Πολιτική Πιστοποιητικού & Δήλωση Πρακτικών Πιστοποίησης για Εγκεκριμένα Πιστοποιητικά ηλεκτρονικών υπογραφών και ηλεκτρονικών σφραγίδων

Έκδοση 2.0

Ημερομηνία έναρξης ισχύος: 1.03.2021

ADACOM A.E.
Κρέοντος 25
Τ.Κ. 10442 Αθήνα
Ελλάδα
Αριθμός τηλεφώνου: +30 210 5193740
https://www.adacom.com

Πολιτική Πιστοποιητικού & Δήλωση Πρακτικών Πιστοποίησης της ADACOM για Εγκεκριμένα Πιστοποιητικά ηλεκτρονικών υπογραφών και ηλεκτρονικών σφραγίδων

© 2021 ADACOM SA. Με την επιφύλαξη παντός δικαιώματος.

Ανακοινώσεις περί εμπορικών σημάτων

ADACOM είναι το εμπορικό σήμα της ADACOM A.E. Άλλες επωνυμίες δύνανται να αποτελούν εμπορικά σήματα των αντίστοιχων κατόχων αυτών.

Χορηγείται άδεια για την αναπαραγωγή και διανομή του παρόντος εγγράφου διά μη αποκλειστικής βάσης και άνευ υποχρέωσης καταβολής δικαιωμάτων με την προϋπόθεση ότι: (i) η ανωτέρω ανακοίνωση περί πνευματικής ιδιοκτησίας και οι αρχικές παράγραφοι αναγράφονται ευκρινώς σε κάθε αντίγραφο και (ii) το παρόν έγγραφο αναπαράγεται με ακρίβεια στο σύνολό του και ολόκληρο, με την απόδοση του εγγράφου στην ADACOM A.E.

Τα αιτήματα για οποιαδήποτε άλλη άδεια αναπαραγωγής του παρόντος εγγράφου (καθώς και αιτήματα για χορήγηση αντιγράφων από την ADACOM A.E.) πρέπει να αποστέλλονται στην ADACOM A.E., Κρέοντος 25, T.K. 10442, Σεπόλια, Ελλάδα Υπόψη: Αρχή Διαχείρισης Πολιτικών. Τηλ.: +30 210 5193750, Φαξ: +30 210 5193555, Email: practices@adacom.com.

Ιστορικό εκδόσεων		
Ημερομηνία	Έκδοση	Μεταβολές
19.08.2020	1.0	Αρχικό έγγραφο
02.10.2020	1.1	Μικρές αλλαγές στις παρ. 1.3.2, 1.3.3, 5.8, 7.1.4.2, 7.1.4.3
17.02.2021	2.0	Αλλαγές στις παρ. 1, 2.2.1, 3.2.2, 3.2.3

Πίνακας περιεχομένων

1. ΕΙΣΑΓΩΓΗ....10
1.1 Επισκόπηση....10
1.2 Όνομα εγγράφου και Αναγνώριση....11
1.3 Συμμετέχοντες στην Υποδομή Δημόσιου Κλειδιού (ΥΔΚ)....12
1.3.1 Αρχές Πιστοποίησης....12
1.3.2 Αρχές Εγγραφής....13
1.3.3 Τοπικές Αρχές Εγγραφής....13
1.3.4 Συνδρομητές....14
1.3.5 Βασιζόμενα Μέρη....15
1.3.6 Άλλοι Συμμετέχοντες....15
1.4 Χρήση Πιστοποιητικού....15
1.4.1 Κατάλληλες Χρήσεις των Πιστοποιητικών....15
1.4.2 Απαγορευμένες χρήσεις πιστοποιητικών....16
1.5 Διαχείριση της Πολιτικής....16
1.5.1 Οργανισμός που διαχειρίζεται το έγγραφο....16
1.5.2 Υπεύθυνος επικοινωνίας....16
1.5.3 Πρόσωπο που προσδιορίζει την καταλληλότητα της ΠΠ ως προς την πολιτική16
1.5.4 Διαδικασία έγκρισης της ΠΠ/ΔΠΠ....16
1.6 Ορισμοί και Ακρωνύμια....17
2. ΔΗΜΟΣΙΕΥΣΗ ΚΑΙ ΥΠΟΧΡΕΣΩΣΕΙΣ ΤΟΥ ΧΩΡΟΥ ΑΠΟΘΗΚΕΥΣΗΣ....17
2.1 Χώροι Αποθήκευσης....17
2.2 Δημοσίευση πληροφοριών πιστοποιητικού....17
2.2.1 Πολιτικές δημοσίευσης και κοινοποίησης....18
2.2.2 Στοιχεία που δεν δημοσιεύονται στη Δήλωση Πρακτικών Πιστοποίησης..18
2.3 Χρόνος ή συχνότητα δημοσίευσης....18
2.4 Έλεγχοι πρόσβασης σε χώρους αποθήκευσης....18
3. ΤΑΥΤΟΤΗΤΑ ΚΑΙ ΕΠΑΛΗΘΕΥΣΗ ΤΗΣ ΤΑΥΤΟΤΗΤΑΣ....18
3.1 Ονοματοδοσία....18
3.1.1 Τύποι ονομάτων....18
3.1.2 Η ανάγκη κατανόησης των ονομάτων....19
3.1.3 Ανωνυμία ή ψευδωνυμία συνδρομητών....19
3.1.4 Κανόνες για την Ερμηνεία των Διαφόρων Τύπων Ονομάτων....19
3.1.5 Μοναδικότητα των Ονομάτων....19
3.1.6 Αναγνώριση, επαλήθευση ταυτότητας και ρόλος εμπορικών σημάτων....19
3.2 Αρχική επαλήθευση ταυτότητας....19
3.2.1 Μέθοδος απόδειξης της κατοχής ιδιωτικού κλειδιού....20
3.2.2 Επαλήθευση ταυτότητας οργανισμού (Νομικό Πρόσωπο)....20
3.2.3 Επαλήθευση ταυτότητας Φυσικού Προσώπου....21
3.2.4 Μη επαληθευμένες πληροφορίες συνδρομητή....22
3.2.5 Ταυτοποίηση εξουσιοδότησης....22
3.3 Ταυτοποίηση και επαλήθευση ταυτότητας για αιτήματα επαναδημιουργίας κλειδιών....22

3.3.1 Ταυτοποίηση και επαλήθευση ταυτότητας για τακτική επαναδημιουργία κλειδιών....22
3.3.2 Ταυτοποίηση και επαλήθευση ταυτότητας για επαναδημιουργία κλειδιών μετά από ανάκληση....22
3.4 Ταυτοποίηση και επαλήθευση ταυτότητας για αίτημα ανάκλησης....23
4. ΛΕΙΤΟΥΡΓΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΤΟΥ ΚΥΚΛΟΥ ΖΩΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ....23
4.1 Αίτηση για πιστοποιητικό....23
4.1.1 Ποιος μπορεί να υποβάλει αίτηση για πιστοποιητικό....23
4.1.2 Διαδικασία εγγραφής και υποχρεώσεις....23
4.2 Επεξεργασία αίτησης πιστοποιητικού....24
4.2.1 Εκτέλεση λειτουργιών ταυτοποίησης και επαλήθευση ταυτότητας....24
4.2.2 Έγκριση ή απόρριψη αιτήσεων για έκδοση πιστοποιητικού....24
4.2.3 Χρόνος επεξεργασίας των αιτήσεων για πιστοποιητικό....24
4.3 Έκδοση Πιστοποιητικού....25
4.3.1 Ενέργειες της ΑΠ κατά την έκδοση πιστοποιητικών....25
4.3.2 Ειδοποίηση του συνδρομητή από την ΑΠ για την έκδοση του πιστοποιητικού....25
4.3.3 Εγγραφή και έκδοση Εγκεκριμένου Πιστοποιητικού Ηλεκτρονικής Σφραγίδας που συμμορφώνεται με το πρότυπο ETSI TS 119 495 κατά PSD2....25
4.4 Αποδοχή πιστοποιητικού....25
4.4.1 Ενέργειες που αποτελούν αποδοχή πιστοποιητικού....25
4.4.2 Δημοσίευση του πιστοποιητικού από την ΑΠ....25
4.4.3 Κοινοποίηση έκδοσης πιστοποιητικού από την ΑΠ προς άλλες οντότητες 26
4.5 Χρήση ζεύγους κλειδιών και πιστοποιητικού....26
4.5.1 Χρήση ιδιωτικού κλειδιού συνδρομητή και πιστοποιητικού....26
4.5.2 Χρήση δημόσιου κλειδιού και πιστοποιητικών από βασιζόμενο μέρος....26
4.6 Ανανέωση πιστοποιητικού....27
4.7 Επαναδημιουργία κλειδιών πιστοποιητικού....27
4.7.1 Συνθήκες για την επαναδημιουργία κλειδιών πιστοποιητικού....27
4.7.2 Ποιοι μπορούν να αιτηθούν την πιστοποίηση νέου δημόσιου κλειδιού....27
4.7.3 Επεξεργασία αιτημάτων επαναδημιουργίας κλειδιών πιστοποιητικού....27
4.7.4 Κοινοποίηση έκδοσης νέου πιστοποιητικού στον συνδρομητή....27
4.7.5 Ενέργεια που συνιστά αποδοχή του Πιστοποιητικού με επαναδημιουργημένα κλειδιά....27
4.7.6 Δημοσίευση του πιστοποιητικού με επαναδημιουργημένα κλειδιά από την ΑΠ 28
4.7.7 Κοινοποίηση έκδοσης πιστοποιητικού από την ΑΠ προς άλλες οντότητες 28
4.8 Τροποποίηση πιστοποιητικού....28
4.8.1 Συνθήκες για την τροποποίηση πιστοποιητικού....28
4.8.2 Ποιος μπορεί να αιτηθεί τροποποίηση πιστοποιητικού....28
4.8.3 Επεξεργασία αιτημάτων τροποποίησης πιστοποιητικού....28
4.8.4 Κοινοποίηση έκδοσης νέου πιστοποιητικού στον συνδρομητή....28
4.8.5 Ενέργεια που συνιστά αποδοχή του τροποποιημένου πιστοποιητικού....28
4.8.6 Δημοσίευση του τροποποιημένου πιστοποιητικού από την ΑΠ....28
4.8.7 Κοινοποίηση έκδοσης πιστοποιητικού από την ΑΠ προς άλλες οντότητες 28

4.9 Αναστολή και ανάκληση πιστοποιητικού....29
4.9.1 Συνθήκες για ανάκληση πιστοποιητικού....29
4.9.2 Ποιοι μπορούν να αιτηθούν την ανάκληση πιστοποιητικού....30
4.9.3 Διαδικασία υποβολής αιτήματος ανάκλησης....30
4.9.4 Περίοδος χάριτος του αιτήματος ανάκλησης....31
4.9.5 Χρονικό διάστημα μέσα στο οποίο η ΑΠ θα πρέπει να επεξεργαστεί το αίτημα ανάκλησης....31
4.9.6 Απαιτήσεις ελέγχου κατάστασης ανακληθέντων πιστοποιητικών για βασιζόμενα μέρη....31
4.9.7 Συχνότητα έκδοσης ΚΑΠ....32
4.9.8 Μέγιστος χρόνος αναμονής για τους ΚΑΠ....32
4.9.9 Διαθεσιμότητα ανάκλησης/κατάστασης πιστοποιητικών σε απευθείας σύνδεση32
4.9.10 Απαιτήσεις ελέγχου κατάστασης ανακληθέντων πιστοποιητικών σε απευθείας σύνδεση....32
4.9.11 Άλλες διαθέσιμες μορφές αναγγελίας ανάκλησης....33
4.9.12 Ειδικές απαιτήσεις σχετικά με την έκθεση του κλειδιού σε κίνδυνο....33
4.9.13 Συνθήκες για αναστολή πιστοποιητικού....33
4.9.14 Ποιοι μπορούν να αιτηθούν την αναστολή πιστοποιητικού....33
4.9.15 Διαδικασία υποβολής αιτήματος αναστολής....33
4.9.16 Περιορισμός για την περίοδο αναστολής....33
4.10 Υπηρεσίες κατάστασης πιστοποιητικού....33
4.10.1 Λειτουργικά χαρακτηριστικά....33
4.10.2 Διαθεσιμότητα υπηρεσιών....33
4.10.3 Προαιρετικά χαρακτηριστικά....33
4.11 Τερματισμός συνδρομής....34
4.12 Παρακαταθήκη και ανάκτηση κλειδιού....34
4.12.1 Πολιτικές και πρακτικές για την παρακαταθήκη και την ανάκτηση κλειδιού 34
4.12.2 Πολιτικές και πρακτικές για την ενθυλάκωση και την ανάκτηση του κλειδιού της περιόδου λειτουργίας....34
5. ΜΕΤΡΑ ΕΛΕΓΧΟΥ ΤΩΝ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΤΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΤΗΣ ΛΕΙΤΟΥΡΓΙΑΣ....34
5.1 Φυσικοί έλεγχοι....34
5.1.1 Τοποθεσία και κατασκευή του χώρου....34
5.1.2 Φυσική πρόσβαση....34
5.1.3 Παροχή ηλεκτρικού ρεύματος και κλιματισμός....35
5.1.4 Έκθεση σε νερό....35
5.1.5 Πρόληψη και προστασία από πυρκαγιά....36
5.1.6 Αποθήκευση μέσων....36
5.1.7 Διάθεση αποβλήτων....36
5.1.8 Δημιουργία εφεδρικών αντιγράφων ασφαλείας εκτός του χώρου εγκατάστασης....36
5.2 Διαδικαστικοί έλεγχοι....36
5.2.1 Ρόλοι εμπιστοσύνης....36
5.2.2 Αριθμός προσώπων που απαιτούνται ανά τομέα εργασίας....37

5.2.3 Ταυτοποίηση και επαλήθευση της ταυτότητας για κάθε ρόλο.....37
5.2.4 Ρόλοι που απαιτούν διαχωρισμό καθηκόντων.....38
5.3 Έλεγχοι προσωπικού.....38
5.3.1 Απαιτήσεις σχετικά με τα προσόντα, την εμπειρία και την εξουσιοδότηση 38
5.3.2 Διαδικασίες ελέγχου ιστορικού.....39
5.3.3 Απαιτήσεις εκπαίδευσης.....39
5.3.4 Συχνότητα και απαιτήσεις επανεκπαίδευσης.....40
5.3.5 Συχνότητα και ακολουθία εναλλαγής θέσεων εργασίας.....40
5.3.6 Κυρώσεις για μη εξουσιοδοτημένες ενέργειες.....40
5.3.7 Απαιτήσεις ανεξάρτητου αναδόχου.....40
5.3.8 Έντυπα που διατίθενται στο προσωπικό.....40
5.4 Διαδικασίες καταγραφής ελέγχου.....41
5.4.1 Τύποι συμβάντων που καταγράφονται.....41
5.4.2 Συχνότητα επεξεργασίας των αρχείων καταγραφής.....42
5.4.3 Περίοδος διατήρησης αρχείου καταγραφής ελέγχων.....42
5.4.4 Προστασία του αρχείου καταγραφής ελέγχου.....42
5.4.5 Διαδικασίες εφεδρικών αντιγράφων των αρχείων καταγραφής ελέγχων....42
5.4.6 Σύστημα συλλογής αρχείων ελέγχου (Εσωτερικό - Εξωτερικό).....43
5.4.7 Κοινοποίηση στο υποκείμενο που προκάλεσε το συμβάν.....43
5.4.8 Αξιολογήσεις ευπάθειας.....43
5.5 Τήρηση αρχείων.....43
5.5.1 Είδη τηρούμενων αρχείων.....43
5.5.2 Περίοδος διατήρησης αρχείων.....43
5.5.3 Προστασία του Αρχείου.....43
5.5.4 Διαδικασίες εφεδρικών αντιγράφων του Αρχείου.....44
5.5.5 Απαιτήσεις για τη χρονοσήμανση των αρχείων.....44
5.5.6 Σύστημα συλλογής αρχείων (Εσωτερικό ή Εξωτερικό).....44
5.5.7 Διαδικασίες για την πρόσβαση και την επαλήθευση πληροφοριών αρχείου 44
5.6 Αντικατάσταση κλειδιών.....44
5.7 Έκθεση σε κίνδυνο και αποκατάσταση καταστροφής.....45
5.7.1 Διαδικασίες χειρισμού περιστατικών και έκθεσης σε κίνδυνο.....45
5.7.2 Φθορά υπολογιστικών πόρων, λογισμικού και/ή δεδομένων.....45
5.7.3 Διαδικασίες σχετικά με την έκθεση ιδιωτικού κλειδιού οντότητας σε κίνδυνο 45
5.7.4 Δυνατότητες επιχειρησιακής συνέχειας έπειτα από καταστροφή.....45
5.8 Διακοπή λειτουργίας ΑΠ ή ΑΕ.....46
6. ΤΕΧΝΙΚΟΙ ΕΛΕΓΧΟΙ ΑΣΦΑΛΕΙΑΣ.....48
6.1 Παραγωγή και εγκατάσταση ζεύγους κλειδιών.....48
6.1.1 Παραγωγή ζεύγους κλειδιών.....48
6.1.2 Παράδοση ιδιωτικού κλειδιού στον συνδρομητή.....48
6.1.3 Παράδοση δημόσιου κλειδιού στον εκδότη του πιστοποιητικού.....48
6.1.4 Παράδοση δημόσιου κλειδιού της ΑΠ σε βασιζόμενα μέρη.....49
6.1.5 Μέγεθος κλειδιού.....49
6.1.6 Δημιουργία παραμέτρων και έλεγχος ποιότητας δημόσιων κλειδιών.....49

6.1.7 Σκοποί χρήσης κλειδιών (σύμφωνα με το πεδίο χρήσης κλειδιών X.509 v3) 49
6.2 Προστασία ιδιωτικού κλειδιού και μηχανικοί έλεγχοι κρυπτογραφικής μονάδας 49
6.2.1 Πρότυπα και έλεγχοι για τις κρυπτογραφικές μονάδες.....50
6.2.2 Έλεγχος του ιδιωτικού κλειδιού από πολλαπλά πρόσωπα (m από n).....50
6.2.3 Παρακαταθήκη ιδιωτικού κλειδιού.....50
6.2.4 Δημιουργία αντίγραφου ασφαλείας ιδιωτικού κλειδιού.....50
6.2.5 Αρχειοθέτηση ιδιωτικών κλειδιών.....51
6.2.6 Μεταφορά ιδιωτικού κλειδιού προς/από την κρυπτογραφική μονάδα.....51
6.2.7 Αποθήκευση ιδιωτικού κλειδιού σε κρυπτογραφική μονάδα.....51
6.2.8 Μέθοδος ενεργοποίησης ιδιωτικού κλειδιού.....51
6.2.9 Μέθοδος απενεργοποίησης ιδιωτικού κλειδιού.....52
6.2.10 Μέθοδος καταστροφής ιδιωτικού κλειδιού.....52
6.2.11 Αξιολόγηση κρυπτογραφικής μονάδας.....53
6.3 Άλλα θέματα διαχείρισης του ζεύγους κλειδιών.....53
6.3.1 Αρχειοθέτηση δημόσιου κλειδιού.....53
6.3.2 Λειτουργικές περίοδοι πιστοποιητικών και περίοδος χρήσης ζεύγους κλειδιών.....53
6.4 Δεδομένα ενεργοποίησης.....54
6.4.1 Παραγωγή και εγκατάσταση δεδομένων ενεργοποίησης.....54
6.4.2 Προστασία δεδομένων ενεργοποίησης.....54
6.4.3 Άλλα θέματα για τα δεδομένα ενεργοποίησης.....54
6.5 Έλεγχοι ασφάλειας υπολογιστών.....55
6.5.1 Ειδικές τεχνικές απαιτήσεις για την ασφάλεια των υπολογιστών.....55
6.5.2 Αξιολόγηση ασφάλειας υπολογιστών.....56
6.6 Τεχνικοί έλεγχοι κατά τον κύκλο ζωής.....56
6.6.1 Έλεγχοι ανάπτυξης συστήματος.....56
6.6.2 Έλεγχοι διαχείρισης ασφάλειας.....56
6.6.3 Έλεγχοι ασφάλειας κατά τον κύκλο ζωής του πιστοποιητικού.....57
6.7 Έλεγχοι ασφάλειας δικτύου.....57
6.8 Χρονοσήμανση.....57
7. ΠΡΟΦΙΛ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ, ΚΑΠ ΚΑΙ OCSP.....57
7.1 Προφίλ Πιστοποιητικού.....57
7.1.1 Αριθμός Έκδοσης.....57
7.1.2 Επεκτάσεις Πιστοποιητικού.....58
7.1.3 Αναγνωριστικά Αντικειμένου Αλγορίθμου.....65
7.1.4 Τύποι Ονομάτων.....65
7.1.5 Περιορισμοί Ονομάτων.....68
7.1.6 Αναγνωριστικά Αντικειμένου Πολιτικής Πιστοποιητικού.....68
7.1.7 Χρήση Επέκτασης των Περιορισμών Πολιτικής.....68
7.1.1 Σύνταξη και σημασιολογία Προδιαγραφών Πολιτικής.....69
7.1.2 Επεξεργασία Σημασιολογίας για την Επέκταση των Κρίσιμων Πολιτικών Πιστοποιητικού.....69
7.2 Προφίλ ΚΑΠ (CRL).....69
7.2.1 Αριθμός Έκδοσης.....69

