπή Πιστοποιητικού

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

4.9 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

Η υπηρεσία ανάκλησης είναι διαθέσιμη 7 ημέρες τη βδομάδα, όλο το εικοσιτετράωρο. Ένας Συνδρομητής που επιθυμεί ανάκληση του Πιστοποιητικού του πρέπει να υποβάλει αίτημα ανάκλησης με τους παρακάτω τρόπους:

- Στη διεύθυνση https://services.aped.gov.gr/apedcitizen/login, όπου η υποβολή του αιτήματος επιτρέπεται μόνο κατόπιν αυθεντικοποίησής του στο σύστημα και με τη χρήση του προσωπικού κωδικού έκδοσης / ανάκλησης εγκεκριμένου πιστοποιητικού στο αντίστοιχο πεδίο της αίτησης ανάκλησης.
- Με Υπεύθυνη Δήλωση ανάκλησης στο gov.gr και αίτηση στη διεύθυνση https://services.aped.gov.gr/apedcitizen/login. Η αίτηση έπειτα δρομολογείται στην Αρχή Εγγραφής για έγκριση.
- Ανάκληση σε περίπτωση αδυναμίας λειτουργίας της εφαρμογής:
  https://services.aped.gov.gr/apedcitizen/login
  Σε περίπτωση αδυναμίας λειτουργίας της ως άνω εφαρμογής, λόγω αιφνίδιου και απρόβλεπτου γεγονότος, ο Συνδρομητής εκδίδει αίτηση/Υπεύθυνη Δήλωση ανάκλησης εγκεκριμένου πιστοποιητικού από την Ενιαία Ψηφιακή Πύλη της Δημόσιας Διοίκησης (gov.gr) και την αποστέλλει μέσω ηλεκτρονικού ταχυδρομείου, στην ηλεκτρονική διεύθυνση aped@mindigital.gr, ή μέσω ταχυδρομείου στο Υπουργείο ψηφιακής Διακυβέρνησης/ΑΠΕΔ, Φραγκούδη 11 και Αλ. Πάντου ΤΚ 17671.

4.9.4 Χρονικό Διάστημα Μέσα στο Οποίο η ΑΠ 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 Βασιζόμενα Μέρη

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

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.

4.10 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.

5. Φυσικά, Διαδικαστικά Μέτρα Προστασίας και Ασφάλειας

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

6. Τεχνικά Μέτρα Ασφαλείας

Σύμφωνα με τα προβλεπόμενα στην §6 της ΠΠ της ΑΠΕΔ.

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 Εμπιστοσύνης

Σύμφωνα με τα προβλεπόμενα στην §9.1 της ΠΠ της ΑΠΕΔ.

9.2 Ευθύνες

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

9.3 Εμπιστευτικότητα Πληροφοριών

Σύμφωνα με τα προβλεπόμενα στην §9.3 της ΠΠ της ΑΠΕΔ.

9.4 Προστασία Δεδομένων Προσωπικού Χαρακτήρα

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

9.5 Δικαιώματα Πνευματικής Ιδιοκτησίας

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

9.6 Δηλώσεις και Εγγυήσεις

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

9.7 Αποποιήσεις Εγγυήσεων

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

9.8 Περιορισμοί Ευθύνης

Σύμφωνα με τα προβλεπόμενα στην §9.8 της ΠΠ της ΑΠΕΔ

9.9 Διάρκεια Ισχύος και Τερματισμός

9.9.1 Έναρξη Ισχύος

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

9.9.2 Λήξη Ισχύος

Η παρούσα ΔΠ θα παραμείνει εν ισχύ έως την αντικατάστασή 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 ΔΠ, η ΥπΑΠ, οι Συνδρομητές και τα Βασιζόμενα Μέρη 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

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

9.11 Τροποποιήσεις

Σύμφωνα με τα προβλεπόμενα στην §9.11 της ΠΠ της ΑΠΕΔ.

9.12 Πολιτική Δημοσίευσης και Κοινοποίησης

Σύμφωνα με τα προβλεπόμενα στην §9.12 της ΠΠ της ΑΠΕΔ.

9.13 Επίλυση Διαφορών

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

9.14 Εφαρμοστέο Δίκαιο

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

9.15 Ανωτέρα Βία

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

Γ. Πολιτική Πιστοποιητικού & Δήλωση Πρακτικών Πιστοποίησης Αρχής Χρονοσφραγίδας

1. Εισαγωγή

Με τον παρόντα Κανονισμό Πιστοποίησης της ΑΠΕΔ καθορίζονται οι όροι, οι προϋποθέσεις και οι διαδικασίες για την παροχή υπηρεσιών εμπιστοσύνης από την Αρχή Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ),) σύμφωνα με το άρθρο 58 του ν. 4727/2020. 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 στην παρούσα ενότητα, με τις διατάξεις της οποίας καθορίζονται οι πολιτικές και πρακτικές που εφαρμόζονται για την παροχή υπηρεσιών χρονοσήμανσης από την ΑΠΕΔ, ως Πάροχος Υπηρεσιών Χρονοσήμανσης (ΠΥΧ).
Η ΑΠΕΔ εφαρμόζει ένα έμπιστο και αξιόπιστο σύστημα ακριβούς χρόνου για την παροχή υπηρεσιών χρονοσήμανσης και λαμβάνει όλα τα αναγκαία μέτρα για τη διασφάλιση της εμπιστευτικότητας και τη διατήρηση της ακεραιότητας των ιδιωτικών κρυπτογραφικών κλειδιών ως ΠΥΧ.
Η παρούσα ενότητα αφενός εξειδικεύει την Πολιτική Πιστοποιητικών της ΑΠΕΔ ως προς τις παρεχόμενες από αυτή Υπηρεσίες Εγκεκριμένων Χρονοσφραγίδων, αφετέρου ορίζει τη Δήλωση Πρακτικών Πιστοποίησης της Αρχής Χρονοσφραγίδας.

2. Γενικές Έννοιες

2.1 Υπηρεσίες Χρονοσφραγίδας

Οι Υπηρεσίες Εγκεκριμένων Χρονοσφραγίδων της ΑΠΕΔ αποτελούνται από τη διαχείριση της υποδομής και την παροχή Χρονοσφραγίδας. Παρέχονται από την Αρχή Χρονοσφραγίδας της ΑΠΕΔ (ΑΧ) στα Βασιζόμενα Μέρη και αποτελούν αναπόσπαστο μέρος της Υποδομής Δημοσίου Κλειδιού (ΥΔΚ) της ΑΠΕΔ και είναι σύμφωνες με τον Κανονισμό ΕΕ 910/2014 (eIDAS) και το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI). Οι Υπηρεσίες Εγκεκριμένης Χρονοσφραγίδας διασφαλίζουν τη χρήση αξιόπιστης πηγής χρόνου και την κατάλληλη διαχείριση όλων των στοιχείων του συστήματος.

2.2 Αρχή Χρονοσφραγίδας

Η Αρχή Χρονοσφραγίδας της ΑΠΕΔ είναι υπεύθυνη για την παροχή Υπηρεσίας Εγκεκριμένης Χρονοσφραγίδας όπως περιγράφεται στο παρόν έγγραφο. Έχει την ευθύνη για τη λειτουργία των σχετικών Μονάδων Χρονοσφραγίδας (ΜΧ) που δημιουργούνται και υπογράφονται εκ μέρους της ΑΧ. Η υπεύθυνη οντότητα για την ΑΧ είναι η ΑΠΕΔ ενεργούσα ως ΕΠΥΧ.

Η ΑΠΕΔ εκδίδει Εγκεκριμένες Χρονοσφραγίδες κατά την παρακάτω ιεραρχία:

Αρχή Πιστοποίησης (ΑΠ) Βάσης (Root CA)
CN = APED Global Root CA
O = APED
C = GR
Serial Number = 6780ecc5cd800b2e85773b1a24324287
Thumbprint = 444dae315d00219c6a152f0cc02aae323bf9c6ac

ΑΠ Αρχής Χρονοσφραγίδας (ΑΧ) (Time Stamping Authority CA)
CN = APED Qualified Timestamping Issuing CA
O = HELLENIC PUBLIC ADMINISTRATION CERTIFICATION AUTHORITY
C = GR
Serial Number = 28901421ae97b7d47c4cc4eb60ea0597

Thumbprint = 59cd4e7b30478a8c907459f0a38337d1d64ce4e3

Οι χρονοσφραγίδες της ΑΧ της ΑΠΕΔ εκδίδονται σύμφωνα με τις παρακάτω πολιτικές πιστοποιητικού:

- OID 1.2.300.0.110001.2.1.2: {iso(1) member-body(2) gr(300) elot(0) ypesdda(110001) APED Trust Services (2) APED Qualified Trust Services (1) Qualified Time Stamping Policy (2)}
- OID 0.4.0.2023.1.1: {itu-t(0) identifiedorganization(4) etsi(0) time-stamp-policy(2023) policyidentifiers(1) baseline-ts-policy (1)}
- OID 0.4.0.2042.1.2: {itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncpplus(2)}

QcStatements πιστοποιητικού:

- OID 0.4.0.1862.1.1: {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcCompliance(1)}
- OID 0.4.0.1862.1.4: {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) 4}
- OID 0.4.0.1862.1.5: {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcPDS(5)}

2.3 Συνδρομητές

Ως Συνδρομητές νοούνται τα φυσικά πρόσωπα, κάτοχοι εγκεκριμένων πιστοποιητικών ηλεκτρονικής υπογραφής, στους οποίους παρέχεται η χρονοσφραγίδα.

2.3.1 Βασιζόμενα Μέρη

Ένα Βασιζόμενο Μέρος είναι ένα άτομο ή μια οντότητα που λαμβάνει ένα ψηφιακό έγγραφο που φέρει χρονοσφραγίδα και λειτουργεί με βάση ένα πιστοποιητικό ή/και μια ψηφιακή υπογραφή που εκδίδεται υπό την ΑΧ. Ένα Βασιζόμενο μέρος πρέπει να αξιολογεί την ορθότητα και εγκυρότητα του ίδιου του εγγράφου στο πλαίσιο που χρησιμοποιείται.

2.3.2 Άλλοι Συμμετέχοντες

Δεν εφαρμόζεται.

2.3.3 Χρήση Χρονοσφραγίδων

Οι Χρονοσφραγίδες που εκδίδονται από την ΑΠΕΔ, όπως ορίζεται στο παρόν έγγραφο, είναι εγκεκριμένες σύμφωνα με το στ. 34) του άρθρου 3 του Κανονισμού eIDAS. Οι Χρονοσφραγίδες θα χρησιμοποιούνται μόνο στο βαθμό που η χρήση τους είναι σύμφωνη με το εφαρμοστέο δίκαιο και εντός των ορίων και του περιεχομένου που καθορίζονται στο παρόν έγγραφο. Απαγορεύεται οποιαδήποτε χρήση εκτός των ορίων αυτών ή για παράνομους σκοπούς ή αντίθετα προς το δημόσιο συμφέρον ή για σκοπούς που ενδέχεται να βλάψουν την ΑΠΕΔ. Ενδεικτικά, η χρήση των Χρονοσφραγίδων απαγορεύεται για οποιονδήποτε από τους ακόλουθους σκοπούς:

- παράνομη δραστηριότητα (συμπεριλαμβανομένων των επιθέσεων στον κυβερνοχώρο)
- έκδοση νέων Χρονοσφραγίδων και πληροφοριών σχετικά με την ισχύ της χρονοσφραγίδας
- χρήση της Χρονοσφραγίδας για τη χρονοσφράγιση εγγράφων που μπορεί να προκαλέσουν ανεπιθύμητες συνέπειες (συμπεριλαμβανομένης της χρονοσφράγισης των εν λόγω εγγράφων για δοκιμαστικούς σκοπούς).

2.4 Πολιτική Χρονοσφραγίδας και Δήλωση Πρακτικών ΑΧ

2.4.1 Σκοπός

Η παρούσα ενότητα καθορίζει τις απαιτήσεις πολιτικής και ασφάλειας που σχετίζονται με τις πρακτικές λειτουργίας και διαχείρισης της ΑΠΕΔ ως Αρχή Χρονοσφραγίδας (ΑΧ) για την έκδοση Εγκεκριμένων Χρονοσφραγίδων. Αυτές μπορούν να χρησιμοποιηθούν ως υποστήριξη ηλεκτρονικών υπογραφών ή σε οποιαδήποτε εφαρμογή που απαιτεί

απόδειξη ότι υπήρχε ένα δεδομένο πριν από μία συγκεκριμένη χρονική στιγμή. Επιπλέον μπορεί να χρησιμοποιηθεί από ανεξάρτητες οντότητες ως βάση για να επιβεβαιωθεί ότι η ΑΧ της ΑΠΕΔ αποτελεί αξιόπιστη οντότητα για την έκδοση Εγκεκριμένων Χρονοσφραγίδων σύμφωνα με τον Κανονισμό eIDAS.

2.4.2 Επίπεδο εξειδίκευσης

Περιγράφονται μόνο οι γενικοί κανόνες έκδοσης και διαχείρισης των ΔΧ. Λεπτομερής περιγραφή της υποδομής και συναφείς επιχειρησιακές διαδικασίες περιγράφονται σε πρόσθετα έγγραφα που δεν δημοσιοποιούνται.

3. Πολιτικές Χρονοσφραγίδας

3.1 Επισκόπηση

Η Πολιτική Χρονοφραγίδας είναι ένα σύνολο κανόνων που αφορά στην έκδοση και διαχείριση των χρονοσημάνσεων που παράγονται από την ΑΠΕΔ ως ΕΠΥΧ για τους Συνδρομητές. Οι υπηρεσίες χρονοσήμανσης περιλαμβάνουν την οργάνωση της υποδομής και την έκδοση χρονοσφραγίδων. Οι συγκεκριμένες υπηρεσίες παρέχονται από την ΑΠΕΔ στους Συνδρομητές στο πλαίσιο λειτουργίας της υποδομής δημοσίου κλειδιού της ΑΠΕΔ. Οι υπηρεσίες παρέχονται κυρίως για την υποστήριξη εγκεκριμένων ηλεκτρονικών 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.

Οι χρονοσφραγίδες παράγονται από την ΑΠΕΔ μέσω του παρακάτω συνδέσμου: https://timestamp.aped.gov.gr/qtss.

Η παρούσα Πολιτική ορίζει το σύνολο των κανόνων που χρησιμοποιούνται κατά την έκδοση ενός ΔΧ και ρυθμίζει το επίπεδο ασφάλειας της ΑΧ της ΑΠΕΔ. Η ΑΧ ΑΠΕΔ εκδίδει ΔΧ σύμφωνα με το πρότυπο ETSI EN 319 422. Τα ΔΧ εκδίδονται με ακρίβεια ενός (1) δευτερόλεπτου. Οι Χρονοσφραγίδες ζητούνται μέσω Hypertext Transfer Protocol (HTTP), όπως περιγράφεται στο RFC 3161.

3.2 Αναγνώριση

Το Αναγνωριστικό Αντικειμένου (OID) της Πολιτικής Πιστοποιητικού και Δήλωσης Πρακτικών Πιστοποίησης για Υπηρεσίες Εγκεκριμένης Χρονοσφραγίδας της ΑΠΕΔ είναι 1.2.300.0.110001.2.1.2.

Αυτό το Αναγνωριστικό αναφέρεται σε κάθε Χρονοσφραγίδα εκδοθείσα από την ΑΠΕΔ και η Πολιτική Πιστοποιητικού και η Δήλωση Πρακτικών Πιστοποίησης για Υπηρεσίες Εγκεκριμένης Χρονοσφραγίδας της ΑΠΕΔ είναι διαθέσιμες και στους Συνδρομητές και στα Βασιζόμενα Μέρη.

Η Πολιτική Πιστοποιητικού και η Δήλωση Πρακτικών Πιστοποίησης για Υπηρεσίες Εγκεκριμένης Χρονοσφραγίδας της ΑΠΕΔ βασίζονται στην Πολιτική Βέλτιστων Πρακτικών Χρονοσφραγίδας (ΠΒΠΧ) ETSI (OID 0.4.0.2023.1.1).

3.3 Κοινότητα Χρηστών και Εφαρμογή

Δεν υπάρχουν περιορισμοί όσον αφορά στην επιλεξιμότητα των χρηστών ή στην εφαρμογή των υπηρεσιών που παρέχονται. Η ΑΧ της ΑΠΕΔ μπορεί να παρέχει Υπηρεσίες Χρονοσφραγίδας ηλεκτρονικών δεδομένων σε οποιονδήποτε χρήστη, συμπεριλαμβανομένων και κλειστών κοινοτήτων.

3.4 Συμμόρφωση

Η ΑΧ της ΑΠΕΔ χρησιμοποιεί το αναγνωριστικό στο ΔΧ όπως αναφέρεται στην παράγραφο 3.2 «Αναγνώριση».

Η ΑΧ της ΑΠΕΔ διασφαλίζει τη συμμόρφωση των παρεχόμενων υπηρεσιών με τους κανονισμούς που ορίζονται στην ενότητα 4.1 «Υποχρεώσεις ΑΧ προς Συνδρομητές» και διασφαλίζει την αξιοπιστία των μηχανισμών ελέγχου που περιγράφονται στην ενότητα Δήλωσης Πρακτικής του παρόντος.