7.2.2 Επεκτάσεις ΚΑΠ και Καταχωρίσεων ΚΑΠ....69
7.3 Προφίλ OCSP....69
7.3.1 Αριθμός Έκδοσης....69
7.3.2 Επεκτάσεις OCSP....69
8. ΕΛΕΓΧΟΣ ΣΥΜΜΟΡΦΩΣΗΣ ΚΑΙ ΑΛΛΕΣ ΑΞΙΟΛΟΓΗΣΕΙΣ....70
8.1 Συχνότητα και συνθήκες αξιολόγησης....71
8.2 Ταυτότητα/τυπικά προσόντα του αξιολογητή....71
8.3 Σχέση του αξιολογητή με την υπό αξιολόγηση οντότητα....71
8.4 Θέματα που καλύπτει η αξιολόγηση....71
8.5 Ανάληψη ενεργειών λόγω ανεπαρκειών....71
8.6 Κοινοποιήσεις των αποτελεσμάτων....72
8.7 Εσωτερικοί Έλεγχοι....72
9. ΑΛΛΑ ΕΠΙΧΕΙΡΗΣΙΑΚΑ ΚΑΙ ΝΟΜΙΚΑ ΘΕΜΑΤΑ....73
9.1 Τέλη....73
9.1.1 Τέλη έκδοσης ή ανανέωσης πιστοποιητικού....73
9.1.2 Τέλη για την πρόσβαση σε πιστοποιητικό....73
9.1.3 Τέλη για την πρόσβαση σε πληροφορίες ανάκλησης ή κατάστασης....73
9.1.4 Τέλη για άλλες υπηρεσίες....73
9.1.5 Πολιτική επιστροφής χρημάτων....73
9.2 Οικονομική Ευθύνη....74
9.2.1 Ασφαλιστική κάλυψη....74
9.2.2 Άλλα περιουσιακά στοιχεία....74
9.2.3 Ασφαλιστική ή εγγυητική κάλυψη για τελικούς χρήστες (οντότητες)....74
9.3 Εμπιστευτικότητα επιχειρηματικών Πληροφοριών....74
9.3.1 Πεδίο εφαρμογής εμπιστευτικών πληροφοριών....74
9.3.2 Πληροφορίες που δεν εμπίπτουν στο πεδίο εφαρμογής των εμπιστευτικών πληροφοριών....74
9.3.3 Ευθύνη προστασίας εμπιστευτικών πληροφοριών....75
9.4 Απόρρητο προσωπικών στοιχείων....75
9.4.1 Σχέδιο απορρήτου....75
9.4.2 Πληροφορίες που αντιμετωπίζονται ως ιδιωτικές....75
9.4.3 Πληροφορίες που δεν θεωρούνται ιδιωτικές....75
9.4.4 Ευθύνη για την προστασία ιδιωτικών πληροφοριών....75
9.4.5 Ειδοποίηση και συγκατάθεση για χρήση ιδιωτικών πληροφοριών....75
9.4.6 Γνωστοποίηση πληροφοριών σύμφωνα με δικαστική ή διοικητική διαδικασία....75
9.4.7 Γνωστοποίηση κατόπιν αιτήματος κατόχου....76
9.4.8 Λοιπές συνθήκες γνωστοποίησης πληροφοριών....76
9.5 Δικαιώματα Πνευματικής Ιδιοκτησίας....76
9.5.1 Δικαιώματα ιδιοκτησίας επί των πιστοποιητικών και των πληροφοριών ανάκλησης....76
9.5.2 Δικαιώματα ιδιοκτησίας επί της ΠΠ/ΔΠΠ....76
9.5.3 Δικαιώματα ιδιοκτησίας επί των ονομάτων....76
9.5.4 Δικαιώματα ιδιοκτησίας επί των κλειδιών και του υλικού κλειδιών....76
9.5.5 Παραβίαση δικαιωμάτων Πνευματικής Ιδιοκτησίας....77
9.6 Δηλώσεις και Εγγυήσεις....77

9.6.1 Δηλώσεις και Εγγυήσεις της ΑΠ....77
9.6.2 Δηλώσεις και Εγγυήσεις της ΑΕ....78
9.6.3 Δηλώσεις και εγγυήσεις του Συνδρομητή....78
9.6.4 Δηλώσεις και εγγυήσεις βασιζόμενου μέρους....79
9.6.5 Δηλώσεις και εγγυήσεις άλλων συμμετεχόντων....79
9.7 Δηλώσεις αποποίησης ευθύνης εγγυήσεων....79
9.8 Περιορισμοί Ευθύνης....80
9.9 Αποζημιώσεις....80
9.9.1 Αποζημίωση από πλευράς συνδρομητών....80
9.9.2 Αποζημίωση από πλευράς βασιζόμενων μερών....80
9.10 Διάρκεια και λήξη ισχύος....81
9.10.1 Διάρκεια ισχύος....81
9.10.2 Λήξη ισχύος....81
9.10.3 Έναρξη ισχύος λήξης και μετενέργεια....81
9.11 Ατομικές ειδοποιήσεις και κοινοποιήσεις με συμμετέχοντες....81
9.12 Τροποποιήσεις....81
9.12.1 Διαδικασία τροποποίησης....81
9.12.2 Μηχανισμός και χρονική περίοδος ειδοποίησης....81
9.12.3 Συνθήκες υπό τις οποίες επιβάλλεται τροποποίηση του αναγνωριστικού αντικειμένου (OID)....82
9.13 Διατάξεις περί επίλυσης διαφορών....82
9.13.1 Διαφορές μεταξύ της ADACOM, των συνδεδεμένων εταιρειών και των πελατών82
9.13.2 Διαφορές με συνδρομητές ή βασιζόμενα μέρη....82
9.14 Εφαρμοστέο δίκαιο....83
9.15 Συμμόρφωση με την ισχύουσα νομοθεσία....83
9.16 Λοιπές διατάξεις....83
9.16.1 Σύνολο σύμβασης....83
9.16.2 Εκχώρηση....83
9.16.3 Διαχωρισμός Όρων....84
9.16.4 Εφαρμογή (αμοιβές δικηγόρων και παραίτηση από δικαιώματα)....84
9.16.5 Ανωτέρα βία....84
9.17 Άλλες διατάξεις....84
Παράρτημα Α. Πίνακας ακρωνυμίων και ορισμών....85
Πίνακας ακρωνυμίων....85
Ορισμοί....85

1. ΕΙΣΑΓΩΓΗ

Το παρόν έγγραφο αποτελεί την Πολιτική Πιστοποιητικού & Δήλωση Πρακτικών Πιστοποίησης της ADACOM (εφεξής «ΠΠ/ΔΠΠ») για Εγκεκριμένα Πιστοποιητικά. Δηλώνει τις πρακτικές που εφαρμόζει η ADACOM ως Πάροχος Υπηρεσιών Εμπιστοσύνης (εφεξής «ΠΥΕ») σχετικά με την παροχή υπηρεσιών πιστοποίησης για τα εγκεκριμένα πιστοποιητικά ηλεκτρονικών υπογραφών και τα εγκεκριμένα πιστοποιητικά ηλεκτρονικών σφραγίδων σύμφωνα, μεταξύ άλλων, με τα άρθρα 19, 24, 28, 38 και 45 του κανονισμού (ΕΕ) αριθ. 910/2014 [eIDAS].
Τα Εγκεκριμένα Πιστοποιητικά ηλεκτρονικών υπογραφών εκδίδονται είτε σε Τοπική Εγκεκριμένη Διάταξη Δημιουργίας Υπογραφής (ΕΔΔΥ) είτε σε εξ αποστάσεως ΕΔΔΥ. Τα Εγκεκριμένα Πιστοποιητικά ηλεκτρονικών σφραγίδων εκδίδονται είτε σε Τοπική ΕΔΔΥ είτε σε εξ αποστάσεως ΕΔΔΥ.

Η ADACOM παρέχει επίσης εγκεκριμένα πιστοποιητικά ηλεκτρονικών σφραγίδων, που συμμορφώνονται με τον eIDAS και το πρότυπο ETSI TS 119 495 ώστε να πληρούν τις προϋποθέσεις της Οδηγίας PSD2.

Το παρόν έγγραφο καθορίζει τις επιχειρηματικές, νομικές και τεχνικές απαιτήσεις για την έκκριση, έκδοση, διαχείριση, χρήση, ανάκληση και ανανέωση των Πιστοποιητικών καθώς και για την παροχή των σχετικών υπηρεσιών εμπιστοσύνης. Οι εν λόγω απαιτήσεις εφαρμόζονται σε όλες τις Αρχές Πιστοποίησης (ΑΠ), Αρχές Εγγραφής (ΑΕ), Συνδρομητές, Βασιζόμενα Μέρη και άλλες οντότητες της ΥΔΚ που αλληλεπιδρούν με την ΥΔΚ της ADACOM.

Συγκεκριμένα περιγράφει τις πρακτικές που η ADACOM εφαρμόζει για τα ακόλουθα:

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

Η παρούσα ΠΠ/ΔΠΠ συμμορφώνεται με το RFC 3647 του Internet Engineering Task Force (IETF) όσον αφορά τη δομή της Πολιτικής Πιστοποιητικού και της Δήλωσης Πρακτικών Πιστοποίησης.

1.1 Επισκόπηση

Η παρούσα ΠΠ/ΔΠΠ περιγράφει τις πρακτικές και τις διαδικασίες που εφαρμόζονται για την εκπλήρωση όλων των απαιτήσεων που προσδιορίζονται από τον κανονισμό (ΕΕ) αριθ. 910/2014 σχετικά με την έκδοση, τη διατήρηση και τη διαχείριση του κύκλου ζωής των Εγκεκριμένων Πιστοποιητικών ηλεκτρονικών υπογραφών και των Εγκεκριμένων Πιστοποιητικών ηλεκτρονικών σφραγίδων.

Οι εν λόγω πρακτικές και διαδικασίες συμμορφώνονται με:

- τις πολιτικές του ETSI EN 319 411-2 :
  - QCP-n-qscd για τα Εγκεκριμένα Πιστοποιητικά ηλεκτρονικών υπογραφών και QCP-l / QCP-l-qscd για τα Εγκεκριμένα Πιστοποιητικά ηλεκτρονικών σφραγίδων
- τις πολιτικές του ETSI EN 319 411-1:
  - Κανονικοποιημένη πολιτική πιστοποιητικού (NCP)
  - Εκτεταμένη κανονικοποιημένη πολιτική πιστοποιητικού (NCP+)
- ETSI TS 119 495 για «PSD2» Πιστοποιητικά ηλεκτρονικών σφραγίδων.

Η ADACOM έχει δημιουργήσει μια ασφαλή εγκατάσταση η οποία στεγάζει, μεταξύ άλλων, συστήματα της ΑΠ, συμπεριλαμβανομένων των κρυπτογραφικών μονάδων που φυλάσσουν τα ιδιωτικά κλειδιά για την έκδοση των πιστοποιητικών. Η ADACOM ενεργεί ως ΑΠ και εκτελεί όλες τις υπηρεσίες του κύκλου ζωής των Πιστοποιητικών όσον αφορά την έκδοση, τη διαχείριση, την ανάκληση και την ανανέωση των Εγκεκριμένων Πιστοποιητικών.

Η παρούσα ΠΠ/ΔΠΠ εφαρμόζεται στις Εκδότριες ΑΠ της ADACOM οι οποίες εκδίδουν Εγκεκριμένα Πιστοποιητικά ηλεκτρονικών υπογραφών και ηλεκτρονικών σφραγίδων .

Οι ιδιωτικές ΑΠ και άλλες ιεραρχικές δομές τις οποίες διαχειρίζεται η ADACOM ή υπηρεσίες που παρέχονται από την ADACOM σε άλλους Οργανισμούς είναι επίσης εντός του πεδίου εφαρμογής της παρούσας ΠΠ/ΔΠΠ. Οι πρακτικές που σχετίζονται με υπηρεσίες που παρέχονται από άλλους Οργανισμούς είναι εκτός του πεδίου εφαρμογής της παρούσας ΠΠ/ΔΠΠ.

Η ADACOM δημοσιεύει την παρούσα ΠΠ/ΔΠΠ προκειμένου να συμμορφωθεί με συγκεκριμένες απαιτήσεις πολιτικής της ισχύουσας νομοθεσίας ή με άλλα πρότυπα και απαιτήσεις του κλάδου.

Η ΠΠ/ΔΠΠ αποτελεί μόνο ένα έγγραφο από το σύνολο εγγράφων που σχετίζονται με τις Υπηρεσίες Εμπιστοσύνης της ADACOM. Τα εν λόγω υπόλοιπα έγγραφα περιλαμβάνουν τα εξής:

- Βοηθητικά εμπιστευτικά έγγραφα για την ασφάλεια και επιχειρησιακά έγγραφα τα οποία συμπληρώνουν την ΠΠ/ΔΠΠ παρέχοντας πιο αναλυτικές απαιτήσεις, όπως τα εξής:
    - τον Οδηγό αναφοράς διαδικασίας παραγωγής κλειδιών, ο οποίος παρουσιάζει αναλυτικά τις λειτουργικές απαιτήσεις διαχείρισης των κλειδιών,
    - την Πολιτική φυσικής ασφάλειας της ADACOM η οποία ορίζει τις αρχές για την ασφάλεια που διέπουν την υποδομή της ADACOM,
    - την Πολιτική ασφάλειας πληροφοριακών συστημάτων της ADACOM η οποία δηλώνει τις απαιτήσεις όσον αφορά την υποδομή των Πληροφοριακών Συστημάτων για την ασφαλή λειτουργία και σύμφωνα με τις σχετικές νομοθετικές και συμβατικές απαιτήσεις,
    - την Πολιτική διαχείρισης κρυπτογραφικών κλειδιών της ADACOM, η οποία παρουσιάζει αναλυτικά τις λειτουργικές απαιτήσεις διαχείρισης κλειδιών,

(Αν και τα συγκεκριμένα έγγραφα δεν διατίθενται στο ευρύ κοινό, οι προδιαγραφές τους περιλαμβάνονται στην Έκθεση Αξιολόγησης Συμμόρφωσης της ADACOM και δύνανται να είναι διαθέσιμα βάσει ειδικής συμφωνίας.)

- τους Γενικούς Όρους και Προϋποθέσεις Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης της ADACOM. Οι συγκεκριμένοι Γενικοί Όροι και Προϋποθέσεις δεσμεύουν τους Πελάτες, τους Συνδρομητές και τα Βασιζόμενα Μέρη της ADACOM. Μεταξύ άλλων, οι Γενικοί Όροι και Προϋποθέσεις καλύπτουν ένα ευρύ φάσμα εμπορικών όρων ή ειδικών όρων που αφορούν τις Υπηρεσίες Εμπιστοσύνης της ADACOM.

Σε πολλές περιπτώσεις, η ΠΠ/ΔΠΠ αναφέρεται στα συγκεκριμένα βοηθητικά έγγραφα για συγκεκριμένες, αναλυτικές πρακτικές για την εφαρμογή των πολιτικών της ADACOM όπου η συμπερίληψη των λεπτομερειών στην ΠΠ/ΔΠΠ θα μπορούσε να διακυβεύσει την ασφάλεια της ΑΠ της ADACOM.

1.2 Όνομα εγγράφου και Αναγνώριση

Το συγκεκριμένο έγγραφο αποτελεί την Πολιτική Πιστοποιητικού & Δήλωση Πρακτικών Πιστοποίησης της ADACOM για τα εγκεκριμένα πιστοποιητικά. Η ADACOM έχει αποδώσει στην παρούσα ΠΠ/ΔΠΠ την ακόλουθη τιμή αναγνωριστικού αντικειμένου:

1.3.6.1.4.1.15976.1.1.0.x(version).y(sub-version)

1.3.6.1.4.1.15976	Αναγνωριστικό αντικειμένου (OID) της ADACOM, καταχωρισμένη στο IANA

1.3.6.1.4.1.15976.1	Πάροχος Υπηρεσιών Εμπιστοσύνης
1.3.6.1.4.1.15976.1.1	Πολιτικές Εγκεκριμένου Πιστοποιητικού
1.3.6.1.4.1.15976.1.1.0.x(version).y(sub-version)	Ισχύουσα έκδοση της παρούσας ΠΠ/ΔΠΠ
1.3.6.1.4.1.15976.1.1.1	Υπηρεσίες Εγκεκριμένων Ηλεκτρονικών Υπογραφών
1.3.6.1.4.1.15976.1.1.2	Υπηρεσίες Εγκεκριμένων Ηλεκτρονικών Σφραγίδων
1.3.6.1.4.1.15976.1.1.3	Υπηρεσίες Εγκεκριμένων Χρονοσφραγίδων

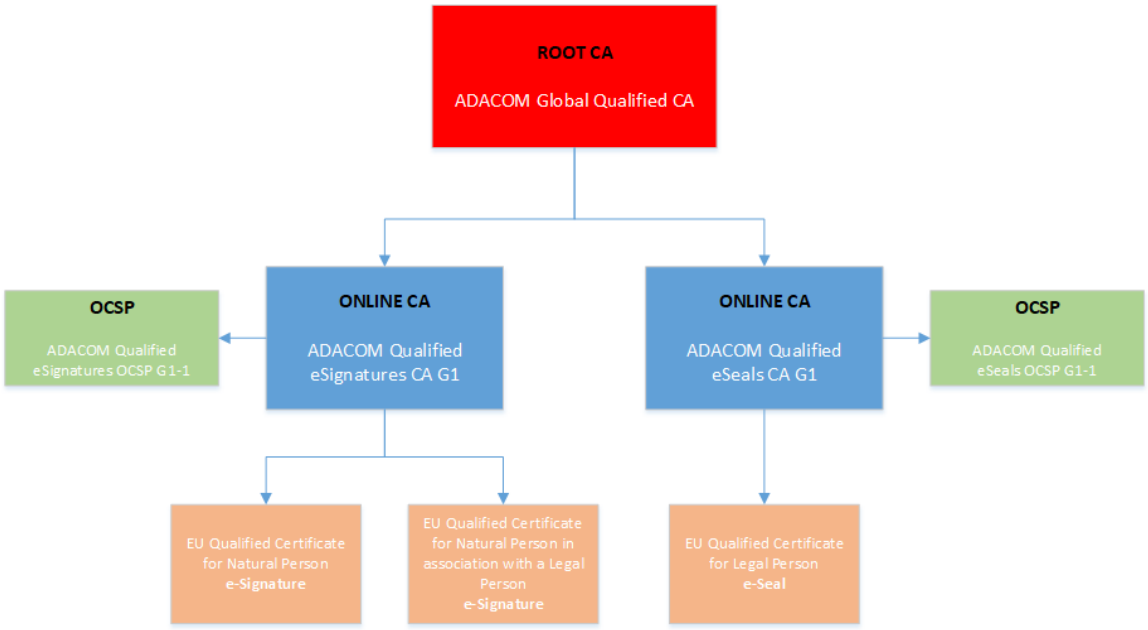
Η ισχύουσα ΠΠ/ΔΠΠ (αναγνωριστικό αντικειμένου) θα εισάγεται με αναφορά σε κάθε Πολιτική Πιστοποιητικού που διέπεται από την ΠΠ/ΔΠΠ της ADACOM.

1.3 Συμμετέχοντες στην Υποδομή Δημόσιου Κλειδιού (ΥΔΚ)

1.3.1 Αρχές Πιστοποίησης

Η αρχή την οποία εμπιστεύονται οι χρήστες των υπηρεσιών πιστοποίησης (δηλαδή οι συνδρομητές, καθώς και τα βασιζόμενα μέρη) για τη δημιουργία και τη έκδοση πιστοποιητικών ονομάζεται Αρχή Πιστοποίησης (ΑΠ).

Η ADACOM λειτουργεί βάσει της ακόλουθης ιεραρχικής δομής:



Η εν λόγω ιεραρχία ΑΠ αποτελείται από τις παρακάτω οντότητες:

ΑΠ Βάσης

A/A	Subject Distinguished Name	Certificate SHA-256 Fingerprint
1	**CN** = ADACOM Global Qualified CA **O** = ADACOM S.A. **2.5.4.97** = VATEL-099554476 **OU** = ADACOM Trust Services **C** = GR	28bdc4eb4587f24f53a9483ab0a62b8a62374673667bc1dd72aa0c5d5439eedf

Εκδότριες ΑΠ

A/A	Subject Distinguished Name	Certificate SHA-256 Fingerprint
1	**CN** = ADACOM Qualified eSignatures CA G1 **O** = ADACOM ADVANCED INTERNET APPLICATIONS S.A. **2.5.4.97** = VATEL-099554476 **OU** = ADACOM Qualified Trust Services **C** = GR	f4e9419e06f537b19e4 9b868edc9b3ac7f4ba1 296391f76108bcf41aa9 656288
2	**CN** = ADACOM Qualified eSeals CA G1 **O** = ADACOM ADVANCED INTERNET APPLICATIONS S.A. **2.5.4.97** = VATEL-099554476 **OU** = ADACOM Qualified Trust Services **C** = GR	6edabb764dadfb913bc 742ae7a335564b66fc6 a2aa6a950547260f566 3607628

1.3.2 Αρχές Εγγραφής

Η Αρχή Εγγραφής είναι μια οντότητα που διενεργεί την ταυτοποίηση και επαλήθευση της ταυτότητας των Συνδρομητών για την έκδοση Πιστοποιητικών, προβαίνει σε ή αποδέχεται αιτήσεις ανάκλησης πιστοποιητικών και εγκρίνει αιτήσεις για την επαναδημιουργία κλειδιών πιστοποιητικών για λογαριασμό της ΑΠ. Η ADACOM ενεργεί ως ΑΕ για τα Εγκεκριμένα Πιστοποιητικά που εκδίδει.

Η ADACOM δύναται να συνάψει συμβατική σχέση με ένα ή περισσότερα τρίτα μέρη προκειμένου να αναθέσει όλες τις αρμοδιότητες της Αρχής Εγγραφής (ΑΕ). Στην περίπτωση αυτή, το τρίτο μέρος αποτελεί μια Αρχή Εγγραφής της ADACOM και εκπληρώνει τις αρμοδιότητές της σύμφωνα με την παρούσα ΠΠ/ΔΠΠ, τα σχετικά Σχέδια Ταυτοποίησης και τους όρους της Σύμβασης ΑΕ που υπεγράφη μεταξύ της ΑΕ και της ADACOM.

Η ταυτοποίηση του τμήματος του τομέα της διεύθυνσης ηλεκτρονικού ταχυδρομείου δεν μπορεί να μεταβιβαστεί σε τρίτο μέρος και ταυτοποιείται μόνο από την ΑΕ της Εκδότριας ΑΠ.

Η ADACOM εκπαιδεύει το εξουσιοδοτημένο προσωπικό της ΑΕ όσον αφορά τη διαδικασία ταυτοποίησης και τις διαδικασίες ασφαλείας πριν από την έναρξη των σχετικών δραστηριοτήτων της ΑΕ και στη συνέχεια πραγματοποιεί επανεκπαίδευση ετησίως.

Η ADACOM διενεργεί ετησίως ελέγχους στις δραστηριότητες και διαδικασίες της ΑΕ προκειμένου να διασφαλίσει τη συμμόρφωση με την παρούσα ΠΠ/ΔΠΠ, τα Σχέδια Ταυτοποίησης και τη Σύμβαση ΑΕ.

1.3.3 Τοπικές Αρχές Εγγραφής

Η Τοπική Αρχή Εγγραφής είναι μια οντότητα που διενεργεί την ταυτοποίηση και την επαλήθευση της ταυτότητας των Συνδρομητών και των Υποκειμένων, καθώς και την αρχική εξέταση των σχετικών εγγράφων τους για την έκδοση, την επαναδημιουργία κλειδιών και την ανάκληση Πιστοποιητικών.

Η ADACOM δύναται να συνάψει συμβατική σχέση με ένα ή περισσότερα τρίτα μέρη προκειμένου να αναθέσει μέρος των αρμοδιοτήτων της Αρχής Εγγραφής, ειδικότερα όσον αφορά την ταυτοποίηση του Συνδρομητή. Στην περίπτωση αυτή, το τρίτο μέρος αποτελεί μια Τοπική Αρχή Εγγραφής (ΤΑΕ). Η ΤΑΕ εκπληρώνει τις αρμοδιότητές της σύμφωνα με την παρούσα ΠΠ/ΔΠΠ, τα σχετικά Σχέδια Ταυτοποίησης και τους όρους της Σύμβασης ΤΑΕ που υπεγράφη μεταξύ της ΤΑΕ και της ADACOM.

Η σχέση μεταξύ της ADACOM, ΤΑΕ και ΑΕ περιγράφεται στη σύμβαση της ΤΑΕ και περιλαμβάνει, μεταξύ άλλων, τα ακόλουθα:

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

Η Τοπική Αρχή Εγγραφής είναι υπεύθυνη για την παράδοση Εγκεκριμένης Διάταξης Δημιουργίας Υπογραφής (ΕΔΔΥ) ή τα διαπιστευτήρια αυθεντικοποίησης σε περίπτωση εξ αποστάσεως Εγκεκριμένων Πιστοποιητικών στον Συνδρομητή ή το Υποκείμενο.

Η Τοπική Αρχή Εγγραφής 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, την επαναδημιουργία κλειδιών ή την ανάκληση Πιστοποιητικών.

Η ADACOM εκπαιδεύει το εξουσιοδοτημένο προσωπικό της ΤΑΕ όσον αφορά τη διαδικασία ταυτοποίησης και τις διαδικασίες ασφαλείας πριν από την έναρξη των σχετικών δραστηριοτήτων της ΤΑΕ και στη συνέχεια πραγματοποιεί επανεκπαίδευση ετησίως.

Η ADACOM διενεργεί ετησίως ελέγχους στις δραστηριότητες και διαδικασίες της ΤΑΕ προκειμένου να διασφαλίσει τη συμμόρφωση με την παρούσα ΠΠ/ΔΠΠ, τα Σχέδια Ταυτοποίησης και τη Σύμβαση ΤΑΕ.

1.3.4 Συνδρομητές

Δύο διαφορετικοί όροι χρησιμοποιούνται στην παρούσα ΠΠ/ΔΠΠ για να γίνει διάκριση μεταξύ των δύο αυτών ρόλων: «Συνδρομητής» είναι η οντότητα που συνάπτει σύμβαση με την ADACOM για την έκδοση διαπιστευτηρίων και το «Υποκείμενο» είναι το άτομο με το οποίο συνδέεται το διαπιστευτήριο. Ο Συνδρομητής φέρει την τελική ευθύνη για τη χρήση του διαπιστευτηρίου αλλά το Υποκείμενο είναι το άτομο του οποίου η ταυτότητα επαληθεύεται όταν το διαπιστευτήριο προσκομίζεται.

Με τον όρο «Συνδρομητής» νοείται είτε ένα φυσικό πρόσωπο είτε ένα νομικό πρόσωπο στο οποίο η ADACOM παρέχει Υπηρεσίες Εμπιστοσύνης σύμφωνα με την παρούσα ΠΠ/ΔΠΠ.

Ο όρος «Υποκείμενο» νοείται:

- ένα φυσικό πρόσωπο,
- ένα φυσικό πρόσωπο που προσδιορίζεται σε σχέση με ένα νομικό πρόσωπο,
- ένα νομικό πρόσωπο.

Ο Συνδρομητής δύναται να είναι ή όχι το Υποκείμενο ενός πιστοποιητικού. Ο σύνδεσμος μεταξύ του συνδρομητή και του υποκειμένου είναι μία από τις ακόλουθες περιπτώσεις:

- Για την αίτηση πιστοποιητικού όσον αφορά φυσικό πρόσωπο, ο συνδρομητής είναι:
  1. το ίδιο το φυσικό πρόσωπο,
  2. ένα φυσικό πρόσωπο το οποίο έχει λάβει εντολή να εκπροσωπεί το υποκείμενο ή
  3. οποιαδήποτε οντότητα με την οποία συνδέεται το φυσικό πρόσωπο.
- Για την αίτηση πιστοποιητικού όσον αφορά το νομικό πρόσωπο, ο συνδρομητής είναι:

1. οποιαδήποτε οντότητα όπως προβλέπεται από οποιοδήποτε αρμόδιο νομικό σύστημα για την εκπροσώπηση του νομικού προσώπου ή
2. ένας νόμιμος εκπρόσωπος του νομικού προσώπου που εγγράφεται για τις θυγατρικές ή τις μονάδες ή τα τμήματά του.

1.3.5 Βασιζόμενα Μέρη

Ως Βασιζόμενο Μέρος νοείται ένα άτομο ή οντότητα που ενεργεί βάσει ενός πιστοποιητικού και/ή ψηφιακής υπογραφής που έχει εκδοθεί υπό την ΑΠ. Το Βασιζόμενο Μέρος δύναται να είναι ή όχι Συνδρομητής. Τα Βασιζόμενα Μέρη πρέπει να ελέγχουν τον κατάλληλο αποκριτή ΚΑΠ ή OCSP πριν βασιστούν σε πληροφορίες που περιλαμβάνονται σε ένα Πιστοποιητικό. Η τοποθεσία του σημείου διανομής ΚΑΠ περιγράφεται λεπτομερώς στο Πιστοποιητικό.

1.3.6 Άλλοι Συμμετέχοντες

Άλλοι συμμετέχοντες περιλαμβάνουν την Αρχή Διαχείρισης Πολιτικών της ADACOM (ΑΔΠ), η οποία είναι υπεύθυνη για τροποποιήσεις της παρούσας ΠΠ/ΔΠΠ.

Η ADACOM δύναται να χρησιμοποιήσει τρίτο πάροχο για την παροχή εξ αποστάσεως ΕΔΔΥ. Η εκ μέρους της ADACOM παροχή εξ αποστάσεως ΕΔΔΥ σε εγκατάσταση τρίτου κατασκευαστή, βάσει της παρούσας ΠΠ/ΔΠΠ, διασφαλίζεται από τους εξωτερικούς παρόχους που υποστηρίζουν τις δραστηριότητες της ADACOM, βάσει συμβατικής συμφωνίας με την ADACOM, που ενεργεί ως ΕΠΥΕ που έχει ελεγχθεί δεόντως βάσει του κανονισμού eIDAS και σε συμμόρφωση με τις απαιτήσεις του άρθρου 20 του κανονισμού (ΕΕ) 910/2014 (eIDAS).

1.4 Χρήση Πιστοποιητικού

1.4.1 Κατάλληλες Χρήσεις των Πιστοποιητικών

1.4.1.1 Πιστοποιητικά που εκδίδονται για ηλεκτρονική υπογραφή

Τα εγκεκριμένα πιστοποιητικά ηλεκτρονικών υπογραφών χρησιμοποιούνται συνήθως από φυσικά πρόσωπα για την υπογραφή εγγράφων, την κρυπτογράφηση του ηλεκτρονικού ταχυδρομείου και για σκοπούς επαλήθευσης ταυτότητας, υπό τον όρο ότι η χρήση δεν απαγορεύεται από το νόμο, από την παρούσα ΠΠ/ΔΠΠ και από τυχόν συμφωνίες με τους Συνδρομητές.

Τα πιστοποιητικά είναι συμμορφούμενα με τις πολιτικές πιστοποιητικού NCP, NCP+, QCP-n and QCP-n-qscd.
Τα πιστοποιητικά που εκδίδονται σύμφωνα με τις συγκεκριμένες απαιτήσεις αποσκοπούν στην υποστήριξη των εγκεκριμένων ηλεκτρονικών υπογραφών με τη χρήση της Εγκεκριμένης Διάταξης Δημιουργίας Υπογραφής (ΕΔΔΥ), όπως ορίζεται στο άρθρο 3 παράγραφος 12 του κανονισμού (ΕΕ) αριθ. 910/2014 [i.1].

1.4.1.2 Πιστοποιητικά που εκδίδονται για ηλεκτρονικές σφραγίδες

Τα εγκεκριμένα πιστοποιητικά ηλεκτρονικών σφραγίδων χρησιμοποιούνται συνήθως για να διασφαλιστεί η ακεραιότητα και η προέλευση των δεδομένων με τα οποία συνδέονται ή για άλλους σκοπούς, υπό τον όρο ότι η χρήση δεν απαγορεύεται από το νόμο, από την παρούσα ΠΠ/ΔΠΠ και από τυχόν συμφωνίες με τους Συνδρομητές.

Τα πιστοποιητικά είναι συμμορφούμενα με τις πολιτικές πιστοποιητικού NCP, NCP+, QCP-l και QCP-lqscd.
Τα πιστοποιητικά που εκδίδονται σύμφωνα με τις συγκεκριμένες απαιτήσεις αποσκοπούν στην υποστήριξη των εγκεκριμένων ηλεκτρονικών σφραγίδων με τη χρήση της Εγκεκριμένης Διάταξης

Δημιουργίας Υπογραφής (ΕΔΔΥ), όπως ορίζεται στο άρθρο 3 παράγραφος 27 του κανονισμού (ΕΕ) αριθ. 910/2014 [i.1] και των προηγμένων ηλεκτρονικών σφραγίδων χωρίς τη χρήση ΕΔΔΥ, όπως ορίζεται στο άρθρο 3 παράγραφος 26 του ίδιου Κανονισμού.

1.4.2 Απαγορευμένες χρήσεις πιστοποιητικών

Τα Πιστοποιητικά χρησιμοποιούνται μόνο στον βαθμό που η εφαρμογή τους είναι σύμφωνη με την ισχύουσα νομοθεσία και ειδικότερα μόνο στον βαθμό που επιτρέπεται από την εφαρμοστέα νομοθεσία περί εισαγωγών και εξαγωγών.

Τα Πιστοποιητικά της ΑΠ δεν μπορούν να χρησιμοποιηθούν για άλλες λειτουργίες πέραν των λειτουργιών της ΑΠ. Επιπλέον, τα Πιστοποιητικά του Συνδρομητή δεν πρέπει να χρησιμοποιούνται ως Πιστοποιητικά της ΑΠ. Απαγορεύεται η χρήση των πιστοποιητικών πέραν της υποστήριξης όσων ορίζονται στο κεφάλαιο 1.4.1 της παρούσας ΠΠ/ΔΠΠ.
Τα Βασιζόμενα Μέρη θα χρησιμοποιούν τα αναγνωριστικά αντικειμένου (OID) της Πολιτικής Πιστοποιητικού της ADACOM όπως καθορίζονται στο Πιστοποιητικό ώστε να αποδεχτούν ή να απορρίψουν κατάλληλα τη χρήση ενός Πιστοποιητικού.

1.5 Διαχείριση της Πολιτικής

1.5.1 Οργανισμός που διαχειρίζεται το έγγραφο

Η παρούσα ΠΠ/ΔΠΠ και τα σχετικά έγγραφα που αναφέρονται στην παρούσα τηρούνται από την Αρχή Διαχείρισης Πολιτικών της ADACOM, με την οποία μπορείτε να επικοινωνείτε στη διεύθυνση:
ADACOM A.E.
Κρέοντος 25
Τ.Κ. 10442, Αθήνα
Ελλάδα

1.5.2 Υπεύθυνος επικοινωνίας

Υπεύθυνος πολιτικής ΥΔΚ
Αρχή Διαχείρισης Πολιτικών της ADACOM
Υπόψη ADACOM A.E.
Κρέοντος 25
Τ.Κ. 10442, Αθήνα,
Ελλάδα
Αριθμός τηλεφώνου: +30 210 5193750
Φαξ: +30 210 5193555
practices@adacom.com

Για αιτήματα ανάκλησης πιστοποιητικών, επικοινωνήστε με την ADACOM αποστέλλοντας e-mail στο revoke@adacom.com.

1.5.3 Πρόσωπο που προσδιορίζει την καταλληλότητα της ΠΠ ως προς την πολιτική

Η Αρχή Διαχείρισης Πολιτικών (ΑΔΠ) της ADACOM προσδιορίζει την καταλληλότητα και την εφαρμοσιμότητα της παρούσας ΠΠ/ΔΠΠ βάσει των αποτελεσμάτων και προτάσεων των ελέγχων συμμόρφωσης.

1.5.4 Διαδικασία έγκρισης της ΠΠ/ΔΠΠ

Η έγκριση της παρούσας ΠΠ/ΔΠΠ και των επακόλουθων τροποποιήσεων πραγματοποιούνται από την ΑΔΠ της ADACOM. Οι τροποποιήσεις πραγματοποιούνται είτε σε μορφή εγγράφου που περιλαμβάνει την τροποποιημένη έκδοση της ΠΠ/ΔΠΠ είτε με σχετική ανακοίνωση επικαιροποίησης. Οι τροποποιημένες εκδόσεις ή οι ενημερώσεις δημοσιεύονται στον δικτυακό Χώρο Αποθήκευσης της ADACOM που βρίσκεται στη διεύθυνση https://pki.adacom.com/repository.

Οι νέες ενημερωμένες εκδόσεις υπερισχύουν έναντι οποιωνδήποτε καθορισμένων ή αντίθετων διατάξεων της αναφερόμενης έκδοσης της ΠΠ/ΔΠΠ. Η ΑΔΠ προσδιορίζει εάν οι αλλαγές στην ΠΠ/ΔΠΠ απαιτούν ή όχι αλλαγές στα αναγνωριστικά αντικειμένου των πολιτικών Πιστοποιητικού.

Ακόμα και αν δεν υφίσταται υποχρεωτικός λόγος τροποποίησης της ΠΠ/ΔΠΠ, η ΑΔΠ την αναθεωρεί τουλάχιστον ετησίως ως προσπάθεια βελτίωσής της.

1.6 Ορισμοί και Ακρωνύμια

Για τον πίνακα ακρωνυμίων και ορισμών, ανατρέξτε στο Παράρτημα Α.

2. ΔΗΜΟΣΙΕΥΣΗ ΚΑΙ ΥΠΟΧΡΕΣΩΣΕΙΣ ΤΟΥ ΧΩΡΟΥ ΑΠΟΘΗΚΕΥΣΗΣ

2.1 Χώροι Αποθήκευσης

Η ADACOM είναι υπεύθυνη για τη λειτουργία του χώρου αποθήκευσης όσον αφορά τις ΑΠ που διαχειρίζεται. Η ADACOM δημοσιεύει τα Πιστοποιητικά που έχουν εκδοθεί σε έναν χώρο αποθήκευσης (repository) σύμφωνα με την ενότητα 2.2.

Με την ανάκληση ενός Πιστοποιητικού Συνδρομητή, η ADACOM δημοσιεύει την ανακοίνωση της σχετικής ανάκλησης αυτής στον χώρο αποθήκευσης. Η ADACOM εκδίδει Καταλόγους Ανακληθέντων Πιστοποιητικών (ΚΑΠ) και παρέχει υπηρεσίες Πρωτοκόλλου Δικτυακού Ελέγχου κατάστασης Πιστοποιητικών (OCSP) σύμφωνα με τις διατάξεις της παρούσας ΠΠ/ΔΠΠ.

Η ADACOM 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 ADACOM, η ADACOM θα καταβάλλει 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 πιστοποιητικού

Η ADACOM διατηρεί έναν δικτυακά προσπελάσιμο αποθηκευτικό χώρο σε ένα δημόσιο δίκτυο επικοινωνίας δεδομένων (https://pki.adacom.com/repository) που επιτρέπει στα Βασιζόμενα Μέρη να υποβάλλουν διαδικτυακά ερωτήματα αναφορικά με την ανάκληση και άλλες πληροφορίες σχετικά με την κατάσταση του Πιστοποιητικού. Η ADACOM 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 ADACOM δημοσιεύει στον δημόσιο αποθηκευτικό χώρο πληροφοριών τουλάχιστον τις ακόλουθες πληροφορίες:

- Επισκόπηση της ιεραρχίας πιστοποίησης
- Δήλωση Πρακτικών Πιστοποίησης
- Αποτελέσματα ελέγχου
- Ασφαλιστήρια συμβόλαια
- Πολιτικές πιστοποίησης
- 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 Πολιτικές δημοσίευσης και κοινοποίησης

Η παρούσα ΠΠ/ΔΠΠ της ADACOM δημοσιεύεται στον δημόσιο χώρο αποθήκευσης πληροφοριών της ADACOM.
Η ΠΠ/ΔΠΠ της ADACOM μαζί με τις ημερομηνίες εκτέλεσης δημοσιεύεται τουλάχιστον 10 ημέρες πριν από την έναρξη ισχύος.

2.2.2 Στοιχεία που δεν δημοσιεύονται στη Δήλωση Πρακτικών Πιστοποίησης

Ανατρέξτε στην ενότητα 9.3.1 της παρούσας ΠΠ/ΔΠΠ.

2.3 Χρόνος ή συχνότητα δημοσίευσης

Πληροφορίες για την κατάσταση των πιστοποιητικών δημοσιεύονται σύμφωνα με τα οριζόμενα στην παρούσα ΠΠ/ΔΠΠ.
Ανατρέξτε στην ενότητα 2.2.1 της τρέχουσας ΠΠ/ΔΠΠ για ενημερώσεις της παρούσας ΠΠ/ΔΠΠ.
Οι Επικαιροποιήσεις των Γενικών Όρων και Προϋποθέσεων δημοσιεύονται όπως απαιτείται.
Τα Πιστοποιητικά δημοσιεύονται μόλις εκδοθούν.

2.4 Έλεγχοι πρόσβασης σε χώρους αποθήκευσης

Οι πληροφορίες που δημοσιεύονται στον χώρο αποθήκευσης του δικτυακού τόπου της ADACOM είναι δημοσίως προσβάσιμες μόνο για ανάγνωση, χωρίς περιορισμό. Η ADACOM απαιτεί από τους χρήστες την αποδοχή των Γενικών Όρων και Προϋποθέσεων ως προϋπόθεση για την πρόσβαση σε Πιστοποιητικά, πληροφορίες κατάστασης Πιστοποιητικών ή ΚΑΠ. Η ADACOM εφαρμόζει λογικά και φυσικά μέτρα ασφαλείας προκειμένου να αποτρέψει την προσθήκη, τη διαγραφή, ή την τροποποίηση των καταχωρήσεων στον χώρο αποθήκευσης από μη εξουσιοδοτημένα πρόσωπα, σύμφωνα με τις εφαρμοστέες πολιτικές ασφάλειας της ADACOM. Η ADACOM καθιστά τον χώρο αποθήκευσής της δημόσια διαθέσιμο αλλά μόνο για ανάγνωση και συγκεκριμένα στον ακόλουθο σύνδεσμο https://pki.adacom.com/repository.

3. ΤΑΥΤΟΤΗΤΑ ΚΑΙ ΕΠΑΛΗΘΕΥΣΗ ΤΗΣ ΤΑΥΤΟΤΗΤΑΣ

3.1 Ονοματοδοσία

Η ονοματοδοσία των πιστοποιητικών πραγματοποιείται όπως προβλέπεται στη Σύσταση ITU-T X.509 [6] ή στο RFC 5280 [7] 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 στον χώρο αποθήκευσης της ADACOM.

Τα Πιστοποιητικά της ΑΠ της ADACOM και του Συνδρομητή περιλαμβάνουν τα Διακριτικά Ονόματα X.501 στα πεδία Εκδότη και Υποκειμένου.

3.1.2 Η ανάγκη κατανόησης των ονομάτων

Τα Πιστοποιητικά του Συνδρομητή περιλαμβάνουν ονόματα με ευρέως κατανοητή σημασιολογία ώστε να επιτρέπουν τον προσδιορισμό της ταυτότητας του ατόμου ή του οργανισμού που αποτελεί το Υποκείμενο του Πιστοποιητικού.
Τα Πιστοποιητικά της ΑΠ της ADACOM 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 Κανόνες για την Ερμηνεία των Διαφόρων Τύπων Ονομάτων

Καμία διατύπωση.

3.1.5 Μοναδικότητα των Ονομάτων

Η ADACOM διασφαλίζει ότι τα Διακριτικά Ονόματα (ΔΟ) του Συνδρομητή είναι μοναδικά εντός του τομέα συγκεκριμένης ΑΠ μέσω αυτοματοποιημένων στοιχείων κατά τη διαδικασία εγγραφής του Συνδρομητή. 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. Για τις ηλεκτρονικές σφραγίδες διασφαλίζεται η τιμή χαρακτηριστικού γνωρίσματος του Αναγνωριστικού του Οργανισμού στο πεδίο Θέμα του πιστοποιητικού.