4. Υποχρεώσεις και Ευθύνη

Η ΑΠΕΔ εγγυάται και διασφαλίζει την εφαρμογή της Πολιτικής Χρονοσφραγίδας σύμφωνα με τις διατάξεις της ενότητας 3, καθώς και των απαιτήσεων της ενότητας «Δήλωση Πρακτικής».
Ειδικότερα, ως προς τους Συνδρομητές και Βασιζόμενα Μέρη η ΑΠΕΔ διασφαλίζει ότι η μέγιστη απόκλιση από το UTC ρολόι της πηγής είναι ένα (1) δευτερόλεπτο.
Οι συνδρομητές και τα βασιζόμενα μέρη οφείλουν να επαληθεύουν την εγκυρότητα και την ορθότητα της χρονοσήμανσης.

4.1 Υποχρεώσεις ΑΧ προς Συνδρομητές

Η ΑΠΕΔ εγγυάται τη διαθεσιμότητα κατά 99,00% των υπηρεσιών της ΑΧ της ΑΠΕΔ, λειτουργία 24 ώρες το εικοσιτετράωρο / 7 ώρες την εβδομάδα, εξαιρουμένων των προγραμματισμένων τεχνικών διακοπών που αφορούν στη συντήρηση του εξοπλισμού και του συστήματος.

Η ΑΠΕΔ αναλαμβάνει τις ακόλουθες υποχρεώσεις προς τους Συνδρομητές:

- Να λειτουργεί σύμφωνα με την παρούσα Πολιτική Πιστοποιητικού & Δήλωση Πρακτικών Πιστοποίησης για Υπηρεσίες Χρονοσφραγίδας της ΑΠΕΔ και άλλες σχετικές επιχειρησιακές πολιτικές και διαδικασίες.
- Να διασφαλίζει ότι οι ΜΧ διατηρούν ελάχιστη ακρίβεια χρόνου UTC ± 1 δευτερόλεπτο.
- Να διασφαλίζει σε μόνιμη βάση τη φυσική και λογική ασφάλεια, καθώς και την ακεραιότητα των υλικών, του λογισμικού και των βάσεων δεδομένων που απαιτούνται για τη σωστή λειτουργία των Υπηρεσιών Χρονοσφραγίδας.
- Να παρακολουθεί και να ελέγχει τις Υπηρεσίες Χρονοσφραγίδας και ολόκληρη την υποδομή της ΑΧ, προκειμένου να αποτρέψει ή να περιορίσει οποιαδήποτε διατάραξη ή μη διαθεσιμότητα των Υπηρεσιών Χρονοσφραγίδας.
- Να υπόκειται σε εσωτερικές και εξωτερικές επιθεωρήσεις για να διασφαλίζεται η συμμόρφωση με τη σχετική νομοθεσία.
- Να παρέχει υψηλής διαθεσιμότητας πρόσβαση στα συστήματα της ΑΧ της ΑΠΕΔ εκτός από την περίπτωση προγραμματισμένων τεχνικών διακοπών και απώλειας συγχρονισμού χρόνου.

4.2 Υποχρεώσεις Συνδρομητών

Οι Συνδρομητές πρέπει να επαληθεύουν τις υπογραφές που δημιουργήθηκαν από την ΑΧ ΑΠΕΔ στο ΔΧ.

Η επαλήθευση αυτή περιλαμβάνει:

- Επαλήθευση ότι η υπογραφή της ΑΧ πάνω στο ΔΧ είναι έγκυρη.
- Επαλήθευση του πιστοποιητικού της ΑΧ:
    - Επαλήθευση της αξιόπιστης διαδρομής έως το αξιόπιστο πιστοποιητικό βάσης, και για κάθε ένα από τα πιστοποιητικά της αλυσίδας (συμπεριλαμβανομένου και του πιστοποιητικού της ΑΧ)

4.3 Υποχρεώσεις Βασιζόμενων Μερών

Τα Βασιζόμενα Μέρη θα πρέπει να επαληθεύουν τις υπογραφές που έχουν δημιουργηθεί από την ΑΧ της ΑΠΕΔ πάνω στο ΔΧ.

Η επαλήθευση αυτή περιλαμβάνει:

- Επαλήθευση ότι η υπογραφή της ΑΧ πάνω στο ΔΧ είναι έγκυρη.
- Επαλήθευση του πιστοποιητικού της ΑΧ:

- Επαλήθευση της αξιόπιστης διαδρομής έως το αξιόπιστο πιστοποιητικό βάσης και για κάθε ένα από τα πιστοποιητικά της αλυσίδας (συμπεριλαμβανομένου και του πιστοποιητικού της ΑΧ).
- Επαλήθευση ότι το πιστοποιητικό δεν έχει λήξει τη στιγμή της υπογραφής από την ΑΧ.
- Επαλήθευση εάν το πιστοποιητικό δεν έχει ανακληθεί τη στιγμή της υπογραφής από την ΑΧ.

Τα Βασιζόμενα Μέρη θα πρέπει να λαμβάνουν υπόψη τυχόν περιορισμούς στη χρήση της χρονοσφραγίδας που υποδεικνύεται από την Πολιτική Πιστοποιητικού και τη Δήλωση Πρακτικών Πιστοποίησης για Υπηρεσίες Χρονοσφραγίδας της ΑΠΕΔ. Εάν η επαλήθευση πραγματοποιηθεί μετά τη λήξη της περιόδου ισχύος του πιστοποιητικού, το Βασιζόμενο Μέρος θα πρέπει να ακολουθήσει τις οδηγίες που αναφέρονται στο Παράρτημα Δ΄ του ETSI EN 319 421.

4.4 Ευθύνη

Το Ελληνικό Δημόσιο ευθύνεται για ζημία που προκλήθηκε από πράξεις ή παραλείψεις των οργάνων της ΑΠΕΔ ή των εκδότριων ΑΠ σε οποιοδήποτε φυσικό ή νομικό πρόσωπο, λόγω μη συμμόρφωσης προς τις υποχρεώσεις που προβλέπονται στον παρόντα κανονισμό και τον κανονισμό ΕΕ 910/2014, σύμφωνα με το άρθρο 105 του Εισαγωγικού Νόμου του Αστικού Κώδικα (ΕισΝΑΚ).

Οι Γενικοί Όροι και Προϋποθέσεις για τη χρήση Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης περιορίζουν την ευθύνη της ΑΠΕΔ. Οι περιορισμοί ευθύνης περιλαμβάνουν αποκλεισμό έμμεσων, ειδικών, παρεπόμενων και επακόλουθων ζημιών. Οι περιορισμοί ευθύνης είναι οι ίδιοι ανεξάρτητα από τον αριθμό των Χρονοσφραγίδων ή των αξιώσεων που σχετίζονται με αυτές. Ειδικότερα, για την ευθύνη του Ελληνικού Δημοσίου λόγω πράξεων ή παραλείψεων των οργάνων της ΑΠΕΔ, ως προς την τήρηση των διατάξεων της παρούσας ισχύουν τα ακόλουθα:

Το Ελληνικό Δημόσιο δεν ευθύνεται για τυχόν δυσλειτουργία των υπηρεσιών της ΑΠΕΔ σε περιπτώσεις ανωτέρας βίας, όπως ενδεικτικά σεισμοί, πλημμύρες, πυρκαγιές κ.λπ., συμπεριλαμβανόμενων των περιπτώσεων διακοπής της παροχής ηλεκτρικού ρεύματος (black-out), προβλημάτων στα τηλεπικοινωνιακά δίκτυα και γενικότερα όλων των εξωτερικών εμποδίων που μπορεί να εμποδίσουν την ομαλή παροχή των υπηρεσιών της και δεν οφείλονται σε υπαιτιότητά της.

Εξάλλου, ισχύουν και εφαρμόζονται εν προκειμένω, οι διατάξεις της παραγράφου 2 του άρθρου 13 «Ευθύνη και βάρος απόδειξης» του κανονισμού 910/2014, κατ' εφαρμογή της παρ. 3 του ιδίου άρθρου.

5. Δήλωση Πρακτικής Πιστοποίησης Αρχής Χρονοσφραγίδας

5.1 Δήλωση Πρακτικών και κοινοποίησης

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 διατήρηση της ακρίβειας του ρολογιού.

Η ΑΠΕΔ διασφαλίζει ότι:

- όλα τα αρχεία καταγραφής ελέγχου και συμβάντων της ΑΧ, που αφορούν το πιστοποιητικό της Μονάδα Χρονοσφραγίδας, διατηρούνται για τουλάχιστον επτά (7) χρόνια μετά τη λήξη ισχύος του πιστοποιητικού της ΜΧ.
- όλα τα αρχεία καταγραφής ελέγχου και συμβάντων της ΑΧ, που αφορούν την υπηρεσία χρονοσφραγίδας, διατηρούνται για τουλάχιστον ένα (1) έτος μετά τη λήξη του Πιστοποιητικού της ΜΧ.

Τα πιστοποιητικά ΜΧ ισχύουν για πέντε (5) έτη. Αντικαθίστανται κάθε ένα (1) έτος.

Τα κρυπτογραφικά κλειδιά και τα πιστοποιητικά των εξυπηρετητών χρονοσφραγίδας (Time Stamping Server) παράγονται, αποθηκεύονται και χρησιμοποιούνται σε ασφαλή Μονάδα Ασφάλειας Υλικού (HSM) για την εκτέλεση

λειτουργιών υπογραφής κλειδιών, η οποία συμμορφώνεται τουλάχιστον με το FIPS140-2 επίπεδο 3 ή ισοδύναμο EAL4+ ή υψηλότερο σύμφωνα με τις προδιαγραφές ISO/ IEC15408.

Τα Πιστοποιητικά των Εξυπηρετητών Χρονοσφραγίδας (Time Stamping Server) δημοσιεύονται στο σχετικό κατάλογο της ΥΔΚ της ΑΠΕΔ (https://pki.aped.gov.gr/repository).

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

Πίνακας 1. Προφίλ των Βασικών Πεδίων του Πιστοποιητικού Χρονοσήμανσης

Πεδίο	Τιμή ή Περιορισμός Τιμής
Version (Έκδοση)	3
Serial Number (Αριθμός Σειράς)	Μοναδική τιμή ανά Διακριτικό Όνομα Εκδότη (Issuer DN)
Signature Algorithm (Αλγόριθμος Υπογραφής)	SHA256withRSAEncryption
Issuer DN (Διακριτικό Όνομα Εκδότη)	cn=APED Qualified Timestamping Issuing CA ou=APED PKI Services o=HELLENIC PUBLIC ADMINISTRATION CERTIFICATION AUTHORITY c=GR
Validity Start (Ισχύει Από)	Βάσει του Universal Coordinate Time
Validity End (Ισχύει Μέχρι)	Βάσει του Universal Coordinate Time. Η περίοδος ισχύος δεν υπερβαίνει τη διάρκεια ισχύος του πιστοποιητικού της Πρωτεύουσας Αρχής Πιστοποίησης.
Subject DN (Διακριτικό Όνομα Υποκειμένου)	cn=APED Qualified Timestamping Unit ou=APED PKI Services o=HELLENIC PUBLIC ADMINISTRATION CERTIFICATION AUTHORITY c=GR
Μέγεθος Κλειδιού	2048 bits
Χρήση κλειδιού	Ψηφιακή υπογραφή, Μη αποποίηση
Βελτιωμένη χρήση κλειδιού	Χρονική σήμανση

Η ΑΧ της ΑΠΕΔ κοινοποιεί σε όλους τους Συνδρομητές και τα πιθανά Βασιζόμενα Μέρη τους όρους και προϋποθέσεις σχετικά με τη χρήση των Υπηρεσιών Χρονοσφραγίδας της ΑΠΕΔ. Η Δήλωση Κοινοποίησης της ΑΧ της ΑΠΕΔ συμμορφώνεται με τις απαιτήσεις του ETSI EN 319 421.
Κάποια στοιχεία της Δήλωσης Κοινοποίησης της ΑΧ ΑΠΕΔ αναφέρονται παρακάτω:

- Κάθε ΔΧ που εκδίδεται από την ΑΧ της ΑΠΕΔ περιλαμβάνει το αναγνωριστικό πολιτικής που ορίζεται στην ενότητα 2.2 του παρόντος εγγράφου.
- Οι λειτουργίες κρυπτογραφικού κατακερματισμού (hashing) που χρησιμοποιούνται στη διαδικασία Χρονοσφραγίδας είναι σύμφωνες με τις κανονιστικές απαιτήσεις SHA-256 and SHA-512.
- Η αναμενόμενη περίοδος ισχύος της ΜΧ της ΑΠΕΔ είναι μέχρι πέντε (5) έτη.
- Η ακρίβεια του χρόνου, που παρέχεται σε ένα ΔΧ ρυθμίζεται στην ενότητα 3.1 του παρόντος εγγράφου.
- Οι περιορισμοί στην εφαρμογή που σχετίζονται με το σύστημα της ΑΧ έχουν καθοριστεί στην ενότητα 3.3 του παρόντος εγγράφου.
- Η επαλήθευση του ΔΧ πρέπει να γίνεται με τη χρήση του κατάλληλου λογισμικού.
- Οι υποχρεώσεις των Συνδρομητών περιγράφονται στην ενότητα 4.2 του παρόντος εγγράφου.
- Οι υποχρεώσεις των Βασιζόμενων Μερών περιγράφονται στην ενότητα 4.3 του παρόντος εγγράφου.
- Η ΑΠΕΔ τηρεί ασφαλή αρχεία που σχετικά με τη λειτουργία της ΑΧ της ΑΠΕΔ.

5.2 Κύκλος Διαχείρισης κλειδιού

Η ΑΠΕΔ, ως Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ), υπογράφει το Πιστοποιητικό της Αρχής Χρονοσήμανσης Εγκεκριμένων Ηλεκτρονικών Χρονοσφραγίδων. Τα Πιστοποιητικά της ΑΠΕΔ, καθώς και της Αρχής Χρονοσήμανσης είναι διαθέσιμα στους Συνδρομητές και στα Βασιζόμενα Μέρη διαδικτυακά μέσω των χώρων αποθήκευσης της ΑΠΕΔ, καθώς και ως μέρος της αλυσίδας πιστοποιητικού η οποία ενσωματώνεται στο πιστοποιητικό χρονοσφραγίδας.

5.2.1 Δημιουργία Κλειδιού ΑΧ

Η δημιουργία των κλειδιών υπογραφής της ΜΧ εκτελείται από εξουσιοδοτημένο προσωπικό σε φυσικά ασφαλές περιβάλλον σύμφωνα με τις πρακτικές της ΑΧ. Η δημιουργία των κλειδιών υπογραφής της ΜΧ πραγματοποιείται μέσα σε ασφαλή κρυπτογραφικές συσκευές, οι οποίες πληρούν τις προϋποθέσεις που ορίζονται στην §5.1 της ΠΠ/ΔΠΠ της ΑΧ. Τα ζεύγη κλειδιών δημιουργούνται χρησιμοποιώντας ασφαλείς αλγόριθμους και παραμέτρους, σύμφωνα με τις συστάσεις του ETSI TS 319 312. Οι δραστηριότητες που εκτελούνται σε κάθε δημιουργία κλειδιού καταγράφονται, χρονολογούνται και υπογράφονται από όλα τα εμπλεκόμενα άτομα. Αυτά τα αρχεία διατηρούνται για σκοπούς επιθεώρησης και παρακολούθησης για χρονικό διάστημα που κρίνεται κατάλληλο από την ΑΠΕΔ.

5.2.2 Προστασία Ιδιωτικού Κλειδιού ΜΧ

Η ΑΠΕΔ λαμβάνει απαραίτητα μέτρα ώστε να βεβαιωθεί ότι τα ιδιωτικά κλειδιά της ΜΧ παραμένουν εμπιστευτικά και διατηρούν την ακεραιότητά τους. Τα ιδιωτικά κλειδιά της ΜΧ αποθηκεύονται σε μια ασφαλή Μονάδα Ασφάλειας Υλικού (HSM) για την εκτέλεση λειτουργιών υπογραφής κλειδιών, η οποία πληροί τις προϋποθέσεις που ορίζονται στην §5.1 της ΠΠ/ΔΠΠ της ΑΧ. Υπάρχουν ειδικοί έλεγχοι για να διασφαλιστεί ότι το υλικό δεν έχει αλλοιωθεί και λειτουργεί σωστά. Τα ιδιωτικά κλειδιά της ΜΧ δεν μπορούν να εξαχθούν σε οποιαδήποτε μορφή και δεν είναι προσβάσιμα εκτός Μονάδας Ασφαλείας Υλικού.
Η ΑΠΕΔ δημιουργεί αντίγραφα ασφαλείας των ιδιωτικών κλειδιών της ΜΧ, για σκοπούς ανάκτησης ρουτίνας και αποκατάστασης καταστροφών. Τέτοια κλειδιά αποθηκεύονται σε κρυπτογραφημένη μορφή μέσα σε κρυπτογραφικές μονάδες υλικού, που διασφαλίζουν αντίστοιχο επίπεδο ασφαλείας με το αρχικό.
Οι κρυπτογραφικές μονάδες που χρησιμοποιούνται για την αποθήκευση ιδιωτικών κλειδιών πληρούν τις απαιτήσεις της παρούσας ΔΠΠ. Τα ιδιωτικά κλειδιά αντιγράφονται σε κρυπτογραφικές μονάδες εφεδρικού υλικού. Η επαναφορά των αντιγράφων ασφαλείας των κλειδιών της ΜΧ απαιτεί διπλό έλεγχο σε ένα φυσικά ασφαλές περιβάλλον.