3.1.6 Αναγνώριση, επαλήθευση ταυτότητας και ρόλος εμπορικών σημάτων

Οι αιτούντες τη χορήγηση Πιστοποιητικού απαγορεύεται να χρησιμοποιούν στις Αιτήσεις τους για Πιστοποιητικό ονόματα τα οποία παραβιάζουν τα Δικαιώματα Πνευματικής Ιδιοκτησίας τρίτων. Η ADACOM, ωστόσο, δεν δύναται να επαληθεύσει εάν κάποιος Αιτών Πιστοποιητικό διαθέτει Δικαιώματα Πνευματικής Ιδιοκτησίας επί του ονόματος που αναγράφεται σε μία Αίτηση για Πιστοποιητικό, ούτε δύναται να λειτουργήσει ως διαιτητής ή διαμεσολαβητής ή με άλλον τρόπο να επιλύσει διαφορές που αφορούν την ιδιοκτησία οποιουδήποτε ονόματος τομέα, εμπορικής

επωνυμίας, εμπορικού σήματος ή σήματος παροχής υπηρεσιών. Η ADACOM έχει το δικαίωμα, χωρίς ευθύνη προς οποιονδήποτε Αιτούντα Πιστοποιητικό, να απορρίψει ή να αναστείλει μία Αίτηση για Πιστοποιητικό λόγω μίας τέτοιας διαφοράς.

3.2 Αρχική επαλήθευση ταυτότητας

Η ADACOM μπορεί να χρησιμοποιήσει τις ακόλουθες μεθόδους που περιγράφονται στην παρούσα ενότητα για να εξακριβώσει την ταυτότητα ενός Συνδρομητή. Η ADACOM μπορεί να αρνηθεί να εκδώσει πιστοποιητικό κατά τη διακριτική της ευχέρεια, εάν η εξακρίβωση της ταυτότητας δεν είναι επιτυχής.

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

3.2.1 Μέθοδος απόδειξης της κατοχής ιδιωτικού κλειδιού

Η διαδικασία δημιουργίας κλειδιού διασφαλίζεται από την παρούσα ΠΠ/ΔΠΠ σε συμμόρφωση με τα τεχνικά πρότυπα ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2.

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 ADACOM. Η συγκεκριμένη απαίτηση δεν ισχύει στην περίπτωση που δημιουργείται ένα ζεύγος κλειδιών από την ADACOM για λογαριασμό του Συνδρομητή, για παράδειγμα, στην περίπτωση που τα κλειδιά που έχουν εκ των προτέρων δημιουργηθεί τοποθετούνται σε ΕΔΔΥ.

Για Εγκεκριμένα Πιστοποιητικά που σχετίζονται με ιδιωτικά κλειδιά σε μια ΕΔΔΥ:

- Στην περίπτωση Τοπικής ΕΔΔΥ, τα ιδιωτικά κλειδιά δημιουργούνται και αποθηκεύονται στην Τοπική ΕΔΔΥ με την παρουσία του κατόχου του Πιστοποιητικού. Ο κάτοχος του Πιστοποιητικού είναι υπεύθυνος να διασφαλίζει την Τοπική ΕΔΔΥ με ένα προσωπικό αριθμό αναγνώρισης (PIN) απευθείας πάνω στην ΕΔΔΥ
- Στην περίπτωση Εξ αποστάσεως ΕΔΔΥ, τα ιδιωτικά κλειδιά δημιουργούνται και αποθηκεύονται υπό τον έλεγχο του κατόχου του Πιστοποιητικού πάνω σε ένα Hardware Security Module (HSM) που βρίσκεται στο κέντρο δεδομένων της ADACOM. Η πρόσβαση στα κλειδιά από τον κάτοχο του Πιστοποιητικού προστατεύεται χρησιμοποιώντας έλεγχο ταυτότητας πολλαπλών παραγόντων (multifactor authentication) που αποσκοπεί στο ίδιο επίπεδο διασφάλισης όπως αποκλειστικός έλεγχος που επιτυγχάνεται από την Τοπική ΕΔΔΥ.

3.2.2 Επαλήθευση ταυτότητας οργανισμού (Νομικό Πρόσωπο)

3.2.2.1 Επαλήθευση ταυτότητας Νομικού Προσώπου

Η ταυτότητα του νομικού προσώπου που είναι Συνδρομητής ενός Εγκεκριμένου Πιστοποιητικού επαληθεύεται από την ΑΕ/ΤΑΕ της ADACOM σύμφωνα με την υφιστάμενη νομοθεσία:

α) μέσω της φυσικής παρουσίας του νόμιμου εκπροσώπου του Συνδρομητή, ή

β) εξ αποστάσεως, μέσω Εγκεκριμένου Πιστοποιητικού για ηλεκτρονική υπογραφή ή ηλεκτρονική σφραγίδα, εφόσον αυτό έχει αρχικά εκδοθεί βάσει φυσικής ταυτοποίησης ή εξ αποστάσεως με τη χρήση μέσων ηλεκτρονικής ταυτοποίησης, ή

γ) μέσω εξ αποστάσεως ταυτοποίησης με χρήση τηλεδιάσκεψης,

Ο νόμιμος εκπρόσωπος παρέχει αποδεικτικό της ταυτότητάς του, επίσημα έγγραφα του νομικού προσώπου που αποδεικνύουν την εγγραφή του στο ΓΕΜΗ, καθώς και την εξουσία να εκπροσωπεί το νομικό πρόσωπο.

3.2.2.2 Επιπρόσθετη ταυτοποίηση σε περίπτωση Πιστοποιητικών PSD2

Σε περίπτωση Παρόχου Υπηρεσιών Πληρωμών (ΠΥΠ) που αιτείται Εγκεκριμένο Πιστοποιητικό Ηλεκτρονικής Σφραγίδας που συμμορφώνεται με το πρότυπο ETSI TS 119 495 ώστε να πληροί τις προϋποθέσεις της Οδηγίας PSD2, τα παρακάτω θα εφαρμόζονται:

Επιπρόσθετες πληροφορίες θα παρέχονται, συγκεκριμένα:

- ο αριθμός εξουσιοδότησης του ΠΥΠ που εκδίδεται από την Αρμόδια Εθνική Αρχή (ΑΕΑ) που εποπτεύει τις υπηρεσίες πληρωμών του ΠΥΠ, ή οποιοσδήποτε άλλος αριθμός καταχώρισης που αναγνωρίζεται από την ΑΕΑ
- ο ρόλος του ΠΥΠ (PSP_AS, PSP_PI, PSP_AI, PSP_IC) και
- το όνομα της ΑΕΑ, καθώς και το συντομογραφημένο μοναδικό αναγνωριστικό της ΑΕΑ.

Επιπρόσθετη ταυτοποίηση θα εκτελείται από την ADACOM, η οποία θα αποτελείται από:

- Επαλήθευση του αριθμού εξουσιοδότησης του ΠΥΠ ή οποιουδήποτε άλλου αριθμού καταχώρισης που παρέχεται σε σχέση με το μητρώο της ΑΕΑ/ ΕΑΤ
- Επαλήθευση του ρόλου του PSP (PSP_AS, PSP_PI, PSP_AI, PSP_IC) σε σχέση με το μητρώο ΑΕΑ/ ΕΑΤ.

3.2.3 Επαλήθευση ταυτότητας Φυσικού Προσώπου

3.2.3.1 Επαλήθευση ταυτότητας Φυσικού Προσώπου

Η ταυτότητα του φυσικού προσώπου που είναι ο Συνδρομητής ενός εγκεκριμένου πιστοποιητικού επαληθεύεται από την ΑΕ/ΤΑΕ της ADACOM σύμφωνα με την ισχύουσα νομοθεσία:

α) μέσω της φυσικής παρουσίας του Συνδρομητή, ή
β) εξ αποστάσεως, μέσω Εγκεκριμένου Πιστοποιητικού για ηλεκτρονική υπογραφή ή ηλεκτρονική σφραγίδα, εφόσον αυτό έχει αρχικά εκδοθεί βάσει φυσικής ταυτοποίησης ή εξ αποστάσεως με τη χρήση μέσων ηλεκτρονικής ταυτοποίησης, ή
γ) μέσω εξ αποστάσεως ταυτοποίησης με χρήση τηλεδιάσκεψης.

Ο Συνδρομητής παρέχει απόδειξη της ταυτότητάς του.

3.2.3.2 Επαλήθευση ταυτότητας Φυσικού Προσώπου που συνδέεται με Νομικό Πρόσωπο

Στην περίπτωση του φυσικού προσώπου που είναι το Υποκείμενο ενός εγκεκριμένου πιστοποιητικού το οποίο συνδέεται με ένα νομικό πρόσωπο που είναι Συνδρομητής, η ταυτότητα επαληθεύεται σύμφωνα με την ισχύουσα νομοθεσία:

α) μέσω της φυσικής παρουσίας του Υποκειμένου και του νόμιμου εκπροσώπου του Συνδρομητή, ή
β) εξ αποστάσεως, μέσω Εγκεκριμένου Πιστοποιητικού για ηλεκτρονική υπογραφή ή ηλεκτρονική σφραγίδα, εφόσον αυτό έχει αρχικά εκδοθεί βάσει φυσικής ταυτοποίησης ή εξ αποστάσεως με τη χρήση μέσων ηλεκτρονικής ταυτοποίησης, ή
γ) μέσω εξ αποστάσεως ταυτοποίησης με χρήση τηλεδιάσκεψης.

Ο Συνδρομητής και το Υποκείμενο παρέχουν απόδειξη της ταυτότητάς τους, τα επίσημα έγγραφα του νομικού προσώπου που αποδεικνύουν την εγγραφή του στο ΓΕΜΗ, καθώς και την σχέση του Υποκειμένου με το νομικό πρόσωπο.

Σε περίπτωση που το πρόσωπο που ζητεί το Πιστοποιητικό είναι εξουσιοδοτημένος υπάλληλος ΑΕ ή ΤΑΕ, η επαλήθευση της ταυτότητας αυτού του προσώπου δεν πρέπει να διεξάγεται από τον ίδιο αλλά από έναν άλλο υπάλληλο της ΑΕ/ΤΑΕ.

3.2.3.3 Επαλήθευση του Τομέα Ηλεκτρονικού Ταχυδρομείου

Η ADACOM επαληθεύει το δικαίωμα ενός Συνδρομητή να χρησιμοποιεί ή να ελέγχει μια διεύθυνση ηλεκτρονικού ταχυδρομείου που περιέχεται σε ένα Πιστοποιητικό που θα έχει το EKU "Secure Email" αποστέλλοντας ένα μήνυμα ηλεκτρονικού ταχυδρομείου έγκρισης στη διεύθυνση ηλεκτρονικού ταχυδρομείου που θα συμπεριληφθεί στο Πιστοποιητικό και αποστέλλοντας μια μοναδική τυχαία τιμή με SMS στον αριθμό κινητού τηλεφώνου που παρέχεται στο υπογεγραμμένο έντυπο αίτησης από τον Συνδρομητή.

3.2.4 Μη επαληθευμένες πληροφορίες συνδρομητή

Μη επαληθευμένες πληροφορίες συνδρομητή περιλαμβάνουν τα εξής:
- τα χαρακτηριστικά του πεδίου «Οργανωτικός Τομέας» (OU),
- οποιαδήποτε άλλη πληροφορία που ορίζεται ως μη επαληθεύσιμη στο Πιστοποιητικό.

3.2.5 Ταυτοποίηση εξουσιοδότησης

Όταν σε ένα πιστοποιητικό το όνομα ενός φυσικού προσώπου συσχετίζεται με το όνομα ενός νομικού προσώπου κατά τρόπο ώστε να υποδεικνύεται ότι το φυσικό πρόσωπο συνδέεται με ή είναι εξουσιοδοτημένο να ενεργεί εκ μέρους του νομικού προσώπου, η ΑΕ της ADACOM:
- επαληθεύει την ύπαρξη του φυσικού προσώπου χρησιμοποιώντας τουλάχιστον μια υπηρεσία απόδειξης ταυτότητας ή βάση δεδομένων τρίτου ή, εναλλακτικά, έγγραφα τεκμηρίωσης του οργανισμού που εκδίδονται ή κατατίθενται σε αρμόδια δημόσια υπηρεσία και τα οποία επιβεβαιώνουν την ύπαρξη του νομικού προσώπου και
- χρησιμοποιεί πληροφορίες που περιλαμβάνονται σε επαγγελματικά μητρώα ή βάσεις δεδομένων επιχειρηματικών πληροφοριών (κατάλογοι υπαλλήλων ή πελατών) μιας ΑΕ που εγκρίνει πιστοποιητικά στα δικά της συνδεδεμένα φυσικά πρόσωπα ή επιβεβαιώνει είτε τηλεφωνικά είτε με ταχυδρομείο ή με ανάλογη διαδικασία, προς το νομικό πρόσωπο, τη σχέση εργασίας με το νομικό πρόσωπο του φυσικού προσώπου που υποβάλει την αίτηση για χορήγηση Πιστοποιητικού και όταν είναι απαραίτητο, την εξουσιοδότησή του/της να ενεργεί για λογαριασμό του φυσικού προσώπου.

3.2.6 Κριτήρια διαλειτουργικότητας
- Καμία διατύπωση.

3.3 Ταυτοποίηση και επαλήθευση ταυτότητας για αιτήματα επαναδημιουργίας κλειδιών

Πριν από τη λήξη του υφιστάμενου Εγκεκριμένου Πιστοποιητικού , ο Συνδρομητής πρέπει να αποκτήσει ένα νέο πιστοποιητικό ώστε να εξασφαλίσει τη συνέχιση της χρήσης του Πιστοποιητικού. Η ADACOM γενικά, απαιτεί από τον Συνδρομητή να δημιουργήσει ένα νέο ζεύγος κλειδιών το οποίο θα αντικαθιστά το ζεύγος κλειδιών που λήγει (τεχνικά ορίζεται ως «επαναδημιουργία κλειδιών»).
Ανατρέξτε στις ενότητες 3.2.2 και 3.2.3 της παρούσας ΠΠ/ΔΠΠ.

Επιπλέον, όλα τα απαιτούμενα έγγραφα μπορούν να αποσταλούν ηλεκτρονικά και υπογεγραμμένα ψηφιακά από το υφιστάμενο Εγκεκριμένο Πιστοποιητικό Ηλεκτρονικών Υπογραφών

3.3.1 Ταυτοποίηση και επαλήθευση ταυτότητας για τακτική επαναδημιουργία κλειδιών

Δεν εφαρμόζεται

3.3.2 Ταυτοποίηση και επαλήθευση ταυτότητας για επαναδημιουργία κλειδιών μετά από ανάκληση

Ανατρέξτε στις ενότητες 3.2.2 και 3.2.3 της παρούσας ΠΠ/ΔΠΠ.

3.4 Ταυτοποίηση και επαλήθευση ταυτότητας για αίτημα ανάκλησης

Η Αρχή Εγγραφής επαληθεύει όλα τα αιτήματα για ανάκληση.
Πριν από την ανάκληση ενός Πιστοποιητικού, η ADACOM επαληθεύει ότι η ανάκληση έχει ζητηθεί από τον Συνδρομητή του Πιστοποιητικού ή την οντότητα που ενέκρινε την Αίτηση για Πιστοποιητικό.

Οι αποδεκτές διαδικασίες για την επαλήθευση ταυτότητας των αιτημάτων ανάκλησης ενός Συνδρομητή περιλαμβάνουν μία ή περισσότερες από τις ακόλουθες διαδικασίες:

- απαίτηση από τον Συνδρομητή να υποβάλει τη Συνθηματική Φράση και αυτόματη ανάκληση του Πιστοποιητικού εφόσον η φράση αυτή συμφωνεί με τη Συνθηματική Φράση που υπάρχει στο αρχείο·
- λήψη μηνύματος που προέρχεται από τον Συνδρομητή με το οποίο ζητά ανάκληση και το οποίο περιλαμβάνει εγκεκριμένη ηλεκτρονική υπογραφή επαληθεύσιμη με αναφορά στο Πιστοποιητικό που πρόκειται να ανακληθεί·
- επικοινωνία με τον Συνδρομητή η οποία παρέχει εύλογες διαβεβαιώσεις ότι το φυσικό ή νομικό πρόσωπο που ζητά την ανάκληση είναι πράγματι ο Συνδρομητής ή διαθέτει τη δέουσα σχετική εξουσιοδότηση. Ανάλογα με τις περιστάσεις, η επικοινωνία αυτή μπορεί να περιλαμβάνει μία ή περισσότερες από τις ακόλουθες μορφές: τηλεφωνική κλήση, τηλεομοιοτυπία, ηλεκτρονικό ταχυδρομείο, ταχυδρομική αλληλογραφία ή υπηρεσία ταχυμεταφοράς.

Οι Διαχειριστές της ADACOM δικαιούνται να ζητήσουν την ανάκληση των Πιστοποιητικών. Η ADACOM επαληθεύει την ταυτότητα των Διαχειριστών μέσω του ελέγχου πρόσβασης χρησιμοποιώντας το SSL και την επαλήθευση ταυτότητας του χρήστη (client) προτού επιτρέψει την ανάκληση από τους Διαχειριστές.

4. ΛΕΙΤΟΥΡΓΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΤΟΥ ΚΥΚΛΟΥ ΖΩΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

4.1 Αίτηση για πιστοποιητικό

4.1.1 Ποιος μπορεί να υποβάλει αίτηση για πιστοποιητικό

Αίτηση για Εγκεκριμένο Πιστοποιητικό δύναται να υποβάλλει το φυσικό ή νομικό πρόσωπο, το οποίο είναι ο Συνδρομητής του Πιστοποιητικού, με την προϋπόθεση ότι είναι επιλέξιμος από νομικής άποψης. Ο αιτών είναι υπεύθυνος για τυχόν δεδομένα που ο ίδιος ή οποιοδήποτε εξουσιοδοτημένο πρόσωπο από τον αιτούντα παρέχει στην ADACOM.

4.1.2 Διαδικασία εγγραφής και υποχρεώσεις

Όλοι οι Συνδρομητές του Πιστοποιητικού εκφράζουν τη συγκατάθεσή τους στους Γενικούς Όρους και Προϋποθέσεις οι οποίοι περιλαμβάνουν τις δηλώσεις και τις εγγυήσεις που περιγράφονται στην ενότητα 9.6.3 και υποβάλλονται σε διαδικασία εγγραφής η οποία συνίσταται στα εξής:

- στην αποδοχή των Όρων και των Προϋποθέσεων που αφορούν τη χρήση του πιστοποιητικού,
- στη συμπλήρωση και την υπογραφή της Αίτησης για Πιστοποιητικό και του εντύπου Συμφωνητικού με την παροχή αληθών και ακριβών στοιχείων σύμφωνα με τις απαιτήσεις της παρούσας πολιτικής,
- στην παροχή των σχετικών εγγράφων ταυτοποίησης,
- στην παραγωγή ή τη μέριμνα για δημιουργία ενός ζεύγους κλειδιών,
- στη λήψη του πιστοποιητικού τους είτε απευθείας είτε μέσω της ΑΕ,
- στην επίδειξη της κατοχής και/ή του αποκλειστικού ελέγχου του ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί που απέστειλε,
- Στην πληρωμή τυχόν τελών εάν απαιτείται.

4.2 Επεξεργασία αίτησης πιστοποιητικού

4.2.1 Εκτέλεση λειτουργιών ταυτοποίησης και επαλήθευση ταυτότητας

Η ADACOM διενεργεί την ταυτοποίηση και την επαλήθευση της ταυτότητας όλων των απαιτούμενων στοιχείων του Συνδρομητή είτε α) είτε μέσω φυσικής παρουσίας, είτε β) εξ αποστάσεως μέσω Εγκεκριμένου Πιστοποιητικού, είτε γ) χρησιμοποιώντας μέθοδο ισοδύναμη με τη φυσική παρουσία σύμφωνα με την ενότητα 3.2.
Εάν η ΤΑΕ / ΑΕ συμμετέχει στην ταυτοποίηση, η ΤΑΕ / ΑΕ πρέπει να δημιουργήσει και να τηρεί αρχεία επαρκή για να αποδείξει ότι έχει εκτελέσει τα απαιτούμενα βήματα ταυτοποίησης και να κοινοποιήσει την ολοκλήρωση αυτής στην ADACOM. Μετά την ολοκλήρωση της ταυτοποίησης, η ADACOM αξιολογεί τις πληροφορίες και αποφασίζει εάν θα εκδώσει ή όχι το Πιστοποιητικό. Στο πλαίσιο αυτής της αξιολόγησης, η ΑΕ της ADACOM μπορεί να ελέγξει το Πιστοποιητικό έναντι μίας εσωτερικής βάσης δεδομένων για πιστοποιητικά που έχουν ήδη ανακληθεί και αιτήσεις που έχουν απορριφθεί, ώστε να εντοπιστούν ύποπτα αιτήματα.

4.2.2 Έγκριση ή απόρριψη αιτήσεων για έκδοση πιστοποιητικού

Η ADACOM εγκρίνει την αίτηση για πιστοποιητικό εφόσον πληρούνται τα ακόλουθα κριτήρια:

- η επιτυχής ταυτοποίηση και επαλήθευση της ταυτότητας όλων των απαιτούμενων στοιχείων του Συνδρομητή σύμφωνα με την ενότητα 3.2,
- ότι έχει ληφθεί η πληρωμή.