5.2.3 Διανομή Δημοσίου Κλειδιού ΜΧ

Τα Δημόσια κλειδιά της ΜΧ της διατίθενται σε Εγκεκριμένο Πιστοποιητικό. Τα Πιστοποιητικά της ΜΧ της ΑΠΕΔ διατίθενται για ασφαλή μεταφόρτωση μέσω του Αποθηκευτικού χώρου της ΑΠΕΔ: https://pki.aped.gov.gr/repository. Είναι επίσης διαθέσιμα στον Κατάλογο Εμπιστοσύνης παρόχων υπηρεσιών εμπιστοσύνης (Trusted List of Certification Service Providers) της Ευρωπαϊκής Ένωσης μέσω της Εθνικής Εποπτικής Αρχής (Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων).

5.2.4 Επαναδημιουργία κλειδιού ΜΧ

Η περίοδος λειτουργίας για τα ζεύγη κλειδιών της ΜΧ μπορεί να οριστεί ρυθμίζοντας μια περίοδο χρήσης ιδιωτικού κλειδιού στο πιστοποιητικό δημόσιου κλειδιού της ΜΧ. Τα ΔΧ της ΑΠΕΔ υπογράφονται με πιστοποιητικά της ΜΧ της ΑΠΕΔ ισχύος πέντε (5) ετών. Τα πιστοποιητικά της ΜΧ της ΑΠΕΔ ισχύος πέντε (5) ετών χρησιμοποιούνται μόνο για την υπογραφή ΔΧ κατά τη διάρκεια περιόδου χρήσης ενός (1) έτους. Η διαδικασία επαναδημιουργίας της ΜΧ της ΑΠΕΔ εκτελείται μετά τη λήξη της περιόδου χρήσης (1 έτους) του πιστοποιητικού της ΜΧ. Τα δημόσια κλειδιά αρχειοθετούνται για περίοδο τουλάχιστον δέκα (10) ετών από την ημερομηνία λήξης του πιστοποιητικού.

5.2.5 Τέλος Κύκλου Ζωής Κλειδιού ΜΧ

Η ΑΧ της ΑΠΕΔ διασφαλίζει ότι τα ιδιωτικά κλειδιά υπογραφής της ΜΧ δεν χρησιμοποιούνται πέρα από το τέλος του κύκλου ζωής τους. Ειδικότερα, εφαρμόζονται λειτουργικές και τεχνικές διαδικασίες για να εξασφαλιστεί ότι ένα νέο κλειδί θα τεθεί σε εφαρμογή πριν λήξει η περίοδος χρήσης του κλειδιού της ΜΧ και ότι τα ιδιωτικά κλειδιά της ΜΧ ή οποιοδήποτε μέρος τους, συμπεριλαμβανομένων τυχόν αντιγράφων, καταστρέφονται κατά τρόπο ώστε να μην μπορεί να ανακτηθεί το ιδιωτικό κλειδί. Το σύστημα δημιουργίας ΔΧ θα απορρίπτει κάθε απόπειρα έκδοσης ενός ΔΧ, εάν έχει λήξει το ιδιωτικό κλειδί υπογραφής ή εάν έχει λήξει η περίοδος χρήσης του ιδιωτικού κλειδιού υπογραφής.

5.2.6 Διαχείριση Κύκλου Ζωής της Κρυπτογραφικής Μονάδας που χρησιμοποιείται για την υπογραφή χρονοσφραγίδων

Η ΑΠΕΔ εξασφαλίζει την ασφάλεια της Μονάδας Ασφάλειας Υλικού (HSM) καθ' όλη τη διάρκεια του κύκλου ζωής της. Η ΑΠΕΔ έχει διαδικασίες για να εξασφαλίσει ότι:

- Οι Μονάδες Ασφάλειας Υλικού δεν παραβιάζονται κατά την αποστολή ή την αποθήκευσή τους.

- Εκτελείται έλεγχος αποδοχής για να επαληθεύσει ότι το κρυπτογραφικό υλικό λειτουργεί σωστά.
- Η εγκατάσταση, ενεργοποίηση και αναπαραγωγή των κλειδιών υπογραφής της ΜΧ στις Μονάδες Ασφάλειας Υλικού γίνεται μόνο από προσωπικό με αξιόπιστους ρόλους, σε φυσικά ασφαλές περιβάλλον.
- Τα ιδιωτικά κλειδιά υπογραφής της ΜΧ που είναι αποθηκευμένα στο HSM διαγράφονται μετά την απόσυρση της συσκευής σύμφωνα με τις οδηγίες του κατασκευαστή.

5.3 Χρονοσφράγιση

5.3.1 Διακριτικό Χρονοσφραγίδας

Η ΑΠΕΔ έχει τεχνικές διαδικασίες για να διασφαλίσει ότι το ΔΧ εκδίδεται με ασφάλεια και συμπεριλαμβάνει τη σωστή ώρα. Κάθε ΔΧ περιλαμβάνει:

- αναπαράσταση του δεδομένου που φέρει τη χρονοσφραγίδα όπως παρασχέθηκε από τον αιτούντα
- έναν μοναδικό αύξοντα αριθμό που μπορεί να χρησιμοποιηθεί τόσο για την παραγγελία του ΔΧ όσο και για την αναγνώριση του συγκεκριμένου ΔΧ
- ένα μοναδικό αναγνωριστικό της πολιτικής όπως περιγράφεται στην ενότητα 2.2 του παρόντος εγγράφου
- μια ηλεκτρονική υπογραφή που παράγεται χρησιμοποιώντας ένα κλειδί που χρησιμοποιείται αποκλειστικά για Χρονοσφράγιση
- αναγνωριστικό για την ΑΧ και την ΜΧ
- τιμή ημερομηνίας και ώρας που μπορεί να ανιχνευθεί στην πραγματική τιμή χρόνου UTC
- αλγόριθμος υπογραφής που χρησιμοποιείται στο ΔΧ όπως ορίζεται στην ενότητα 5.1 του παρόντος.

Οι ΜΧ της ΑΠΕΔ διατηρούν αρχεία καταγραφής ελέγχου για όλες τις βαθμονομήσεις έναντι των αναφορών UTC.

5.3.2 Συγχρονισμός Ρολογιού με UTC

Η ΑΧ της ΑΠΕΔ εξασφαλίζει ότι η ώρα της συγχρονίζεται με το UTC εντός της δηλωμένης ακρίβειας με πολλαπλές ανεξάρτητες πηγές ώρας. Η ΑΧ της ΑΠΕΔ ενσωματώνει το χρόνο στο ΔΧ με την ακρίβεια που περιγράφεται στην ενότητα 4.1 του παρόντος εγγράφου. Τα αρχεία ελέγχου και βαθμονόμησης του συγχρονισμού τηρούνται από την ΑΠΕΔ. Η ΑΧ της ΑΠΕΔ διασφαλίζει ότι εάν ο χρόνος που θα υποδεικνύεται σε ένα ΔΧ μετακινείται εκτός του συγχρονισμού με το UTC, αυτό θα ανιχνευθεί. Εάν το ρολόι της ΜΧ παρασυρθεί εκτός της δηλωμένης ακρίβειας και ο επαναβαθμονόμος αποτύχει, η ΑΧ δεν θα εκδώσει χρονοσφραγίδες μέχρι να αποκατασταθεί ο σωστός χρόνος. Η ΑΠΕΔ εφαρμόζει ελέγχους ασφαλείας που εμποδίζουν τη μη εξουσιοδοτημένη λειτουργία, με σκοπό τη βαθμονόμηση της ώρας εκτός λειτουργίας.

5.3.3 Διαδικασία Χειρισμού Άλματος Δευτερολέπτου

Το άλμα δευτερολέπτου είναι μια προσαρμογή στο UTC παρακάμπτοντας ή προσθέτοντας ένα επιπλέον δευτερόλεπτο στο τελευταίο δευτερόλεπτο ενός μήνα UTC. Πρώτη προτίμηση δίνεται στο τέλος του Δεκεμβρίου και Ιουνίου και δεύτερη προτίμηση δίνεται στο τέλος του Μαρτίου και Σεπτεμβρίου. Η ΑΠΕΔ παρακολουθεί ότι ο συγχρονισμός διατηρείται όταν εμφανιστεί ένα άλμα δευτερολέπτου.

5.4 Διαχείριση και Λειτουργία Αρχής Χρονοσήμανσης

5.4.1 Διαχείριση Ασφάλειας

Η ΑΧ της ΑΠΕΔ διασφαλίζει ότι εφαρμόζονται διοικητικές και διαχειριστικές διαδικασίες που είναι επαρκείς και ανταποκρίνονται στις αναγνωρισμένες βέλτιστες πρακτικές. Η ΑΠΕΔ εκτελεί όλες τις λειτουργίες της ΑΧ χρησιμοποιώντας αξιόπιστα συστήματα.

5.4.2 Ασφάλεια Προσωπικού

Η ΑΠΕΔ διατηρεί τους κατάλληλους ελέγχους προσωπικού που πληρούν τις βέλτιστες πρακτικές ασφαλείας και απαιτήσεις των σχετικών προτύπων. Το προσωπικό διαθέτει τις κατάλληλες δεξιότητες και γνώσεις σχετικά με τη Χρονοσφράγιση, τις εγκεκριμένες υπογραφές και τις Υπηρεσίες Εμπιστοσύνης, καθώς και τις διαδικασίες ασφαλείας για το προσωπικό με αρμοδιότητες στον τομέα της ασφάλειας, την ασφάλεια των πληροφοριών και την αξιολόγηση των κινδύνων.
Σε ότι αφορά τα Έμπιστα Πρόσωπα ισχύουν τα αναφερόμενα στην ενότητα 5.2 της ΠΠ (Ενότητα Α του παρόντος εγγράφου) της ΑΠΕΔ.

5.4.3 Φυσική και Περιβαλλοντική Ασφάλεια

Η ΑΧ ΑΠΕΔ εφαρμόζει την Πολιτική Φυσικής Ασφάλειας της ΑΠΕΔ, όπως αυτή ορίζεται στην ενότητα 5.1 της ΠΠ (Ενότητα Α του παρόντος εγγράφου) της ΑΠΕΔ.

5.4.4 Επιχειρησιακή Διαχείριση

Η ΑΧ της ΑΠΕΔ ενεργεί σύμφωνα με τις διατάξεις της παραγράφου 9 του Κανονισμού Πιστοποίησης ΑΠΕΔ όπως ισχύει, καθώς και το ETSI EN 319 421 για τη διαχείριση περιστατικών.

5.4.5 Εγκατάσταση και συντήρηση αξιόπιστων συστημάτων

Η ΑΠΕΔ διασφαλίζει ότι τα συστήματα που διατηρούν λογισμικό της ΑΧ και αρχεία δεδομένων είναι αξιόπιστα συστήματα, ασφαλή από μη εξουσιοδοτημένη πρόσβαση και τροποποίηση.

5.4.6 Έκθεση σε κίνδυνο των Υπηρεσιών της ΑΧ

Σε περίπτωση έκθεσης σε κίνδυνο της λειτουργίας της ΜΧ (π.χ. μείζονος έκθεσης σε κίνδυνο του κλειδιού της ΜΧ), πιθανολογούμενης έκθεσης σε κίνδυνο ή απώλειας βαθμονόμησης, η ΜΧ δεν θα εκδίδει χρονοσφραγίδες μέχρις ότου ληφθούν μέτρα για την αποκατάστασή της. Σε περίπτωση πιθανολογούμενης έκθεσης σε κίνδυνο ή απώλειας βαθμονόμησης κατά την έκδοση χρονοσφραγίδων, η ΑΠΕΔ θα θέσει στη διάθεση όλων των Συνδρομητών και των Βασιζόμενων Μερών περιγραφή του συμβάντος. Σε περίπτωση μείζονος έκθεσης σε κίνδυνο της λειτουργίας της ΜΧ, η ΑΠΕΔ θα θέσει στη διάθεση όλων των Συνδρομητών και Βασιζόμενων Μερών πληροφορίες που μπορούν να χρησιμοποιηθούν για τον προσδιορισμό των χρονοσφραγίδων που ενδέχεται να επηρεάστηκαν, εκτός εάν αυτό παραβιάζει το απόρρητο των χρηστών της ΜΧ ή την ασφάλεια των υπηρεσιών της ΜΧ.

5.4.7 Διακοπή ΑΧ

Η λειτουργία της ΑΧ τερματίζεται με:

- απόφαση της αρχής που ασκεί την εποπτεία της παροχής της υπηρεσίας
- δικαστική απόφαση
- εκκαθάριση ή διακοπή των λειτουργιών της ΑΠΕΔ

Η ΑΠΕΔ διασφαλίζει ότι ελαχιστοποιούνται οι πιθανές διαταραχές στους Συνδρομητές και τα Βασιζόμενα Μέρη λόγω της διακοπής των υπηρεσιών της ΑΠΕΔ και, συγκεκριμένα, διασφαλίζει τη συνεχή διατήρηση των πληροφοριών που απαιτούνται για την επαλήθευση της ορθότητας των Υπηρεσιών Εμπιστοσύνης.
Στην περίπτωση που είναι απαραίτητη η διακοπή λειτουργίας της ΑΧ της ΑΠΕΔ, η ΑΠΕΔ θα καταβάλλει προσπάθειες ώστε να ειδοποιήσει τους Συνδρομητές και τα Βασιζόμενα Μέρη πριν από τη διακοπή λειτουργίας της ΑΧ. Η ΑΧ της ΑΠΕΔ ανακαλεί τα πιστοποιητικά των ΜΧ όταν τερματίζει τις υπηρεσίες της.

5.4.8 Συμμόρφωση με τη νομοθεσία

Η ΑΠΕΔ διασφαλίζει τη συμμόρφωση με τις νομικές απαιτήσεις προκειμένου να πληροί όλες τις εφαρμοστέες κανονιστικές απαιτήσεις όσον αφορά στην προστασία των αρχείων από απώλεια, καταστροφή και παραποίηση, καθώς και τις απαιτήσεις των εξής:

- του Κανονισμού (ΕΕ) αριθμ. 910/2014 (eIDAS) του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ,
- των κανονισμών της ΕΕ και νόμων περί προσωπικών δεδομένων,
- των σχετικών ευρωπαϊκών προτύπων:

- ETSI EN 319 401 Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) – Απαιτήσεις γενικής πολιτικής για παρόχους υπηρεσιών εμπιστοσύνης·
- ETSI EN 319 411-1 Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) – Απαιτήσεις πολιτικής και ασφάλειας για παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν πιστοποιητικά, Μέρος 1: Γενικές Απαιτήσεις·
- ETSI EN 319 411-2 Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) – Απαιτήσεις πολιτικής και ασφάλειας για παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν πιστοποιητικά, Μέρος 2: Απαιτήσεις πολιτικής για αρχές πιστοποίησης που εκδίδουν εγκεκριμένα πιστοποιητικά
- ETSI EN 319 421 Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) - Απαιτήσεις πολιτικής και ασφάλειας για παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν Χρονοσφραγίδες.
- ETSI EN 319 422 Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) – Πρωτόκολλο Χρονοσφραγίδας και Προφίλ Διακριτικών Χρονοσφραγίδας

Η ΑΠΕΔ, η οποία ενεργεί ως ΕΠΥΕ, αποδέχεται τον έλεγχο συμμόρφωσης για τις υπηρεσίες της ΑΧ για να διασφαλίσει ότι πληροί τις απαιτήσεις του eIDAS.

5.4.9 Καταγραφή πληροφοριών σχετικά με τη Λειτουργία των Υπηρεσιών Χρονοσφραγίδας

Η ΑΧ της ΑΠΕΔ διασφαλίζει ότι όλες οι σχετικές πληροφορίες σχετικά με τις λειτουργίες των Υπηρεσιών Χρονοσφραγίδας της ΑΠΕΔ καταγράφονται για καθορισμένο χρονικό διάστημα, ιδίως για την παροχή αποδεικτικών στοιχείων για σκοπούς δικαστικών διαδικασιών.
Η ΑΠΕΔ διατηρεί αρχείο για όλες τις πληροφορίες σχετικά με τη λειτουργία την ΑΧ της ΑΠΕΔ για περίοδο επτά (7) ετών. Η ΑΧ της ΑΠΕΔ τηρεί αρχεία για:

- το συγχρονισμό των ρολογιών που χρησιμοποιούνται στη χρονοσφράγιση
- την ανίχνευση απώλειας συγχρονισμού
- αιτήσεις χρονοσφραγίδων και χρονοσφραγίδες που έχουν δημιουργηθεί
- γεγονότα που σχετίζονται με τον κύκλο ζωής των κλειδιών ΜΧ (TSU) και των Πιστοποιητικών.