Η ADACOM απορρίπτει μια αίτηση για πιστοποιητικό εάν:

- η ταυτοποίηση και η επαλήθευση της ταυτότητας όλων των απαιτούμενων στοιχείων του Συνδρομητή σύμφωνα με την ενότητα 3.2 δεν μπορεί να ολοκληρωθεί ή
- ο Συνδρομητής αδυνατεί να υποβάλλει τη σχετική τεκμηρίωση που του ζητείται ή
- ο Συνδρομητής αδυνατεί να ανταποκριθεί στις ειδοποιήσεις εντός του καθορισμένου χρόνου ή
- η πληρωμή δεν έχει ληφθεί ή
- η ADACOM θεωρεί ότι η έκδοση πιστοποιητικού στον Συνδρομητή θα βλάψει την υπόληψη της ADACOM.

Με την απόρριψη της αίτησης για πιστοποιητικό, ο Συνδρομητής δικαιούται είτε να επιστρέψει την ΕΔΔΥ σύμφωνα με την Ενότητα 9.1.5 είτε να τη φυλάξει για μελλοντική χρήση με δική του πλήρη ευθύνη. Σε περίπτωση που η ADACOM απορρίψει την αίτηση για εξ αποστάσεως Ψηφιακό Πιστοποιητικό, ο σχετικός λογαριασμός του Συνδρομητή δεν δημιουργείται και δεν απαιτούνται άλλες ενέργειες από το Συνδρομητή.

4.2.3 Χρόνος επεξεργασίας των αιτήσεων για πιστοποιητικό

Η ADACOM ξεκινά την επεξεργασία των αιτήσεων για πιστοποιητικό μέσα σε εύλογο χρονικό διάστημα από την παραλαβή τους. Ο χρόνος έκδοσης εξαρτάται σε ένα μεγάλο βαθμό από το εάν ο Συνδρομητής παρέχει τα στοιχεία και τα έγγραφα που είναι απαραίτητα για την εξακρίβωση της ταυτότητας. Δεν υπάρχει χρονική διατύπωση ως προς την ολοκλήρωση της επεξεργασίας μιας αίτησης εκτός εάν άλλως υποδεικνύεται στους σχετικούς Γενικούς Όρους και Προϋποθέσεις, στη ΠΠ/ΔΠΠ ή σε άλλη συμφωνία. Η αίτηση για Πιστοποιητικό παραμένει ενεργή έως ότου ολοκληρωθεί η διαδικασία εγγραφής από τον Συνδρομητή η οποία δεν μπορεί να ξεπερνάει τον ένα (1) μήνα από την ημερομηνία υποβολής του Εντύπου Αίτησης για έκδοση Πιστοποιητικού.

4.3 Έκδοση Πιστοποιητικού

4.3.1 Ενέργειες της ΑΠ κατά την έκδοση πιστοποιητικών

Το Πιστοποιητικό δημιουργείται και εκδίδεται μετά την έγκριση Αίτησης για Πιστοποιητικό από την ADACOM βάσει των στοιχείων της Αίτησης για Πιστοποιητικό.
Οι βάσεις δεδομένων και οι διαδικασίες της ΑΠ που συμβαίνουν κατά τη διάρκεια έκδοσης πιστοποιητικού προστατεύονται από μη εξουσιοδοτημένη μεταβολή. Μόλις ολοκληρωθεί η έκδοση, το Πιστοποιητικό αποθηκεύεται σε μια βάση δεδομένων και αποστέλλεται στον Συνδρομητή.

4.3.2 Ειδοποίηση του συνδρομητή από την ΑΠ για την έκδοση του πιστοποιητικού

Η ADACOM ενημερώνει τους Συνδρομητές ότι έχουν δημιουργηθεί τα σχετικά Πιστοποιητικά και παρέχει πρόσβαση στα Πιστοποιητικά ενημερώνοντάς τους ότι τα Πιστοποιητικά τους είναι διαθέσιμα. Τα Πιστοποιητικά καθίστανται διαθέσιμα στους Συνδρομητές ενημερώνοντάς τους μέσω ενός μηνύματος ηλεκτρονικού ταχυδρομείου.

4.3.3 Εγγραφή και έκδοση Εγκεκριμένου Πιστοποιητικού Ηλεκτρονικής Σφραγίδας που συμμορφώνεται με το πρότυπο ETSI TS 119 495 κατά PSD2

Πριν από την έναρξη της διαδικασίας έκδοσης, ο ΠΥΠ πρέπει να καταχωριστεί από μια ΑΕΑ και όλες οι σχετικές πληροφορίες πρέπει να είναι διαθέσιμες στο μητρώο ΑΕΑ / ΕΑΤ. Ο ΠΥΠ

υποβάλλει την αίτηση για πιστοποιητικό και παρέχει στην ADACOM όλη την απαραίτητη τεκμηρίωση που περιέχει ειδικά χαρακτηριστικά PSD2 (αριθμός εξουσιοδότησης PSD2 ή άλλο αναγνωρισμένο αναγνωριστικό, ρόλους, όνομα της ΑΕΑ), η ADACOM εκτελεί την επαλήθευση ταυτότητας, όπως απαιτείται στην παρ. 3.2.2.2 της παρούσας ΠΠ/ΔΠΠ. Η ADACOM επαληθεύει τα ειδικά χαρακτηριστικά PSD2 χρησιμοποιώντας πληροφορίες που παρέχονται από το μητρώο ΑΕΑ / ΕΑΤ. Η ADACOM εκδίδει το Εγκεκριμένο Πιστοποιητικό ηλεκτρονικής σφραγίδας σύμφωνα με τις απαιτήσεις προφίλ που παρέχονται στο ETSI TS 119 495.

4.4 Αποδοχή πιστοποιητικού

4.4.1 Ενέργειες που αποτελούν αποδοχή πιστοποιητικού

Οι ακόλουθες ενέργειες συνιστούν αποδοχή του πιστοποιητικού:

- η πραγματοποίηση λήψης (download) ενός Πιστοποιητικού συνιστά την αποδοχή του Πιστοποιητικού από τον Συνδρομητή,
- η μη υποβολή αντίρρησης όσον αφορά το Πιστοποιητικό ή το περιεχόμενό του εντός 24 ωρών, συνιστά αποδοχή του Πιστοποιητικού.

4.4.2 Δημοσίευση του πιστοποιητικού από την ΑΠ

Η ADACOM δημοσιεύει τα Πιστοποιητικά που εκδίδει σε δημοσίως προσβάσιμο διαδικτυακό χώρο αποθήκευσης.

4.4.3 Κοινοποίηση έκδοσης πιστοποιητικού από την ΑΠ προς άλλες οντότητες

Οι ΑΕ και οι ΤΑΕ δύναται να λάβουν ενημέρωση για την έκδοση των πιστοποιητικών που εγκρίνουν.

4.5 Χρήση ζεύγους κλειδιών και πιστοποιητικού

4.5.1 Χρήση ιδιωτικού κλειδιού συνδρομητή και πιστοποιητικού

Η χρήση του ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί του Πιστοποιητικού επιτρέπεται μόνο εφόσον ο Συνδρομητής έχει συμφωνήσει με τους Γενικούς Όρους και Προϋποθέσεις και έχει αποδεχτεί το Πιστοποιητικό. Το Πιστοποιητικό πρέπει να χρησιμοποιείται νόμιμα σύμφωνα με τους Γενικούς Όρους και Προϋποθέσεις Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης της ADACOM, και την παρούσα ΠΠ/ΔΠΠ. Η χρήση του Πιστοποιητικού πρέπει να συνάδει με τις επεκτάσεις του πεδίου «Χρήση Κλειδιού» (KeyUsage) που περιλαμβάνεται στο Πιστοποιητικό. Η χρήση του κλειδιού πιστοποιητικού είναι τύπου Β όπως ορίζεται στην ενότητα 4.3.2 of ETSI EN 319 412-2.

Οι Συνδρομητές πρέπει να κρατούν τα ιδιωτικά κλειδιά τους υπό τον αποκλειστικό έλεγχό τους, να προστατεύουν τα ιδιωτικά κλειδιά τους από μη εξουσιοδοτημένη χρήση και πρέπει να διακόψουν τη χρήση των ιδιωτικών κλειδιών μετά τη λήξη ή ανάκληση του πιστοποιητικού. Μέρη άλλα πέραν του Συνδρομητή δεν αρχειοθετούν το Ιδιωτικό Κλειδί του Συνδρομητή.

4.5.2 Χρήση δημόσιου κλειδιού και πιστοποιητικών από βασιζόμενο μέρος

Τα βασιζόμενα μέρη πρέπει να συναινούν στους Γενικούς Όρους και Προϋποθέσεις της ADACOM ως προϋπόθεση για να βασιστούν σε ένα Πιστοποιητικό.

Η εμπιστοσύνη σε ένα Πιστοποιητικό πρέπει να είναι εύλογη βάσει των συνθηκών. 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 πράξη εμπιστοσύνης, τα Βασιζόμενα Μέρη πρέπει να αξιολογούν ανεξάρτητα τα ακόλουθα:

- την καταλληλότητα της χρήσης του Πιστοποιητικού για κάθε σκοπό και να επιβεβαιώσουν ότι το Πιστοποιητικό έχει πράγματι χρησιμοποιηθεί για έναν κατάλληλο σκοπό ο οποίος δεν απαγορεύεται ή άλλως περιορίζεται από την παρούσα ΠΠ/ΔΠΠ. Η ADACOM δεν ευθύνεται για την καταλληλότητα της χρήσης του Πιστοποιητικού·
- ότι η χρήση του Πιστοποιητικού χρησιμοποιείται σύμφωνα με τις επεκτάσεις του πεδίου «Χρήση Κλειδιού» (KeyUsage) που περιλαμβάνεται στο Πιστοποιητικό·
- την κατάσταση του Πιστοποιητικού και όλων των ΑΠ στην αλυσίδα που εξέδωσε το Πιστοποιητικό. Εάν κάποιο από τα Πιστοποιητικά στην αλυσίδα Πιστοποιητικού έχει ανακληθεί, το Βασιζόμενο Μέρος είναι αποκλειστικά υπεύθυνο να αποφασίσει εάν η εμπιστοσύνη σε μια ψηφιακή υπογραφή από πλευράς Πιστοποιητικού Συνδρομητή τελικού χρήστη πριν από την ανάκληση του Πιστοποιητικού στην αλυσίδα Πιστοποιητικού, είναι εύλογη. Κάθε τέτοια εμπιστοσύνη γίνεται αποκλειστικά με κίνδυνο του ίδιου του Βασιζόμενου Μέρους.

Εάν υποτεθεί ότι η χρήση του Πιστοποιητικού είναι κατάλληλη, τα Βασιζόμενα Μέρη πρέπει να χρησιμοποιήσουν το κατάλληλο λογισμικό και/ή υλικό ώστε να μπορέσουν να εξακριβώσουν την υπογραφή ή άλλες κρυπτογραφικές λειτουργίες που επιθυμούν να διενεργήσουν, ως όρο αποδοχής ενός Πιστοποιητικού σε συνάρτηση με κάθε σχετική λειτουργία. Οι εν λόγω λειτουργίες περιλαμβάνουν την ταυτοποίηση της Αλυσίδας Πιστοποιητικών και την εξακρίβωση των ψηφιακών υπογραφών σε όλα τα Πιστοποιητικά της Αλυσίδας Πιστοποιητικών.

4.6 Ανανέωση πιστοποιητικού

Δεν εφαρμόζεται.

4.7 Επαναδημιουργία κλειδιών πιστοποιητικού

Η επαναδημιουργία κλειδιών πιστοποιητικού είναι η αίτηση για την έκδοση ενός νέου πιστοποιητικού που πιστοποιεί το νέο δημόσιο κλειδί.

4.7.1 Συνθήκες για την επαναδημιουργία κλειδιών πιστοποιητικού

Πριν από τη λήξη του υφιστάμενου Πιστοποιητικού του Συνδρομητή, ο Συνδρομητής πρέπει να επαναδημιουργήσει κλειδιά για το πιστοποιητικό ώστε να εξασφαλίσει τη συνέχιση της χρήσης του Πιστοποιητικού. Μπορεί να επαναδημιουργηθούν κλειδιά για το πιστοποιητικό και μετά τη λήξη του.

4.7.2 Ποιοι μπορούν να αιτηθούν την πιστοποίηση νέου δημόσιου κλειδιού

Μόνο ο Συνδρομητής δύναται να αιτηθεί την επαναδημιουργία κλειδιών για το Πιστοποιητικό.

4.7.3 Επεξεργασία αιτημάτων επαναδημιουργίας κλειδιών πιστοποιητικού

Οι διαδικασίες επαναδημιουργίας κλειδιών επιβεβαιώνουν ότι ο Συνδρομητής που επιθυμεί να ανανεώσει ένα Πιστοποιητικό Συνδρομητή είναι πράγματι ο Συνδρομητής (ή εξουσιοδοτημένος από τον Συνδρομητή) του Πιστοποιητικού.

Ο Συνδρομητής υποβάλλει μία αίτηση επαναδημιουργίας κλειδιών στην ΑΕ ή την ΤΑΕ της ADACOM και η ΑΕ ή η ΤΑΕ της ADACOM επαναβεβαιώνει την ταυτότητα του Συνδρομητή σύμφωνα με τις απαιτήσεις ταυτοποίησης και επαλήθευσης της ταυτότητας, όπως αυτές περιγράφονται στην ενότητα 3.3.1.

Εκτός της συγκεκριμένης διαδικασίας ή άλλης που έχει εγκριθεί από την ADACOM, οι απαιτήσεις για την επαλήθευση ταυτότητας μιας αρχικής Αίτησης για Πιστοποιητικό εφαρμόζονται για την επαναδημιουργία κλειδιών Πιστοποιητικού Συνδρομητή τελικού χρήστη.

4.7.4 Κοινοποίηση έκδοσης νέου πιστοποιητικού στον συνδρομητή

Η ενημέρωση του Συνδρομητή για την έκδοση του Πιστοποιητικού με επαναδημιουργημένα κλειδιά, πραγματοποιείται σύμφωνα με την ενότητα 4.3.2.

4.7.5 Ενέργεια που συνιστά αποδοχή του Πιστοποιητικού με επαναδημιουργημένα κλειδιά

Η ενέργεια που συνιστά αποδοχή του Πιστοποιητικού με επαναδημιουργημένα κλειδιά πραγματοποιείται σύμφωνα με την ενότητα 4.4.1.

4.7.6 Δημοσίευση του πιστοποιητικού με επαναδημιουργημένα κλειδιά από την ΑΠ

Το πιστοποιητικό με επαναδημιουργημένα κλειδιά δημοσιεύεται στον δημοσίως προσβάσιμο χώρο αποθήκευσης της ADACOM.

4.7.7 Κοινοποίηση έκδοσης πιστοποιητικού από την ΑΠ προς άλλες οντότητες

Οι ΑΕ και οι ΤΑΕ δύνανται να λάβουν ενημέρωση για την έκδοση των Πιστοποιητικών που εγκρίνουν.

4.8 Τροποποίηση πιστοποιητικού

4.8.1 Συνθήκες για την τροποποίηση πιστοποιητικού

Η τροποποίηση Πιστοποιητικού αναφέρεται στην αίτηση για την έκδοση ενός νέου πιστοποιητικού λόγω αλλαγών στις πληροφορίες που περιέχονται στο υφιστάμενο πιστοποιητικό (άλλες εκτός από το δημόσιο κλειδί του συνδρομητή).

Η τροποποίηση Πιστοποιητικού νοείται ως η Αίτηση για Πιστοποιητικό, σύμφωνα με τους όρους της ενότητας 4.1.

4.8.2 Ποιος μπορεί να αιτηθεί τροποποίηση πιστοποιητικού

Ανατρέξτε στην ενότητα 4.1.1.

4.8.3 Επεξεργασία αιτημάτων τροποποίησης πιστοποιητικού

Η ADACOM διενεργεί την ταυτοποίηση και την επαλήθευση της ταυτότητας όλων των απαιτούμενων στοιχείων του Συνδρομητή σύμφωνα με την ενότητα 3.2.

4.8.4 Κοινοποίηση έκδοσης νέου πιστοποιητικού στον συνδρομητή

Ανατρέξτε στην ενότητα 4.3.2.

4.8.5 Ενέργεια που συνιστά αποδοχή του τροποποιημένου πιστοποιητικού

Ανατρέξτε στην ενότητα 4.4.1.

4.8.6 Δημοσίευση του τροποποιημένου πιστοποιητικού από την ΑΠ

Ανατρέξτε στην ενότητα 4.4.2.

4.8.7 Κοινοποίηση έκδοσης πιστοποιητικού από την ΑΠ προς άλλες οντότητες

Ανατρέξτε στην ενότητα 4.4.3.

4.9 Αναστολή και ανάκληση πιστοποιητικού

Πριν τη λήξη τέλος της καθορισμένης περιόδου ισχύος του Πιστοποιητικού, η ανάκλησή του τερματίζει μόνιμα την ισχύ του. Πριν από την ανάκληση ενός Πιστοποιητικού, όλα τα αιτήματα ανάκλησης ταυτοποιούνται σύμφωνα με την Ενότητα 3.4.

Η ανάκληση των πιστοποιητικών γίνεται σύμφωνα με τις ακόλουθες ενότητες.
Για πιστοποιητικά που περιέχουν διεύθυνση ηλεκτρονικού ταχυδρομείου, η ανάκληση και η αναστολή πιστοποιητικών συμμορφώνονται με τις απαιτήσεις του CA/B Forum.

4.9.1 Συνθήκες για ανάκληση πιστοποιητικού

Οι Γενικοί Όροι και Προϋποθέσεις της ADACOM προβλέπουν την υποχρέωση και/ή το δικαίωμα στον Συνδρομητή να αιτηθεί την ανάκληση ενός Πιστοποιητικού. Μόνο στις περιπτώσεις που αναφέρονται παρακάτω μπορεί ένα Πιστοποιητικό Συνδρομητή να ανακληθεί από την ADACOM (ή από τον Συνδρομητή) και να δημοσιευτεί σε έναν Κατάλογο Ανακληθέντων Πιστοποιητικών (ΚΑΠ).

Ένα Πιστοποιητικό Συνδρομητή ανακαλείται εφόσον:

- Η ADACOM ή ένας Συνδρομητής έχουν λόγο να πιστεύουν ή έχουν σοβαρές υπόνοιες ότι έχει υπάρξει Έκθεση του ιδιωτικού κλειδιού ενός Συνδρομητή σε Κίνδυνο. Σε περίπτωση που αναφέρεται η σύναψη συμβιβασμού από τρίτο μέρος, η ADACOM απαιτεί την αντίστοιχη επιβεβαίωση από τον Συνδρομητή.

- Η ADACOM έχει λόγο να πιστεύει ότι ο Συνδρομητής έχει αθετήσει ουσιώδη υποχρέωση, δήλωση ή εγγύηση σύμφωνα με τους ισχύοντες Γενικούς Όρους και Προϋποθέσεις Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης
- Η ADACOM έχει λόγο να πιστεύει ότι το Πιστοποιητικό έχει εκδοθεί με τρόπο που δεν είναι ουσιαστικά σύμφωνος με τις διαδικασίες που απαιτούνται από την παρούσα ΠΠ/ΔΠΠ, ότι το Πιστοποιητικό εκδόθηκε προς πρόσωπο διαφορετικό από αυτό που κατονομάζεται ως το Υποκείμενο του Πιστοποιητικού ή το Πιστοποιητικό εκδόθηκε χωρίς την εξουσιοδότηση του προσώπου που κατονομάζεται ως το Υποκείμενο του εν λόγω Πιστοποιητικού.
- Η ADACOM γνωρίζει αλλαγές που επηρεάζουν την εγκυρότητα του πιστοποιητικού.
- Η κρυπτογράφηση που χρησιμοποιείται δεν εξασφαλίζει πλέον τη σύνδεση μεταξύ του Υποκειμένου και του δημόσιου κλειδιού.
- Η ADACOM έχει λόγο να πιστεύει ότι κάποιο πραγματολογικό στοιχείο στην Αίτηση για Πιστοποιητικό είναι ψευδές.
- Η ADACOM αποφαίνεται ότι δεν πληρούται ή δεν αίρεται καμία βασική προϋπόθεση για την Έκδοση Πιστοποιητικού.
- Ο Συνδρομητής χάνει τη δικαιοπρακτική του ικανότητα, κηρύσσεται απών ή αποβιώσας, έχει ρευστοποιηθεί ή δηλώσει πτώχευση, λαμβάνοντας υπόψη ότι το Πιστοποιητικό είναι σε κάθε περίπτωση μη μεταβιβάσιμο.
- Ο Συνδρομητής χάσει την ικανότητα να χρησιμοποιεί την τοπική ΕΔΔΥ ή κινητή συσκευή που απαιτείται για την πρόσβαση σε Εξ αποστάσεως ΕΔΔΥ
- Σε περίπτωση που το Υποκείμενο του Πιστοποιητικού είναι φυσικό πρόσωπο που συνδέεται με το νομικό πρόσωπο του Συνδρομητή και ο Συνδρομητής απαιτεί ανάκληση.
- Σε περίπτωση τελεσίδικης δικαστικής απόφασης που απαιτεί την εν λόγω ανάκληση ή ακύρωση.
- Το ιδιωτικό κλειδί της ΑΠ έχει εκτεθεί σε κίνδυνο.
- Ο Εποπτικός Φορέας ζητήσει την ανάκληση βάσει νόμου.
- Η ταυτότητα του Συνδρομητή δεν επανεπαληθεύεται με επιτυχία.
- Ο Συνδρομητής δεν έχει καταβάλει εγκαίρως το οφειλόμενο ποσό.
- Η συνέχιση της χρήσης του Πιστοποιητικού αυτού, ενδέχεται να προκαλέσει βλάβη στην ADACOM.
- Η εξουσιοδότηση του ΠΥΠ έχει ανακληθεί.
- Ο ρόλος του ΠΥΠ που περιέχεται στο πιστοποιητικό έχει ανακληθεί.