5.4.10 Οργανωτικά

Η ΑΧ της ΑΠΕΔ εξασφαλίζει ότι η επιχείρησή της είναι αξιόπιστη, όπως απαιτείται στο ETSI EN 319 421.
Τα έγγραφα πολιτικής και πρακτικής για την ΑΧ της ΑΠΕΔ είναι διαθέσιμα στο https://pki.aped.gov.gr/repository.

ΠΑΡΑΡΤΗΜΑ Α – Πηγές, Ακρωνύμια και Ορισμοί

Πηγές

Τα παρακάτω έγγραφα σχετίζονται με τον παρόντα Κανονισμό Πιστοποίησης της ΑΠΕΔ:

[1] Κανονισμός (ΕΕ) 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ

[2] ETSI EN 319 401 «Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) – Γενικές Απαιτήσεις Πολιτικής για παρόχους υπηρεσιών εμπιστοσύνης»

[3] ETSI EN 319 421: «Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) - Απαιτήσεις πολιτικής και ασφάλειας για τους παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν χρονοσφραγίδες»

[4] ETSI EN 319 422: «Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) –- Πρωτόκολλο Χρονοσφραγίδας και προφίλ token Χρονοσφραγίδας»

[5] IETF RFC 3161 (2001): «Internet X.509 Υποδομή δημόσιου κλειδιού: Πρωτόκολλο Χρονοσφραγίδας»

[6] ETSI EN 319 411-1: «Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) –- Απαιτήσεις πολιτικής και ασφάλειας για τους παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν πιστοποιητικά, – Μέρος 1: Γενικές Απαιτήσεις»

[7] ETSI EN 319 411-2: «Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) –- Απαιτήσεις πολιτικής και ασφάλειας για τους παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν πιστοποιητικά, – Μέρος 2: Απαιτήσεις πολιτικής για παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν εγκεκριμένα πιστοποιητικά»

Ορισμοί

Πίνακας 1: Πίνακας Ορισμών

Όρος	Ορισμός
eIDAS	Κανονισμός (ΕΕ) αριθμ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ.
OCSP (Online Certificate Status Protocol) /Πρωτόκολλο Δικτυακού Ελέγχου Κατάστασης Πιστοποιητικών	Το πρωτόκολλο που χρησιμοποιείται για την παροχή σε Βασιζόμενα Μέρη 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 SecurityInc., 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.
Αίτηση για πιστοποιητικό	Το αίτημα από τον Αιτούντα για Πιστοποιητικό προς μια ΑΠ για την έκδοση ενός Πιστοποιητικού.
Αιτών Πιστοποιητικό	Φυσικό πρόσωπο ή οργανισμός που ζητά την έκδοση πιστοποιητικού από μια ΑΠ.
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.
Αλυσίδα Πιστοποιητικού	Ο κατάλογος κατά σειρά κατάταξης των Πιστοποιητικών που περιλαμβάνει ένα Πιστοποιητικό Συνδρομητή, Πιστοποιητικά της ΑΠ και καταλήγει σε ένα Πιστοποιητικό Βάσης (Root).
ΑΠ βάσης	Η αρχή πιστοποίησης η οποία βρίσκεται στο υψηλότερο επίπεδο εντός του τομέα του ΠΥΕ και η οποία χρησιμοποιείται για να υπογράψει ιεραρχικά υφιστάμενες ΑΠ.
Αρχή Εγγραφής (ΑΕ)	Οντότητα 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 Πιστοποιητικών.
Αρχή Πιστοποίησης (ΑΠ)	Η οντότητα που έχει πιστοποιηθεί να εκδίδει, να χειρίζεται και να ανακαλεί Πιστοποιητικά.
Ασφαλής Κρυπτογραφική Μονάδα (ΑΚΜ –HSM)	Το χρησιμοποιούμενο από τους Παρόχους Υπηρεσιών Εμπιστοσύνης Αναγνωρισμένων Πιστοποιητικών, Προϊόν Ηλεκτρονικής Υπογραφής που προστατεύεται έναντι τροποποίησης και διασφαλίζει τεχνική και κρυπτογραφική ασφάλεια.
Βασιζόμενο Μέρος	Το φυσικό πρόσωπο ή φορέας που ενεργεί βασιζόμενος σε κάποιο πιστοποιητικά ή/και ηλεκτρονική υπογραφή.
Γενικοί Όροι και Προϋποθέσεις Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης	Δεσμευτικό έγγραφο που καθορίζει του όρους και τις προϋποθέσεις βάσει των οποίων ένα φυσικό ή νομικό πρόσωπο ενεργεί ως Συνδρομητής ή ως Βασιζόμενο Μέρος και η ΑΠΕΔ παρέχει τις αντίστοιχες Υπηρεσίες Εμπιστοσύνης.
Δήλωση Πρακτικής	Δήλωση των πρακτικών τις οποίες εφαρμόζει μια Αρχή Πιστοποίησης κατά την έκδοση, τη διαχείριση, την ανάκληση, την ανανέωση ή την επαναδημιουργία κλειδιών πιστοποιητικών.
Δημόσιο Κλειδί	Το κλειδί ενός ζεύγους κλειδιών που μπορεί να δημοσιοποιηθεί από τον κάτοχο του αντίστοιχου ιδιωτικού κλειδιού και το οποίο χρησιμοποιείται από Βασιζόμενο Μέρος για την επαλήθευση ενός εγκεκριμένου πιστοποιητικού που έχει δημιουργηθεί με το αντίστοιχο ιδιωτικό κλειδί του κατόχου και/ή για την κρυπτογράφηση μηνυμάτων ώστε να μπορούν να αποκρυπτογραφηθούν μόνο με το αντίστοιχο ιδιωτικό κλειδί του κατόχου.
Διαδικασία Παραγωγής Κλειδιών	Μια διαδικασία δια της οποίας παράγεται το ζεύγος κλειδιών μιας ΑΠ ή μιας ΑΕ, το ιδιωτικό κλειδί της μεταφέρεται σε μια κρυπτογραφική μονάδα, παράγεται εφεδρικό αντίγραφο του ιδιωτικού της κλειδιού και/ή πιστοποιείται το δημόσιο κλειδί της
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
Εγκεκριμένη Διάταξη Δημιουργίας Υπογραφής	Διάταξη που είναι υπεύθυνη για την έγκριση ψηφιακών υπογραφών με τη χρήση ειδικού υλικού και λογισμικού που διασφαλίζει ότι μόνο ο υπογράφων έχει τον έλεγχο του ιδιωτικού του κλειδιού. Οι εγκεκριμένες διατάξεις δημιουργίας ηλεκτρονικής υπογραφής ή σφραγίδας πληρούν τις απαιτήσεις του κανονισμού eIDAS, και συγκεκριμένα τους όρους του Παραρτήματος ΙΙ του Κανονισμού.
Εγκεκριμένη ηλεκτρονική υπογραφή	Πρόκειται για μια προηγμένη ηλεκτρονική υπογραφή που δημιουργείται από εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής και βασίζεται σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής.
Εγκεκριμένο Πιστοποιητικό	Το Εγκεκριμένο Πιστοποιητικό είναι ένα Πιστοποιητικό που εκδίδεται από μια ΑΠ η οποία έχει διαπιστευτεί και εποπτεύεται από αρχές που ορίζονται από κράτος μέλος της ΕΕ και πληροί τις απαιτήσεις του κανονισμού eIDAS.

Εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής	Πιστοποιητικό ηλεκτρονικής υπογραφής που εκδίδεται από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης και πληροί τις οριζόμενες απαιτήσεις στο Παράρτημα I του Κανονισμού eIDAS.
Εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης	Ο πάροχος υπηρεσιών εμπιστοσύνης ο οποίος παρέχει μία ή περισσότερες εγκεκριμένες υπηρεσίες εμπιστοσύνης και έχει αναγνωριστεί ως τέτοιος από τον Εποπτικό Φορέα.
Εκδότρια Αρχή Πιστοποίησης	Η Αρχή Πιστοποίησης που εκδίδει Πιστοποιητικά σε Συνδρομητές ακολουθώντας τουλάχιστον μία εκ των πολιτικών πιστοποιητικών της ΑΠΕΔ.
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 στα 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.
Έμπιστα Πρόσωπα	Οι υπάλληλοι που έχουν πρόσβαση ή ελέγχουν τις κρυπτογραφικές διαδικασίες.
Εμπιστευτικές/ Προσωπικές Πληροφορίες	Οι πληροφορίες που είναι απαραίτητο να παραμείνουν εμπιστευτικές και προσωπικές.
Εξ αποστάσεως ΕΔΔΥ	Εγκεκριμένη Διάταξη Δημιουργίας Υπογραφής Εξ αποστάσεως που πληροί τις απαιτήσεις του Παραρτήματος II του Κανονισμού eIDAS.
Ηλεκτρονική Εγγραφή ή Αίτηση	Η ηλεκτρονική διαδικασία που περιγράφεται στους Κανονισμούς Πιστοποίησης των ΥπΑΠ και που αφορά στα βήματα που πρέπει να προβεί ο Συνδρομητής προκειμένου να αποκτήσει εγκεκριμένο πιστοποιητικό.
Ηλεκτρονική σφραγίδα	Δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε ή συσχετίζονται λογικά με άλλα δεδομένα σε ηλεκτρονική μορφή, με σκοπό τη διασφάλιση της προέλευσης και της ακεραιότητάς τους.
Ηλεκτρονική υπογραφή	Δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε ή συσχετίζονται λογικά με άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμοποιούνται από τον υπογράφοντα για να υπογράφει.
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.
Ιδιωτικό Κλειδί	Το κλειδί ενός ζεύγους κλειδιών το οποίο διατηρείται κρυφό από τον κάτοχο του ζεύγους κλειδιών και το οποίο χρησιμοποιείται για την εισαγωγή εγκεκριμένης ηλεκτρονικής υπογραφής.
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).
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.
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.
Πάροχος Υπηρεσίας Εμπιστοσύνης	Οντότητα που παρέχει μία ή περισσότερες Υπηρεσίες Εμπιστοσύνης. Εγκεκριμένος Πάροχος Υπηρεσιών Εμπιστοσύνης κατ` εφαρμογή του θεσμικού πλαισίου διαπίστευσης της ΕΕΤΤ περιλαμβάνεται στον Κατάλογο Εμπιστοσύνης της ΕΕΤΤ

	(Κατάλογος εποπτευόμενων/ διαπιστευμένων Παροχών Υπηρεσιών Εμπιστοσύνης-TSL).
Πάροχος Υπηρεσιών Χρονοσήμανσης	Ο φορέας που εκδίδει Ηλεκτρονικές Χρονοσφραγίδες. Εγκεκριμένος Πάροχος Υπηρεσιών Χρονοσήμανσης κατ` εφαρμογή του θεσμικού πλαισίου διαπίστευσης της ΕΕΤΤ περιλαμβάνεται στον Κατάλογο Εμπιστοσύνης της ΕΕΤΤ (Κατάλογος Εμπιστοσύνης εποπτευόμενων/ διαπιστευμένων Παροχών Υπηρεσιών Εμπιστοσύνης - TSL).
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.
Πολιτική Πιστοποιητικού	Κατονομαζόμενο σύνολο κανόνων που υποδεικνύει την εφαρμοσιμότητα ενός πιστοποιητικού σε μια συγκεκριμένη κοινότητα και/ή κατηγορία εφαρμογής με κοινές απαιτήσεις για την ασφάλεια.
Πολιτική Πιστοποιητικού (ΠΠ)	Κατονομαζόμενο σύνολο κανόνων που υποδεικνύει την εφαρμοσιμότητα ενός πιστοποιητικού σε μια συγκεκριμένη κοινότητα και/ή κατηγορία εφαρμογής με κοινές απαιτήσεις για την ασφάλεια.
Προηγμένη Ηλεκτρονική Υπογραφή	Ηλεκτρονική υπογραφή που πληροί τους εξής όρους: • Συνδέεται μονοσήμαντα με τον υπογράφοντα • Είναι ικανή να καθορίσει ειδικά και αποκλειστικά την ταυτότητα του υπογράφοντα • Δημιουργείται με δεδομένα δημιουργίας ηλεκτρονικής υπογραφής τα οποία ο υπογράφων μπορεί, με υψηλό βαθμό εμπιστοσύνης, να χρησιμοποιεί υπό τον αποκλειστικό του έλεγχο και • Συνδέεται με τα δεδομένα που έχουν υπογραφεί σε σχέση με αυτήν κατά τρόπο ώστε να μπορεί να ανιχνευθεί οποιαδήποτε επακόλουθη τροποποίηση των εν λόγω δεδομένων.
Προϊόν Ηλεκτρονικής Υπογραφής	Υλικό ή λογισμικό ή συναφή συστατικά στοιχεία τους, που προορίζονται προς χρήση από τον πάροχο υπηρεσιών Εμπιστοσύνης 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.
Συνδρομητής (Τελικός Χρήστης)	Το πρόσωπο που αποτελεί το Υποκείμενο (Subject), στο όνομα του οποίου έχει εκδοθεί ένα Πιστοποιητικό. Ο Συνδρομητής (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.
Συντονισμένη παγκόσμια ώρα (UTC)	Χρονική κλίμακα βασισμένη στο δευτερόλεπτο όπως ορίζεται στη Σύσταση ITU-R TF.460-5.
Συντονισμένος Παγκόσμιος Χρόνος (Coordinated Universal Time -UTC)	Χρονική κλίμακα με βάση το δευτερόλεπτο όπως ορίζεται στη σύσταση ITU-R TF.460-5.
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.
Υπηρεσία Εμπιστοσύνης	Πρόκειται για την ηλεκτρονική υπηρεσία για τα ακόλουθα: i. τη δημιουργία, την εξακρίβωση και την επικύρωση ψηφιακών υπογραφών και σχετικών πιστοποιητικών ii. τη δημιουργία, την εξακρίβωση και την επικύρωση χρονοσφραγίδων και σχετικών πιστοποιητικών iii. τη συστημένη παράδοση και τα πιστοποιητικά που σχετίζονται με την υπηρεσία αυτή iv. τη δημιουργία, την εξακρίβωση και την επικύρωση πιστοποιητικών για επαλήθευση της ταυτότητας ιστότοπων v. τη διαφύλαξη ψηφιακών υπογραφών ή πιστοποιητικών που σχετίζονται με τις υπηρεσίες αυτές.
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.

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.
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.
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).

Ακρωνύμια

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 CommonCriteria).
	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)
ΑΠΕΔ		Αρχή Πιστοποίησης του Ελληνικού Δημοσίου
ΑΤΛΑ	LSVA	Αξιολόγηση Τρωτότητας της Λογικής Ασφάλειας (Logical Security Vulnerability Assessment)
ΑΥΠ	CSR	Αίτημα Υπογραφής Πιστοποιητικού (Certificate Signing Request)
ΑΧ	TSA	Αρχή Χρονοσφραγίδας (Time Stamping Authority)
ΔΠ	CPS	Δήλωση Πρακτικής (Certification Practice Statement)
ΔΧ		Διακριτικό Χρονοσφραγίδας
ΕΕΤΤ		Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
ΕΠΥΕ		Εγκεκριμένος Πάροχος Υπηρεσιών Εμπιστοσύνης
ΕΠΥΧ		Εγκεκριμένος Πάροχος Υπηρεσιών Χρονοσήμανσης
ΚΑΠ	CRL	Κατάλογος Ανακληθέντων Πιστοποιητικών (Certificate Revocation List)
ΚΜΥ		Κρυπτογραφική Μονάδα Υπογραφής
ΚΠ		Κανονισμός Πιστοποίησης
ΜΧ		Μονάδα Χρονοσήμανσης
ΠΑ	OID	Προσδιοριστής Αντικειμένου (Object Identifier)
ΠΑΠ	RCA	Πρωτεύουσα Αρχή Πιστοποίησης (Root Certification Authority)
ΠΔΠΧ		Πολιτική/Δήλωση Πρακτικής Χρονοσήμανσης
ΠΠ	CP	Πολιτική Πιστοποιητικού
ΠΥΧ		Πάροχος Υπηρεσιών Χρονοσφραγίδας
ΥΔΚ	PKI	Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure)
ΥπΑΠ		Υποκείμενη Αρχή Πιστοποίησης

Με την παρούσα καταργείται η υπό στοιχεία 243 ΕΞ 2022/5.1.2022 απόφαση του Υπουργού Επικρατείας «Κανονισμός Πιστοποίησης της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ)» (Β΄ 43).

Η ισχύς της παρούσας απόφασης αρχίζει από τη δημοσίευσή της στην Εφημερίδα της Κυβερνήσεως.

Η απόφαση αυτή να δημοσιευτεί στην Εφημερίδα της Κυβερνήσεως.