Όταν η ADACOM εξετάζει εάν η χρήση ενός Πιστοποιητικού είναι επιζήμια για αυτήν συνεκτιμά, μεταξύ άλλων, τα ακόλουθα:

- τη φύση και των αριθμό των καταγγελιών που έχει λάβει,
- την ταυτότητα των καταγγελλόντων,
- τη σχετική ισχύουσα νομοθεσία,
- τις αποκρίσεις στην επικαλούμενη επιζήμια χρήση από πλευράς Συνδρομητή.

Η ADACOM δύναται επίσης να ανακαλέσει ένα Πιστοποιητικό Διαχειριστή εάν η εξουσία του Διαχειριστή βάσει της οποίας ενεργεί με την ιδιότητα αυτή, έχει τερματιστεί ή με άλλον τρόπο ολοκληρωθεί.

Οι Γενικοί Όροι και Προϋποθέσεις Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης της ADACOM απαιτούν οι Συνδρομητές να ειδοποιούν αμέσως την ADACOM σχετικά με γνωστή ή πιθανολογούμενη έκθεση του ιδιωτικού τους κλειδιού σε κίνδυνο.

Μετά την έγκριση του αιτήματος για ανάκληση από πλευράς ΑΠ, το ανακληθέν Πιστοποιητικό δεν μπορεί να επανατεθεί σε ισχύ.

4.9.2 Ποιοι μπορούν να αιτηθούν την ανάκληση πιστοποιητικού

Αίτημα για την ανάκληση Εγκεκριμένου Πιστοποιητικού δύναται να υποβάλλει

- Η ΑΕ ή ΤΑΕ
- το φυσικό ή νομικό πρόσωπο, ή ο νόμιμος εκπρόσωπός του, το οποίο είναι ο Συνδρομητής του Πιστοποιητικού, ή ο διάδοχος που επιθυμεί την ανάκληση σε περίπτωση θανούντος Συνδρομητή (φυσικού προσώπου), με την προϋπόθεση ότι είναι επιλέξιμος από νομικής άποψης
- αρμόδιο δικαστήριο ή αρχή
- τον Εποπτικό Φορέα.
- Την ΑΕΑ που έχει εξουσιοδοτήσει ή καταχωρίσει τον ΠΥΠ

Αίτημα για την ανάκληση Πιστοποιητικού της ΑΠ δύναται να υποβάλλει

- το νομικό πρόσωπο το οποίο είναι ο Συνδρομητής του Πιστοποιητικού, με την προϋπόθεση ότι είναι επιλέξιμος από νομικής άποψης
- αρμόδιο δικαστήριο ή αρχή
- ο Εποπτικός Φορέας.

4.9.3 Διαδικασία υποβολής αιτήματος ανάκλησης

4.9.3.1 Διαδικασία για υποβολή αιτήματος ανάκλησης πιστοποιητικού συνδρομητή

Ένας Συνδρομητής ή ο διάδοχος του Συνδρομητή φυσικού προσώπου που επιθυμεί να υποβάλει αίτημα ανάκλησης πρέπει να κοινοποιήσει το αίτημά του στην ADACOM μέσω της αποστολής μηνύματος ηλεκτρονικού ταχυδρομείου στη διεύθυνση revoke@adacom.com, τηλεφωνικώς στο +30 210 9577255 ή εναλλακτικά μέσω της διαδικτυακής πύλης αυτοεξυπηρέτησης. Η ADACOM θα ανακαλέσει άμεσα το σχετικό Πιστοποιητικό.
Η κοινοποίηση για τη σχετική αίτηση ανάκλησης θα είναι σύμφωνη με την ενότητα 3.4.
Στην περίπτωση Πιστοποιητικού Σύντομης Διάρκειας, η ανάκλησή του από τον Συνδρομητή δεν είναι διαθέσιμη.

4.9.3.2 Procedure for Requesting Revocation in case of Qualified Certificates for Electronic Seal compliant with ETSI TS 119 495 under PSD2

Η ΑΕΑ, ως κάτοχος των ειδικών πληροφοριών PSD2, μπορεί να υποβάλει αίτημα ανάκλησης πιστοποιητικού μέσω της ηλεκτρονικής διεύθυνσης psd2@adacom.com.

- Το αίτημα πρέπει να έχει κάποια μορφή πιστοποίησης από την ΑΕΑ που το υποβάλλει. Η ADACOM θα ανακαλέσει το πιστοποιητικό μόλις επαληθεύσει το αίτημα ανάκλησης. Εάν δεν είναι ξεκάθαρο ή δεν υπονοείται γιατί ζητείται η ανάκληση ή ο λόγος δεν εμπίπτει στο πεδίο αρμοδιότητας της ΑΕΑ, τότε η ADACOM μπορεί να αποφασίσει να μην προβεί σε καμία ενέργεια.
- Εάν η ΑΕΑ ειδοποιήσει στην ADACOM ότι έχουν αλλάξει πληροφορίες που μπορούν να επηρεάσουν την εγκυρότητα του πιστοποιητικού, αλλά χωρίς πιστοποιημένο αίτημα με αποδεκτό λόγο για τον οποίο πρέπει να ανακληθεί το πιστοποιητικό, η ADACOM θα διερευνήσει αυτή την ειδοποίηση ανεξάρτητα από το περιεχόμενο και τη μορφή της, και θα ανακαλέσει το πιστοποιητικό εάν είναι απαραίτητο. Η ειδοποίηση αυτή δεν χρειάζεται να υποβληθεί σε επεξεργασία εντός 24 ωρών.

Εάν η ADACOM ενημερωθεί για τη διεύθυνση ηλεκτρονικού ταχυδρομείου όπου μπορεί να ενημερώνει την ΑΕΑ που προσδιορίζεται σε ανακλημένο πιστοποιητικό, τότε η ADACOM θα στείλει σε αυτή τη διεύθυνση πληροφορίες σχετικά με την ανάκληση του πιστοποιητικού.

4.9.4 Περίοδος χάριτος του αιτήματος ανάκλησης

Τα αιτήματα ανάκλησης πρέπει να υποβάλλονται το συντομότερο δυνατό, σε εύλογο από εμπορικής άποψης χρονικό διάστημα.

4.9.5 Χρονικό διάστημα μέσα στο οποίο η ΑΠ θα πρέπει να επεξεργαστεί το αίτημα ανάκλησης

Η ADACOM λαμβάνει όλα τα εύλογα από εμπορικής άποψης βήματα προκειμένου να επεξεργαστεί τα αιτήματα ανάκλησης χωρίς καθυστέρηση και, σε κάθε περίπτωση, η μέγιστη καθυστέρηση από τη στιγμή που η ADACOM λαμβάνει το αίτημα ανάκλησης σύμφωνα με την ενότητα 4.9.3, ενώ παράλληλα η απόφαση να αλλάξει τις πληροφορίες κατάστασης που είναι διαθέσιμες σε όλα τα βασιζόμενα μέρη πρέπει να μην ξεπερνά τις 24 ώρες. Εάν, παρόλα αυτά, το αίτημα ανάκλησης δεν μπορεί να επιβεβαιωθεί εντός 24 ωρών, τότε η κατάσταση δεν πρέπει να αλλάξει.

Αμέσως μετά την έγκριση του αιτήματος ανάκλησης, η ΑΠ ενημερώνει, όπου είναι εφικτό, τον Συνδρομητή και το Υποκείμενο του πιστοποιητικού για την εν λόγω ανάκληση μέσω μηνύματος ηλεκτρονικού ταχυδρομείου.

4.9.6 Απαιτήσεις ελέγχου κατάστασης ανακληθέντων πιστοποιητικών για βασιζόμενα μέρη

Τα Βασιζόμενα Μέρη πρέπει να ελέγχουν την κατάσταση του Πιστοποιητικού στο οποίο επιθυμούν να βασιστούν. Μία μέθοδος με την οποία τα Βασιζόμενα Μέρη μπορούν να ελέγξουν την κατάσταση του Πιστοποιητικού είναι να ανατρέξουν στον πιο πρόσφατο ΚΑΠ της ΑΠ που εξέδωσε το Πιστοποιητικό αυτό, στο οποίο το Βασιζόμενο Μέρος επιθυμεί να βασιστεί. Εναλλακτικά, τα Βασιζόμενα Μέρη δύνανται να ελέγχουν την κατάσταση του Πιστοποιητικού χρησιμοποιώντας τον δικτυακό αποθηκευτικό χώρο της ADACOM ή χρησιμοποιώντας την υπηρεσία OCSP. Η ADACOM παρέχει στα Βασιζόμενα Μέρη πληροφορίες σχετικά με τον τρόπο εξεύρεσης του κατάλληλου ΚΑΠ και του δικτυακού αποθηκευτικού χώρου ή του αποκριτή OCSP για τον έλεγχο της κατάστασης της ανάκλησης.
Λόγω των πολυάριθμων και διάφορων τοποθεσιών για τους αποθηκευτικούς χώρους του ΚΑΠ, συνιστάται στα βασιζόμενα μέρη να αποκτούν πρόσβαση στους ΚΑΠ με τη χρήση ενσωματωμένων διευθύνσεων URL στην επέκταση των Σημείων Διανομής ΚΑΠ ενός πιστοποιητικού.
Τοποθετείται ο κατάλληλος αποκριτής OCSP για ένα συγκεκριμένο πιστοποιητικό στην επέκταση Πρόσβασης Πληροφοριών Αρχής.
Οι πληροφορίες σχετικά με την κατάσταση ανάκλησης καθίστανται διαθέσιμες πέραν της περιόδου ισχύος του πιστοποιητικού.

4.9.7 Συχνότητα έκδοσης ΚΑΠ

Η ADACOM χρησιμοποιεί τις εκτός σύνδεσης ΑΠ Βάσης για να δημοσιεύει ΚΑΠ για τις Εκδότριες ΑΠ της τουλάχιστον κάθε 6 μήνες αλλά και κάθε φορά που ανακαλείται το Πιστοποιητικό μιας ΑΠ. ΟΙ ΚΑΠ για τα Πιστοποιητικά του Συνδρομητή εκδίδονται τουλάχιστον μία φορά την ημέρα.

4.9.8 Μέγιστος χρόνος αναμονής για τους ΚΑΠ

Οι ΚΑΠ ανακοινώνονται στον χώρο αποθήκευσης εντός εμπορικώς εύλογου χρονικού διαστήματος από τη δημιουργία τους. Πρόκειται για μια κατά κανόνα αυτοματοποιημένη διαδικασία, η οποία πραγματοποιείται μερικά λεπτά μετά τη δημιουργία του ΚΑΠ.

4.9.9 Διαθεσιμότητα ανάκλησης/κατάστασης πιστοποιητικών σε απευθείας σύνδεση

Η ανάκληση σε σύνδεση και άλλες πληροφορίες της κατάστασης του Πιστοποιητικού είναι διαθέσιμες μέσω ενός δικτυακού χώρου αποθήκευσης και του OCSP. Πέραν της δημοσίευσης των ΚΑΠ, η ADACOM παρέχει πληροφορίες για την κατάσταση των Πιστοποιητικών μέσω λειτουργιών διερευνήσεων στον αποθηκευτικό χώρο της ADACOM.
Οι πληροφορίες για την κατάσταση των Πιστοποιητικών όσον αφορά των Εγκεκριμένων Πιστοποιητικών είναι διαθέσιμες στον αποθηκευτικό χώρο της ADACOM στην εξής διεύθυνση: https://pki.adacom.com/repository

Οι αποκρίσεις OCSP παρέχονται εντός εμπορικά εύλογου χρόνου και το πολύ 10 δευτερόλεπτα μετά τη λήψη του αιτήματος, που υπόκεινται σε τυχόν καθυστερήσεις μετάδοσης μέσω του Διαδικτύου.
Οι αποκρίσεις OCSP συμμορφώνονται με το RFC 5019 ή/και το RFC 6960. Οι αποκρίσεις OCSP είτε
1. υπογράφονται από την ΑΠ που εξέδωσε το Πιστοποιητικό του οποίου ελέγχεται η κατάσταση ανάκλησης, ή
2. υπογράφονται από τον Αποκριτή OCSP του οποίου το πιστοποιητικό υπογράφεται από την ΑΠ που εξέδωσε το Πιστοποιητικό του οποίου ελέγχεται η κατάσταση ανάκλησης.
Στην τελευταία περίπτωση, το πιστοποιητικό που υπογράφει τον OCSP περιέχει μια επέκταση τύπου id-pkix-ocsp-nocheck, όπως ορίζεται από το RFC 6960.

Η μέγιστη καθυστέρηση μεταξύ της επιβεβαίωσης της ανάκλησης ενός πιστοποιητικού να τεθεί σε ισχύ και της αλλαγής των πληροφοριών για την κατάσταση του συγκεκριμένου πιστοποιητικού που καθίστανται διαθέσιμες στα βασιζόμενα μέρη είναι το ανώτερο τα 60 λεπτά. Εάν παρόλο που το αίτημα ανάκλησης απαιτεί την ανάκληση εκ των προτέρων (π.χ. η προγραμματισμένη παύση του Υποκειμένου από τα καθήκοντά του σε συγκεκριμένη ημερομηνία), η προγραμματισμένη ημερομηνία μπορεί να θεωρηθεί ως ο χρόνος επαλήθευσης.

4.9.10 Απαιτήσεις ελέγχου κατάστασης ανακληθέντων πιστοποιητικών σε απευθείας σύνδεση

Ένα βασιζόμενο μέρος πρέπει να ελέγχει την κατάσταση ενός πιστοποιητικού στο οποίο επιθυμεί να βασιστεί. Εάν ένα Βασιζόμενο Μέρος δεν ελέγχει την κατάσταση ενός Πιστοποιητικού στο οποίο το Βασιζόμενο Μέρος επιθυμεί να βασιστεί ανατρέχοντας στον πιο πρόσφατο σχετικό ΚΑΠ, το Βασιζόμενο Μέρος ελέγχει την κατάσταση του Πιστοποιητικού ανατρέχοντας στον αποθηκευτικό χώρο της ADACOM ή ζητώντας την κατάσταση του Πιστοποιητικού χρησιμοποιώντας τον ισχύοντα αποκριτή OCSP.

4.9.11 Άλλες διαθέσιμες μορφές αναγγελίας ανάκλησης

Δεν εφαρμόζεται.

4.9.12 Ειδικές απαιτήσεις σχετικά με την έκθεση του κλειδιού σε κίνδυνο

Η ADACOM καταβάλλει κάθε εύλογη από εμπορικής άποψης προσπάθεια προκειμένου να ειδοποιήσει τα πιθανά Βασιζόμενα Μέρη εάν ανακαλύψει ή έχει λόγο να πιστεύει ότι έχει υπάρξει Έκθεση σε Κίνδυνο του ιδιωτικού κλειδιού μιας εκ των ΑΠ της.

4.9.13 Συνθήκες για αναστολή πιστοποιητικού

Δεν εφαρμόζεται.

4.9.14 Ποιοι μπορούν να αιτηθούν την αναστολή πιστοποιητικού

Δεν εφαρμόζεται.

4.9.15 Διαδικασία υποβολής αιτήματος αναστολής

Δεν εφαρμόζεται.

4.9.16 Περιορισμός για την περίοδο αναστολής

Δεν εφαρμόζεται.

4.10 Υπηρεσίες κατάστασης πιστοποιητικού

4.10.1 Λειτουργικά χαρακτηριστικά

Οι πληροφορίες κατάστασης πιστοποιητικών είναι διαθέσιμες μέσω του ανταποκριτή CRL (ΚΑΠ) και OCSP. Ο αύξων αριθμός του πιστοποιητικού που έχει ανακληθεί παραμένει στον ΚΑΠ μέχρι να δημοσιευθεί ένας επιπλέον ΚΑΠ μετά τη λήξη της περιόδου ισχύος του πιστοποιητικού. Οι πληροφορίες OCSP για τα πιστοποιητικά συνδρομητών ενημερώνονται σύμφωνα με την ενότητα 4.9.9.

4.10.2 Διαθεσιμότητα υπηρεσιών

Η ADACOM διασφαλίζει ότι 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 0,1% ετησίως.

4.10.3 Προαιρετικά χαρακτηριστικά

Δεν εφαρμόζεται.

4.11 Τερματισμός συνδρομής

Ένας Συνδρομητής μπορεί να τερματίσει τη συνδρομή του για ένα Εγκεκριμένο Πιστοποιητικό της ADACOM με τους εξής τρόπους:

- επιτρέποντας τη λήξη του Εγκεκριμένου Πιστοποιητικού χωρίς την επαναδημιουργία κλειδιών για το συγκεκριμένο Πιστοποιητικό,
- ανακαλώντας το Εγκεκριμένο Πιστοποιητικό πριν από τη λήξη του χωρίς να προχωρήσει σε αντικατάστασή του.

4.12 Παρακαταθήκη και ανάκτηση κλειδιού

Δεν εφαρμόζεται.

4.12.1 Πολιτικές και πρακτικές για την παρακαταθήκη και την ανάκτηση κλειδιού

Δεν εφαρμόζεται.

4.12.2 Πολιτικές και πρακτικές για την ενθυλάκωση και την ανάκτηση του κλειδιού της περιόδου λειτουργίας

Δεν εφαρμόζεται.

5. ΜΕΤΡΑ ΕΛΕΓΧΟΥ ΤΩΝ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΤΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΤΗΣ ΛΕΙΤΟΥΡΓΙΑΣ

5.1 Φυσικοί έλεγχοι

Η ADACOM εφαρμόζει την Πολιτική Φυσικής Ασφάλειας (Physical Security Policy) της ADACOM, η οποία υποστηρίζει τις απαιτήσεις ασφαλείας που παρατίθενται στην παρούσα ΠΠ/ΔΠΠ. Η συμμόρφωση με τις συγκεκριμένες πολιτικές αποτελεί μέρος των απαιτήσεων ελέγχου της ADACOM, όπως αυτές περιγράφονται στην ενότητα 8. Η Πολιτική Φυσικής Ασφάλειας της ADACOM περιέχει ευαίσθητες πληροφορίες για την ασφάλεια και διατίθεται μόνο κατόπιν συμφωνίας με την ADACOM. Μια περίληψη των απαιτήσεων αυτών, παρατίθεται κατωτέρω.

5.1.1 Τοποθεσία και κατασκευή του χώρου

Οι λειτουργίες των ΑΠ και ΑΕ της ADACOM διενεργούνται εντός ενός φυσικά προστατευόμενου περιβάλλοντος το οποίο αποτρέπει, προλαμβάνει και εντοπίζει τη μη εξουσιοδοτημένη χρήση και πρόσβαση σε εσωτερικά ή εξωτερικά συστήματα και ευαίσθητες πληροφορίες ή την αποκάλυψη αυτών.

Η ADACOM διατηρεί εγκαταστάσεις Αποκατάστασης Καταστροφών όσον αφορά τις λειτουργίες ΑΠ. Οι εγκαταστάσεις Αποκατάστασης Καταστροφών της ADACOM προστατεύονται από πολλαπλά επίπεδα φυσικής ασφάλειας συγκρίσιμα προς αυτά της κύριας εγκατάστασης της ADACOM.

5.1.2 Φυσική πρόσβαση

Τα συστήματα της ΑΠ της ADACOM προστατεύονται από επτά (7) επίπεδα φυσικής ασφάλειας, όπου απαιτείται η απόκτηση πρόσβασης στο χαμηλότερο επίπεδο ασφάλειας πριν δοθεί η πρόσβαση σε υψηλότερο επίπεδο.

Η προοδευτική περιοριστική προνομιακή φυσική πρόσβαση ελέγχει την πρόσβαση σε κάθε επίπεδο ασφάλειας. Οι ευαίσθητες λειτουργίες της ΑΠ, κάθε δραστηριότητα που σχετίζεται με τον κύκλο ζωής της διαδικασίας πιστοποίησης, όπως η πιστοποίηση γνησιότητας, η εξακρίβωση και η έκδοση, διενεργούνται εντός ενός αυστηρώς περιορισμένου φυσικού χώρου. Η πρόσβαση σε κάθε επίπεδο απαιτεί τη χρήση ειδικής κάρτας πρόσβασης (proximity card) από τους υπαλλήλους. Η φυσική πρόσβαση καταγράφεται και βιντεοσκοπείται αυτόματα. Για τη φυσική πρόσβαση σε ορισμένα επίπεδα ασφάλειας απαιτείται η ταυτόχρονη χρήση των ειδικών καρτών πρόσβασης και των βιομετρικών στοιχείων (επαλήθευση ταυτότητας με δύο παραμέτρους). Δεν επιτρέπεται η πρόσβαση προσωπικού άνευ συνοδείας, συμπεριλαμβανομένων των μη έμπιστων υπαλλήλων ή επισκεπτών, σε αυτούς τους χώρους ασφάλειας.

Το σύστημα φυσικής ασφάλειας περιλαμβάνει επίπεδα για την ασφάλεια της διαχείρισης των κλειδιών τα οποία εξυπηρετούν για την προστασία τόσο της αποθήκευσης με σύνδεση (online) όσο και της αποθήκευσης εκτός σύνδεσης (offline) των Κρυπτογραφικών Μονάδων Υπογραφών (ΚΜΥ) και του υλικού δημιουργίας κλειδιών. Οι χώροι που χρησιμοποιούνται για τη δημιουργία και την αποθήκευση κρυπτογραφικού υλικού απαιτούν διπλό έλεγχο, ο κάθε έλεγχος διενεργείται μέσω της ταυτόχρονης χρήσης των ειδικών καρτών πρόσβασης και των βιομετρικών στοιχείων. Οι ΚΜΥ σε σύνδεση (Online) προστατεύονται μέσω της χρήσης κλειδωμένων ερμαριών. Οι ΚΜΥ εκτός σύνδεσης (Offline) προστατεύονται μέσω της χρήσης κλειδωμένων θυρίδων, ερμαριών και κιβωτίων. Η πρόσβαση στις ΚΜΥ και το υλικό δημιουργίας κλειδιών είναι περιορισμένη σύμφωνα με τις απαιτήσεις που αφορούν τον διαχωρισμό των καθηκόντων της ADACOM. Το άνοιγμα και το κλείσιμο των ερμαριών και θυρίδων στα εν λόγω επίπεδα, καταγράφεται για τους σκοπούς του ελέγχου.
Οι λειτουργίες της ΑΕ της ADACOM προστατεύονται με χρήση ελέγχου φυσικής πρόσβασης καθιστώντας την προσβάσιμη μόνο από τους εξουσιοδοτημένους υπαλλήλους. Η πρόσβαση σε ασφαλείς χώρους του κτιρίου απαιτεί τη χρήση κάρτας πρόσβασης. Η χρήση της κάρτας πρόσβασης καταγράφεται στο κεντρικό σύστημα ελέγχου του κτιρίου.

Οι καταγραφές χρήσης καρτών και αρχείων εικόνας ελέγχονται συστηματικά. Η ADACOM αποθηκεύει με ασφάλεια σε ειδικά μέσα, όλα τα μέσα αποθήκευσης (ψηφιακά και έντυπα), τα οποία περιέχουν ευαίσθητα δεδομένα σχετικά με τις λειτουργίες της ΑΕ.

Η ADACOM αποθηκεύει με ασφάλεια τις Κρυπτογραφικές Μονάδες Υπογραφών (ΚΜΥ) που χρησιμοποιούνται για τη δημιουργία και αποθήκευση των ιδιωτικών κλειδιών των εξ αποστάσεως Ψηφιακών Υπογραφών των Συνδρομητών. Η πρόσβαση στους χώρους που χρησιμοποιούνται για την αποθήκευση και δημιουργία των κλειδιών ελέγχεται και καταγράφεται από το κεντρικό σύστημα ελέγχου πρόσβασης του κτιρίου. Οι καταγραφές χρήσης καρτών και αρχείων εικόνας ελέγχονται συστηματικά

5.1.3 Παροχή ηλεκτρικού ρεύματος και κλιματισμός

Οι ασφαλείς εγκαταστάσεις της ADACOM είναι εξοπλισμένες με κύρια και εφεδρικά:

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

5.1.4 Έκθεση σε νερό

Η ADACOM έχει λάβει εύλογα μέτρα προφύλαξης προκειμένου να ελαχιστοποιήσει τους κινδύνους έκθεσης των συστημάτων της σε νερό.

5.1.5 Πρόληψη και προστασία από πυρκαγιά

Η ADACOM έχει λάβει όλες τις εύλογες προφυλάξεις για την πρόληψη και κατάσβεση πυρκαγιάς ή άλλης επιζήμιας έκθεσης σε φλόγα ή καπνό. Αυτά τα μέτρα πρόληψης και προστασίας από φωτιά της ADACOM έχουν σχεδιαστεί ώστε να πληρούν τους εθνικούς κανονισμούς πυρασφάλειας.

5.1.6 Αποθήκευση μέσων

Όλα τα μέσα που περιέχουν τις πληροφορίες για το λογισμικό και τα δεδομένα παραγωγής, για τους ελέγχους, τα αρχεία ή τα εφεδρικά αντίγραφα αποθηκεύονται εντός των εγκαταστάσεων της ADACOM ή σε ασφαλή εγκατάσταση αποθήκευσης, εκτός του χώρου εγκατάστασης της ADACOM η οποία διαθέτει τα απαραίτητα φυσικά και λογικά μέτρα ελέγχου πρόσβασης. Τα μέτρα αυτά έχουν σχεδιαστεί ώστε να περιορίζουν την πρόσβαση αποκλειστικά σε

εξουσιοδοτημένο προσωπικό και να προστατεύουν τα εν λόγω μέσα αποθήκευσης έναντι οιασδήποτε τυχαίας καταστροφής (π.χ. από νερό, φωτιά).

5.1.7 Διάθεση αποβλήτων

Τα ευαίσθητα έγγραφα και υλικά περνάνε σε καταστροφέα εγγράφων πριν από την απόρριψή τους. Τα μέσα που χρησιμοποιήθηκαν για τη συλλογή ή τη μεταβίβαση ευαίσθητων πληροφοριών καθίστανται μη αναγνώσιμα πριν από την απόρριψή τους. Οι διατάξεις κρυπτογράφησης καταστρέφονται με φυσικό τρόπο ή διαγράφονται τα δεδομένα τους σύμφωνα με τις οδηγίες του κατασκευαστή πριν από την απόρριψή τους. Τα υπόλοιπα απόβλητα διατίθενται σύμφωνα με τις σύνηθες απαιτήσεις διάθεσης αποβλήτων της ADACOM.

5.1.8 Δημιουργία εφεδρικών αντιγράφων ασφαλείας εκτός του χώρου εγκατάστασης

Η ADACOM δημιουργεί σε τακτά διαστήματα εφεδρικά αντίγραφα για τα δεδομένα των κυριότερων συστημάτων,τα δεδομένα αρχείων καταγραφής ελέγχου και άλλων ευαίσθητων πληροφοριών. Τα εφεδρικά αντίγραφα αποθηκεύονται εκτός του κυρίου χώρου εγκατάστασης με φυσικά μέσα προστασίας, χρησιμοποιώντας την ασφαλή Εγκατάσταση Αποκατάστασης Καταστροφών εκτός του κυρίως χώρου εγκατάστασης σύμφωνα με το «Σχέδιο Αποκατάστασης Καταστροφών της ADACOM».

5.2 Διαδικαστικοί έλεγχοι

5.2.1 Ρόλοι εμπιστοσύνης

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 αιτημάτων για επαναδημιουργία κλειδιών 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 εξυπηρέτησης πελατών,
- το προσωπικό της ΤΑΕ/ΑΕ,
- το προσωπικό που εμπλέκεται στις διαδικασίες κρυπτογράφησης,
- το προσωπικό ασφαλείας,
- οι εσωτερικού ελεγκτές,
- το προσωπικό διαχείρισης συστημάτων,
- οι εξουσιοδοτημένοι μηχανικοί και
- τα στελέχη στα οποία έχει ανατεθεί η διαχείριση της αξιοπιστίας της υποδομής.

Η ADACOM θεωρεί τις κατηγορίες του προσωπικού που προσδιορίζονται στην παρούσα ενότητα ως Έμπιστα Πρόσωπα τα οποία κατέχουν Θέση Εμπιστοσύνης. Τα άτομα που επιθυμούν να αποκτήσουν Θέση Εμπιστοσύνης πρέπει να ολοκληρώσουν με επιτυχία τις απαιτήσεις ελέγχου που καθορίζονται στην παρούσα ΠΠ/ΔΠΠ. Οι λειτουργίες και τα καθήκοντα που εκτελούνται από άτομα με έμπιστους ρόλους διανέμονται έτσι ώστε ένα μόνο άτομο να μην μπορεί να παρακάμψει τα μέτρα ασφαλείας ή να υπονομεύσει την ασφάλεια και την αξιοπιστία των λειτουργιών της ΥΔΚ.

Οι έμπιστοι ρόλοι διορίζονται από ανώτερα στελέχη. Ο κατάλογος του προσωπικού που διορίζεται σε αξιόπιστους ρόλους διατηρείται και αναθεωρείται κάθε χρόνο. Τα πρόσωπα που επιθυμούν να αποκτήσουν την ιδιότητα του Έμπιστου Προσώπου αποκτώντας μια Θέση Εμπιστοσύνης πρέπει να πληρούν επιτυχώς τις απαιτήσεις ελέγχου ασφαλείας της παρούσας ΠΠ/ΔΠΠ.

5.2.2 Αριθμός προσώπων που απαιτούνται ανά τομέα εργασίας

Η ADACOM έχει θεσπίσει, διατηρεί και επιβάλλει αυστηρές διαδικασίες ελέγχου προκειμένου να διασφαλίσει τον διαχωρισμό των καθηκόντων βάσει των αρμοδιοτήτων κάθε θέσης εργασίας και να εξασφαλίσει ότι για την εκτέλεση ευαίσθητων εργασιών απαιτείται η συμμετοχή πολλών Έμπιστων Προσώπων.

Εφαρμόζονται πολιτικές και διαδικασίες ελέγχου προκειμένου να διασφαλιστεί ο διαχωρισμός των καθηκόντων βάσει των αρμοδιοτήτων κάθε θέσης εργασίας. Οι πιο ευαίσθητες εργασίες, όπως είναι η πρόσβαση και ο χειρισμός του κρυπτογραφικού εξοπλισμού (ΑΚΜ) της ΑΠ και του σχετικού υλικού των κλειδιών, απαιτούν τη συμμετοχή πολλών Έμπιστων Προσώπων.

Αυτές οι εσωτερικές διαδικασίες ελέγχου έχουν σχεδιαστεί με τρόπο τέτοιο ώστε να διασφαλίζουν ότι τουλάχιστον δύο Έμπιστα Πρόσωπα του προσωπικού πρέπει να διαθέτουν φυσική ή λογική πρόσβαση στη διάταξη. Η πρόσβαση στον κρυπτογραφικό εξοπλισμό της ΑΠ πραγματοποιείται αυστηρά από πολλαπλά Έμπιστα Πρόσωπα καθ' όλη τη διάρκεια ζωής του, από την παραλαβή και τον έλεγχό του μέχρι την τελική λογική ή/και φυσική καταστροφή του. Μόλις μια μονάδα ενεργοποιηθεί με τα κλειδιά λειτουργίας, εφαρμόζονται περαιτέρω μέτρα ελέγχου πρόσβασης ώστε να υπάρχει διαμοιρασμένος έλεγχος τόσο της φυσικής όσο και της λογικής πρόσβασης στη διάταξη. Τα πρόσωπα που έχουν φυσική πρόσβαση σε μονάδες δεν κατέχουν «Μερίδια Απορρήτου» και αντιστρόφως.

5.2.3 Ταυτοποίηση και επαλήθευση της ταυτότητας για κάθε ρόλο

Για τα μέλη του προσωπικού που επιθυμούν να καταστούν Έμπιστα Πρόσωπα, η εξακρίβωση της ταυτότητας διενεργείται μέσω της διαδικασίας του Ανθρώπινου Δυναμικού της ADACOM βάσει ελέγχων ευρέως αναγνωρισμένων μορφών ταυτοποίησης (π.χ., διαβατήρια ή δελτία ταυτότητας). Η ταυτότητα επαληθεύεται περαιτέρω με τις διαδικασίες ελέγχου του ιστορικού, σύμφωνα με την ενότητα 5.3.2.

Η ADACOM διασφαλίζει ότι το προσωπικό έχει αποκτήσει την ιδιότητα του Έμπιστου και έχει ήδη χορηγηθεί η έγκριση του αρμόδιου τμήματος, προτού στο συγκεκριμένο προσωπικό:

- εκδοθούν διατάξεις πρόσβασης και χορηγηθούν άδειες πρόσβασης στις απαιτούμενες εγκαταστάσεις,
- εκδοθούν ηλεκτρονικά διαπιστευτήρια για την πρόσβαση και την τέλεση συγκεκριμένων λειτουργιών της ΑΠ, της ΑΕ ή άλλων πληροφοριακών συστημάτων της ADACOM.

Η ADACOM έχει υλοποιήσει ένα σύστημα ελέγχου πρόσβασης το οποίο ταυτοποιεί τις αρχές και καταχωρεί όλους τους χρήστες των πληροφοριακών συστημάτων της ADACOM κατά τρόπο αξιόπιστο.

Δημιουργούνται λογαριασμοί χρηστών για το προσωπικό σε συγκεκριμένους ρόλους που απαιτούν πρόσβαση στο σχετικό σύστημα. Όλοι οι χρήστες πρέπει να συνδέονται με συγκεκριμένο λογαριασμό και οι εντολές διαχείρισης είναι διαθέσιμες μόνο με ρητή άδεια και έλεγχο της εκτέλεσης. Οι άδειες του συστήματος αρχείων, καθώς και άλλες διαθέσιμες δυνατότητες στο μοντέλο ασφάλειας του λειτουργικού συστήματος χρησιμοποιούνται για να αποτραπεί οποιαδήποτε άλλη χρήση.

Οι λογαριασμοί χρηστών κλειδώνονται το συντομότερο δυνατό όταν το επιβάλει η αλλαγή των ρόλων. Οι κανόνες που αφορούν την ασφάλεια ελέγχονται ετησίως.

5.2.4 Ρόλοι που απαιτούν διαχωρισμό καθηκόντων

Οι ρόλοι που απαιτούν τον διαχωρισμό καθηκόντων περιλαμβάνουν, ενδεικτικά, σε αυτούς που έχουν ως αντικείμενο τα εξής:

- την ταυτοποίηση και τον χειρισμό των στοιχείων στις Αιτήσεις για Πιστοποιητικό,
- την αποδοχή, την απόρριψη ή άλλη επεξεργασία των Αιτήσεων για Πιστοποιητικό, των αιτημάτων για ανάκληση ή των αιτημάτων για επαναδημιουργία κλειδιών ή των πληροφοριών εγγραφής,
- την έκδοση ή την ανάκληση Πιστοποιητικών, συμπεριλαμβανομένου του προσωπικού που έχει πρόσβαση στα τμήματα περιορισμένης πρόσβασης του χώρου αποθήκευσης,
- τη δημιουργία, την έκδοση ή την καταστροφή ενός πιστοποιητικού της ΑΠ,
- τη φόρτωση μιας ΑΠ σε ένα περιβάλλον Παραγωγής,
- Την πρόσβαση σε εξ αποστάσεως ΕΔΔΥ
- Τα αντίγραφα ασφαλείας, αρχεία και τις λειτουργίες τήρησης αρχείων,
- Τις λειτουργίες ελέγχου, αναθεώρησης, εποπτείας ή συνδιαλλαγής

5.3 Έλεγχοι προσωπικού

Το προσωπικό που πρόκειται να αποκτήσει την ιδιότητα του Έμπιστου Προσώπου πρέπει να προσκομίζει τα απαραίτητα αποδεικτικά στοιχεία για το παρελθόν του, τα τυπικά του προσόντα και την εμπειρία που απαιτούνται για την εκτέλεση των καθηκόντων της επιδιωκόμενης θέσης με επαρκή και ικανοποιητικό τρόπο, καθώς και αποδεικτικά στοιχεία από κρατική εξουσιοδότηση, εάν υπάρχει, που είναι απαραίτητη για την εκτέλεση υπηρεσιών πιστοποίησης δυνάμει κρατικών συμβάσεων. Για το προσωπικό που κατέχει Θέσεις Εμπιστοσύνης, οι έλεγχοι ιστορικού επαναλαμβάνονται τουλάχιστον κάθε πέντε (5) έτη.

5.3.1 Απαιτήσεις σχετικά με τα προσόντα, την εμπειρία και την εξουσιοδότηση

Η ADACOM ζητά από το προσωπικό που πρόκειται να αποκτήσει την ιδιότητα του Έμπιστου Προσώπου να προσκομίσει τα απαραίτητα αποδεικτικά στοιχεία για το ιστορικό του, τα τυπικά του προσόντα και την εμπειρία που απαιτούνται για την εκτέλεση των καθηκόντων της επιδιωκόμενης θέσης, όπως ορίζονται στα έγγραφα της σύμβασης απασχόλησης, της περιγραφής της θέσης εργασίας και των ρόλων και αρμοδιοτήτων με επαρκή και ικανοποιητικό τρόπο, καθώς και αποδεικτικά στοιχεία από κρατική εξουσιοδότηση, εάν υπάρχει, που είναι απαραίτητη για την εκτέλεση των υπηρεσιών πιστοποίησης δυνάμει κρατικών συμβάσεων προτού εκτελεστεί οποιαδήποτε επιχειρησιακή λειτουργία ή λειτουργία για την ασφάλεια.

Οι συμβάσεις απασχόλησης που είναι υπογεγραμμένες από τους υπαλλήλους της ADACOM προβλέπουν τις ακόλουθες υποχρεώσεις:

- τη διατήρηση του απορρήτου των εμπιστευτικών πληροφοριών που έχουν λάβει γνώση κατά την εκτέλεση των καθηκόντων τους,
- την αποτροπή κατοχής επιχειρηματικών συμφερόντων σε μια εταιρεία που μπορεί να επηρεάσει την κρίση τους όσον αφορά την παροχή της υπηρεσίας και τη διασφάλιση ότι δεν έχουν τιμωρηθεί για έγκλημα που έχουν διαπράξει με δόλο.
- Όλα τα μέλη του προσωπικού σε Ρόλους Εμπιστοσύνης δεν έχουν συμφέροντα που δύνανται να επηρεάσουν την αμεροληψία τους αναφορικά με τις δραστηριότητες της ADACOM.

5.3.2 Διαδικασίες ελέγχου ιστορικού

Πριν από την έναρξη απασχόλησης σε Ρόλο Εμπιστοσύνης, η ADACOM διενεργεί έλεγχο ιστορικού ο οποίος περιλαμβάνει τα ακόλουθα:

- την επαλήθευση της ταυτότητας,
- τον έλεγχο της προηγούμενης απασχόλησης και των επαγγελματικών συστάσεων (εφόσον είναι διαθέσιμες),
- την επιβεβαίωση του ανώτερου ή πιο πρόσφατου πτυχίου εκπαίδευσης,
- την αναζήτηση του εθνικού ποινικού μητρώου,
- τον έλεγχο χρηματοοικονομικών αρχείων.

Στο μέτρο που οι απαιτήσεις που επιβάλλονται από την παρούσα ενότητα δεν δύνανται να ικανοποιηθούν εξαιτίας απαγόρευσης ή περιορισμού της ισχύουσας νομοθεσίας ή άλλων συνθηκών, η ADACOM θα χρησιμοποιήσει μια υποκατάστατη διερευνητική τεχνική η οποία επιτρέπεται από τον νόμο και παρέχει παρόμοιες πληροφορίες.

Στοιχεία που αποκαλύπτονται κατά τον έλεγχο ιστορικού και τα οποία μπορούν να αποτελέσουν τη βάση για απόρριψη υποψηφίων από Θέσεις Εμπιστοσύνης ή για τη λήψη μέτρων κατά υφιστάμενου Έμπιστου Προσώπου περιλαμβάνουν γενικά (ενδεικτικά) τα εξής:

- τις ψευδείς δηλώσεις που πραγματοποίησε ο υποψήφιος ή το Έμπιστο Πρόσωπο,
- τις ιδιαίτερα δυσμενείς ή αναξιόπιστες προσωπικές συστάσεις,
- τις καταδίκες για ορισμένα ποινικά αδικήματα, και
- τις ενδείξεις για έλλειψη φορολογικής ενημερότητας.

Οι αναφορές που περιλαμβάνουν τέτοιου είδους πληροφορίες αξιολογούνται από το προσωπικό της διεύθυνσης ανθρώπινου δυναμικού και του τομέα ασφάλειας, το οποίο προσδιορίζει τις απαραίτητες ενέργειες ανάλογα με τη μορφή, τη σπουδαιότητα, και τη συχνότητα της συμπεριφοράς που αποκαλύπτεται από τον έλεγχο του ιστορικού. Οι ενέργειες αυτές δύνανται να περιλαμβάνουν μέτρα που αφορούν έως και την ακύρωση της προσφοράς εργασίας στον υποψήφιο για τη Θέση Εμπιστοσύνης ή την καταγγελία της σύμβασης όσον αφορά υφιστάμενα Έμπιστα Πρόσωπα.

Η χρήση των πληροφοριών που αποκαλύπτονται κατά τον έλεγχο του ιστορικού ώστε να ληφθούν οι σχετικές ενέργειες, υπόκειται στην ισχύουσα νομοθεσία.

5.3.3 Απαιτήσεις εκπαίδευσης

Η ADACOM, με την πρόσληψη, παρέχει εκπαίδευση στο προσωπικό της που συμμετέχει στις λειτουργίες της ΥΔΚ, καθώς και κατά τη διάρκεια της εργασίας, η οποία κρίνεται απαραίτητη για την εκτέλεση των εργασιακών καθηκόντων τους με επαρκή και ικανοποιητικό τρόπο. Η ADACOM διατηρεί αρχεία για τις εκπαιδεύσεις αυτές. Η ADACOM αναθεωρεί και βελτιώνει περιοδικά τα εκπαιδευτικά της προγράμματα ανάλογα με τις ανάγκες της.

Τα εκπαιδευτικά προγράμματα της ADACOM είναι προσαρμοσμένα στις αρμοδιότητες του ατόμου και περιλαμβάνουν τα ακόλουθα:

- τις βασικές έννοιες της ΥΔΚ,
- τις αρμοδιότητες των θέσεων εργασίας,
- την πολιτική και τις διαδικασίες ασφάλειας και λειτουργίας της ADACOM,
- 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 ADACOM παρέχει επανεκπαίδευση και ενημέρωση για τις σύγχρονες εξελίξεις στο προσωπικό της στον βαθμό και τη συχνότητα που απαιτείται προκειμένου να διασφαλιστεί ότι το εν λόγω προσωπικό διατηρεί το απαιτούμενο επίπεδο επάρκειας γνώσεων ώστε να εκτελεί τα καθήκοντα του με επαρκή και ικανοποιητικό τρόπο.

5.3.5 Συχνότητα και ακολουθία εναλλαγής θέσεων εργασίας

Η εναλλαγή θέσεων δεν εφαρμόζεται.

5.3.6 Κυρώσεις για μη εξουσιοδοτημένες ενέργειες

Λαμβάνονται τα κατάλληλα πειθαρχικά μέτρα για τους εργαζομένους ή αντιπροσώπους που δεν συμμορφώνονται με την παρούσα ΠΠ/ΔΠΠ, για μη εξουσιοδοτημένες ενέργειες ή άλλες παραβάσεις των πολιτικών και διαδικασιών της ADACOM. Τα εν λόγω πειθαρχικά μέτρα μπορούν να περιλαμβάνουν ακόμα και την καταγγελία της σύμβασης εργασίας και είναι ανάλογα με τη συχνότητα και τη σοβαρότητα των μη εξουσιοδοτημένων ενεργειών.

5.3.7 Απαιτήσεις ανεξάρτητου αναδόχου

Σε περιορισμένες περιπτώσεις, ανεξάρτητοι ανάδοχοι ή σύμβουλοι δύνανται να χρησιμοποιούνται για την πλήρωση Θέσεων Εμπιστοσύνης. Οποιοσδήποτε σχετικός ανεξάρτητος ανάδοχος ή σύμβουλος υπόκειται στα ίδια λειτουργικά κριτήρια και κριτήρια ασφαλείας που ισχύουν και για τους εργαζομένους της ADACOM που κατέχουν ανάλογη θέση.

Σε ανεξάρτητους αναδόχους και συμβούλους για τους οποίους δεν έχουν ολοκληρωθεί οι διαδικασίες ελέγχου του ιστορικού που προσδιορίζονται στην ενότητα 5.3.2, η πρόσβαση στις ασφαλείς εγκαταστάσεις της ADACOM επιτρέπεται μόνον εφόσον οι ανωτέρω αναφερόμενοι συνοδεύονται και επιβλέπονται άμεσα και συνεχώς από Έμπιστα Πρόσωπα.

5.3.8 Έντυπα που διατίθενται στο προσωπικό

Η ADACOM παρέχει στους υπαλλήλους της την απαιτούμενη εκπαιδευτική και άλλη τεκμηρίωση που είναι απαραίτητη για την εκτέλεση των αρμοδιοτήτων της θέσης εργασίας τους με επαρκή και ικανοποιητικό τρόπο, συμπεριλαμβανομένου ενός αντιγράφου της παρούσας ΠΠ/ΔΠΠ και άλλων τεχνικών και επιχειρησιακών εγγράφων που απαιτούνται για τη διατήρηση της ακεραιότητας των λειτουργιών της ΑΠ της ADACOM. Οι εργαζόμενοι έχουν επίσης πρόσβαση σε πληροφορίες σχετικά με τα εσωτερικά συστήματα και την ασφάλεια, τις διαδικασίες επαλήθευσης ταυτότητας (ταυτοποίησης) και άλλες σχετικές πληροφορίες.

5.4 Διαδικασίες καταγραφής ελέγχου

5.4.1 Τύποι συμβάντων που καταγράφονται

Η ADACOM διασφαλίζει ότι όλες οι σχετικές πληροφορίες που αφορούν τη λειτουργία των Υπηρεσιών Εμπιστοσύνης καταγράφονται για την παροχή αποδεικτικών στοιχείων για τον σκοπό νομικών διαδικασιών. Οι εν λόγω πληροφορίες περιλαμβάνουν την τήρηση αρχείων που απαιτείται για την απόδειξη της εγκυρότητας της λειτουργίας της Υπηρεσίας Εμπιστοσύνης.

Η ADACOM καταγράφει είτε αυτόματα είτε όχι (χειροκίνητα) τα ακόλουθα σημαντικά περιστατικά:

- Συμβάντα διαχείρισης του πιστοποιητικού της ΑΠ και του κύκλου ζωής κλειδιού της, συμπεριλαμβανομένων των εξής:

- της παραγωγής, δημιουργίας εφεδρικών αντιγράφων, αποθήκευσης, ανάκτησης, αρχειοθέτησης, και καταστροφής κλειδιών,
- των αλλαγών σε στοιχεία ή κλειδιά της ΑΠ,
- των συμβάντων διαχείρισης του κύκλου ζωής κρυπτογραφικής διάταξης.

- Συμβάντα διαχείρισης πιστοποιητικών Συνδρομητών και του κύκλου ζωής των κλειδιών τους, συμπεριλαμβανομένων των εξής:
  - των Αιτήσεων για Πιστοποιητικό, της ανανέωσης, της επαναδημιουργίας κλειδιού και της ανάκλησης,
  - δημιουργία κλειδιών, εφεδρικού αντιγράφου ασφαλείας, αποθήκευση, ανάκτηση, αρχειοθέτηση και καταστροφή
  - της επιτυχούς ή μη επιτυχούς επεξεργασίας αιτημάτων,
  - των αλλαγών στις πολιτικές δημιουργίας πιστοποιητικών,
  - της παραγωγής και έκδοσης Πιστοποιητικών και ΚΑΠ.
- Συμβάντα σχετικά με Έμπιστους Υπάλληλους, συμπεριλαμβανομένων των εξής:
  - των προσπαθειών σύνδεσης και αποσύνδεσης,
  - των προσπαθειών δημιουργίας, αφαίρεσης, ορισμού κωδικών πρόσβασης ή της αλλαγής των δικαιωμάτων συστήματος οποιουδήποτε προνομιούχου χρήστη,
  - των αλλαγών στο προσωπικό.
- Όλα τα σημαντικά συμβάντα που σχετίζονται με την ασφάλεια, συμπεριλαμβανομένων των εξής:
  - των επιτυχών και μη επιτυχών προσπαθειών πρόσβασης στο σύστημα της ΥΔΚ,
  - της έναρξης και του τερματισμού των συστημάτων και των εφαρμογών,
  - της κατοχής δεδομένων ενεργοποίησης για τις λειτουργίες του ιδιωτικού κλειδιού της ΑΠ,
  - των αλλαγών διαμόρφωσης και της συντήρησης του συστήματος,
  - των ενεργειών του συστήματος ασφαλείας και της ΥΔΚ οι οποίες εκτελούνται από το προσωπικό της ADACOM,
  - της ανάγνωσης, της εγγραφής ή διαγραφής ευαίσθητων από άποψη ασφάλειας φακέλων ή αρχείων,
  - των αλλαγών των ρυθμίσεων της πολιτικής ασφάλειας,
  - των σφαλμάτων του συστήματος, της αποτυχίας υλικού και άλλων ανωμαλιών,
  - της δραστηριότητας του τείχους προστασίας και του δρομολογητή,
  - της εισόδου/εξόδου επισκεπτών στις εγκαταστάσεις της ΑΠ.
  - Έλεγχος εισόδου/εξόδου εγκαταστάσεων εξ αποστάσεως ΕΔΔΥ

Οι καταχωρίσεις των αρχείων καταγραφής περιλαμβάνουν τα ακόλουθα στοιχεία:

- την ημερομηνία και την ώρα της καταχώρισης
- τον σειριακό ή αύξοντα αριθμό καταχώρισης, για αυτόματες καταχωρίσεις,
- τα στοιχεία ταυτότητας του προσώπου που κάνει την καταχώριση,
- το είδος καταχώρισης.

Η ΑΕ και η ΤΑΕ της ADACOM καταγράφει τα στοιχεία των Αιτήσεων για Πιστοποιητικό, συμπεριλαμβανομένων των εξής:

- του είδους του(των) εγγράφου(ων) ταυτοποίησης που προσκομίζεται(ονται) από τον Αιτούντα Πιστοποιητικό·
- της καταγραφής των αποκλειστικών αναγνωριστικών δεδομένων, των αριθμών ή του συνδυασμού των συγκεκριμένων εγγράφων ταυτοποίησης (π.χ. του αριθμού του δελτίου ταυτότητας του Αιτούντος Πιστοποιητικό), εφόσον ισχύει· της τοποθεσίας αποθήκευσης των αντιγράφων των αιτήσεων και των εγγράφων ταυτοποίησης για τα Εγκεκριμένα Πιστοποιητικά ·
- οποιωνδήποτε συγκεκριμένων επιλογών στην Αίτηση για Πιστοποιητικό·
- της ταυτότητας της οντότητας που αποδέχεται την αίτηση και, στην περίπτωση των εγκεκριμένων ηλεκτρονικών σφραγίδων , της ταυτότητας του φυσικού προσώπου που

εκπροσωπεί το νομικό πρόσωπο στο οποίο παρέχεται το Εγκεκριμένο Πιστοποιητικό ηλεκτρονικών σφραγίδων ·
- της μεθόδου που εφαρμόστηκε για την επικύρωση των εγγράφων ταυτοποίησης, εφόσον υπάρχει·
- του ονόματος της λαμβάνουσας ΑΠ ή της υποβάλλουσας ΑΕ και ΤΑΕ, εφόσον ισχύει.

5.4.2 Συχνότητα επεξεργασίας των αρχείων καταγραφής

Το σύστημα της ADACOM παρακολουθούνται συνεχώς παρέχοντας σε πραγματικό χρόνο ειδοποιήσεις για σημαντικά συμβάντα ασφάλειας και λειτουργίας για τους σκοπούς του ελέγχου μέσω εξουσιοδοτημένου προσωπικού υπεύθυνου για την ασφάλεια του συστήματος. Οι μηνιαίες ανασκοπήσεις των αρχείων καταγραφής περιλαμβάνουν την επαλήθευση ότι δεν έχει σημειωθεί παραποίηση των αρχείων καταγραφής και διενεργείται ενδελεχής έλεγχος για τυχόν προειδοποιήσεις ή παρατυπίες στα αρχεία καταγραφής. Οι ενέργειες που λαμβάνονται βάσει των ανασκοπήσεων των αρχείων καταγραφής ελέγχου επίσης τεκμηριώνονται.

5.4.3 Περίοδος διατήρησης αρχείου καταγραφής ελέγχων

Τα αρχεία καταγραφής ελέγχων τηρούνται τουλάχιστον για δύο (2) μήνες μετά την επεξεργασία και, στη συνέχεια, αρχειοθετούνται σύμφωνα με την ενότητα 5.5.

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 ADACOM φυλάσσονται και είναι προσβάσιμα έως την ανωτέρω αναφερόμενη περίοδο διατήρησης σύμφωνα με την ενότητα 5.8.

5.4.4 Προστασία του αρχείου καταγραφής ελέγχου

Τα αρχεία καταγραφής ελέγχων προστατεύονται από ένα ηλεκτρονικό σύστημα αρχείων καταγραφής ελέγχου το οποίο περιλαμβάνει μηχανισμούς προστασίας των αρχείων καταγραφής από τη μη-εξουσιοδοτημένη προβολή, τροποποίηση, διαγραφή ή άλλη παραποίηση.

5.4.5 Διαδικασίες εφεδρικών αντιγράφων των αρχείων καταγραφής ελέγχων

Επαυξητικοί τύποι αντιγράφων ασφαλείας (incremental backups) των αρχείων καταγραφής ελέγχων δημιουργούνται καθημερινά ενώ πλήρη αντίγραφα ασφαλείας παράγονται σε εβδομαδιαία βάση.

5.4.6 Σύστημα συλλογής αρχείων ελέγχου (Εσωτερικό - Εξωτερικό)

Αυτοματοποιημένα δεδομένα ελέγχου παράγονται και καταγράφονται σε επίπεδο εφαρμογής, δικτύου και λειτουργικού συστήματος. Τα μη αυτοματοποιημένα δεδομένα ελέγχου καταγράφονται από το προσωπικό της ADACOM οι οποίοι κατέχουν Ρόλους Εμπιστοσύνης.

5.4.7 Κοινοποίηση στο υποκείμενο που προκάλεσε το συμβάν

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 τη 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 Αξιολογήσεις ευπάθειας

Τα συμβάντα καταγράφονται, εν μέρει, στη διαδικασία ελέγχου για την παρακολούθηση των ευπαθειών του συστήματος. Οι εκτιμήσεις ευπάθειας εκτελούνται και αναθεωρούνται ετησίως για τον εντοπισμό και την εκτίμηση ευλόγως προβλέψιμων εσωτερικών και εξωτερικών απειλών που θα μπορούσαν να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση, αποκάλυψη, κατάχρηση, τροποποίηση ή καταστροφή οποιωνδήποτε δεδομένων των πιστοποιητικών ή της διαδικασίας έκδοσης των πιστοποιητικών. Η ADACOM αξιολογεί επίσης τακτικά την επάρκεια των πολιτικών, διαδικασιών, πληροφοριακών συστημάτων, τεχνολογιών και άλλων διαδικασιών που έχει τεθεί για τον έλεγχο τέτοιων κινδύνων. Η αξιολόγηση ευπάθειας και η εκτίμηση κινδύνου αποτελούν μέρος του ετήσιου ελέγχου συμμόρφωσης της ADACOM.

5.5 Τήρηση αρχείων

5.5.1 Είδη τηρούμενων αρχείων

Η ADACOM τηρεί αρχεία για:

- όλα τα δεδομένα ελέγχου που συλλέγονται σύμφωνα με την ενότητα 5.4,
- τις πληροφορίες σχετικά με τις αιτήσεις για πιστοποιητικά,
- την υποστηρικτική τεκμηρίωση για τις αιτήσεις πιστοποιητικών,
- τις πληροφορίες σχετικά με τον κύκλο ζωής των πιστοποιητικών,

5.5.2 Περίοδος διατήρησης αρχείων

Η περίοδος διατήρησης των αρχείων περιγράφεται στην ενότητα 5.4.3.

5.5.3 Προστασία του Αρχείου

Η ADACOM προστατεύει τα αρχεία έτσι ώστε μόνο τα εξουσιοδοτημένα Έμπιστα Πρόσωπα έχουν τη δυνατότητα απόκτησης πρόσβασης στο Αρχείο. Το Αρχείο προστατεύεται έναντι της μη εξουσιοδοτημένης προβολής, τροποποίησης, διαγραφής ή άλλης παραποίησης μέσω της αποθήκευσης σε ένα αξιόπιστο σύστημα. Τα μέσα που φυλάσσουν τα δεδομένα του Αρχείου και των εφαρμογών που απαιτούνται για την επεξεργασία των δεδομένων του Αρχείου διατηρούνται προκειμένου να διασφαλιστεί η δυνατότητα προσπέλασής τους, για το χρονικό διάστημα που προσδιορίζεται στην παρούσα ΠΠ/ΔΠΠ.

5.5.4 Διαδικασίες εφεδρικών αντιγράφων του Αρχείου

Σε καθημερινή βάση, η ADACOM δημιουργεί επαυξητικούς τύπους αντιγράφων ασφαλείας (incremental backups) για τα ηλεκτρονικά αρχεία και, σε εβδομαδιαία βάση, δημιουργεί πλήρη αντίγραφα ασφαλείας. Διατηρούνται ηλεκτρονικά αντίγραφα των έντυπων αρχείων σε ασφαλή εγκατάσταση της ADACOM εκτός των κύριων εγκαταστάσεών της.

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 Σύστημα συλλογής αρχείων (Εσωτερικό ή Εξωτερικό)

Η ADACOM χρησιμοποιεί ένα εσωτερικό σύστημα συλλογής αρχείων.

5.5.7 Διαδικασίες για την πρόσβαση και την επαλήθευση πληροφοριών αρχείου

Μόνο το εξουσιοδοτημένο Έμπιστο Προσωπικό έχει τη δυνατότητα απόκτησης πρόσβασης στο Αρχείο. Η ακεραιότητα των πληροφοριών εξακριβώνεται όταν αποκαθίσταται.

Εάν τα αρχεία αφορούν τη 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 νόμιμο δικαίωμα πρόσβασης.

5.6 Αντικατάσταση κλειδιών

Τα ζεύγη κλειδιών ΑΠ της ADACOM αποσύρονται με το πέρας του αντίστοιχου ανώτατου χρόνου ζωής τους όπως ορίζεται στην παρούσα ΠΠ/ΔΠΠ. Τα Πιστοποιητικά ΑΠ της ADACOM δύνανται να ανανεωθούν εφόσον ο αθροιστικός πιστοποιημένος χρόνος ζωής του ζεύγους κλειδιών μιας ΑΠ δεν υπερβαίνει τον ανώτατο χρόνο ζωής αυτού του ζεύγους κλειδιών. Νέα ζεύγη κλειδιών της ΑΠ παράγονται ανάλογα με τις ανάγκες, για παράδειγμα για την αντικατάσταση ζεύγους κλειδιών ΑΠ τα οποία αποσύρονται, ώστε να συμπληρωθούν τα υφιστάμενα, ενεργά ζεύγη κλειδιών και να υποστηριχτούν νέες υπηρεσίες.

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(-α) νέο(-α) ζεύγος(-η) κλειδιών. Η διαδικασία αντικατάστασης κλειδιών της ΑΠ της ADACOM 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(τις) συγκεκριμένη(-ες) μορφή(-ές) 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 Έκθεση σε κίνδυνο και αποκατάσταση καταστροφής

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 ΠΠ/ΔΠΠ.

5.7.2 Φθορά υπολογιστικών πόρων, λογισμικού και/ή δεδομένων

Σε περίπτωση φθοράς των υπολογιστικών πόρων, του λογισμικού και/ή των δεδομένων, τα σχετικά περιστατικά αναφέρονται στο τμήμα Ασφάλειας της ADACOM και εφαρμόζονται οι διαδικασίες διαχείρισης περιστατικών ασφάλειας της ADACOM. Οι διαδικασίες αυτές απαιτούν την κατάλληλη κλιμάκωση, διερεύνηση και απόκριση στο περιστατικό. Εφόσον κριθεί απαραίτητο, θα τεθούν σε εφαρμογή οι διαδικασίες της ADACOM για την έκθεση του κλειδιού σε κίνδυνο ή την αποκατάσταση καταστροφής.

5.7.3 Διαδικασίες σχετικά με την έκθεση ιδιωτικού κλειδιού οντότητας σε κίνδυνο

Κατά την υποπτευόμενη ή πραγματική Έκθεση σε Κίνδυνο του ιδιωτικού κλειδιού ΑΠ της ADACOM, υπηρεσιών υποδομής ή Πελάτη ΑΠ, η ADACOM ακολουθεί το σχέδιο ενεργειών που περιγράφονται στη διαδικασία Διαχείρισης Περιστατικών Ασφαλείας.

Εφόσον απαιτείται ανάκληση του Πιστοποιητικού της ΑΠ, εκτελούνται οι ακόλουθες διαδικασίες:

- η κατάσταση ανάκλησης του Πιστοποιητικού κοινοποιείται στα Βασιζόμενα Μέρη μέσω του Χώρου Αποθήκευσης της ADACOM σύμφωνα με την ενότητα 4.9.9·
- θα καταβληθεί κάθε εύλογη από εμπορικής άποψης προσπάθεια προκειμένου να παρασχεθεί πρόσθετη ενημέρωση σχετικά με την ανάκληση προς όλους τους επηρεαζόμενους Συμμετέχοντες και
- η ΑΠ θα παραγάγει ένα νέο ζεύγος κλειδιών σύμφωνα με την ενότητα 5.6, εκτός της περίπτωσης που η λειτουργία της ΑΠ τερματίζεται σύμφωνα με την ενότητα 5.8.

Η παράγραφος αυτή ισχύει επίσης σε περίπτωση που αλγόριθμοι ΥΔΚ και σχετικοί παράμετροι γίνουν ανεπαρκείς για την υπολειπόμενη αποσκοπούμενη χρήση.

5.7.4 Δυνατότητες επιχειρησιακής συνέχειας έπειτα από καταστροφή

Η ADACOM διατηρεί ένα Σχέδιο Επιχειρησιακής Συνέχειας (ΣΕΣ) προκειμένου να καθορίσει τις διαδικασίες αποκατάστασης των κρίσιμων επιχειρηματικών λειτουργιών της έπειτα από μια καταστροφή.

Οι ακόλουθοι στόχοι έχουν οριστεί για το συγκεκριμένο σχέδιο:

- Μεγιστοποίηση της αποτελεσματικότητας των λειτουργιών εκτάκτου ανάγκης μέσω ενός καταρτισμένου σχεδίου το οποίο απαρτίζεται από τις ακόλουθες φάσεις:
    - Η φάση ειδοποίησης/ενεργοποίησης η οποία εντοπίζει και αξιολογεί τη ζημιά και ενεργοποιεί το σχέδιο.
    - Η φάση αποκατάστασης η οποία αποκαθιστά τις προσωρινές λειτουργίες των πληροφοριακών συστημάτων και αποκαθιστά τη ζημιά που έχει υποστεί το αρχικό σύστημα.

- Προσδιορισμός των δραστηριοτήτων, των πόρων και των διαδικασιών που είναι απαραίτητες για τη διενέργεια των λειτουργιών των Πιστοποιητικών και της ΑΠ της ADACOM κατά τη διάρκεια παρατεταμένων διακοπών των συνήθων λειτουργιών.
- Ανάθεση αρμοδιοτήτων στο εξουσιοδοτημένο προσωπικό της ADACOM και καθοδήγηση όσον αφορά τις διαδικασίες αποκατάστασης της ADACOM κατά τη διάρκεια παρατεταμένων περιόδων διακοπών των συνήθων λειτουργιών.
- Εξασφάλιση του συντονισμού με άλλο προσωπικό της ADACOM το οποίο θα συμμετάσχει στις στρατηγικές σχεδιασμού έκτακτης ανάγκης. Εξασφάλιση του συντονισμού με εξωτερικά σημεία επικοινωνίας και προμηθευτές που θα συμμετάσχουν στις στρατηγικές σχεδιασμού έκτακτης ανάγκης.

Η ADACOM έχει τη δυνατότητα επαναφοράς ή αποκατάστασης των βασικών λειτουργιών της εντός είκοσι τεσσάρων (24) ωρών μετά την επέλευση της καταστροφής παρέχοντας τουλάχιστον υποστήριξη για τις ακόλουθες υπηρεσίες:
- έκδοση πιστοποιητικού,
- ανάκληση πιστοποιητικών,
- δημοσίευση πληροφοριών ανάκλησης.

Η ADACOM διατηρεί πρόσθετο υλικό και εφεδρικά αντίγραφα της ΑΠ και του λογισμικού συστημάτων υποδομής στην Εγκατάσταση Αποκατάστασης έπειτα από καταστροφή. Επιπλέον, δημιουργούνται αντίγραφα ασφαλείας για τα ιδιωτικά κλειδιά της ΑΠ και φυλάσσονται για τους σκοπούς της αποκατάστασης έπειτα από καταστροφή σύμφωνα με την ενότητα 6.2.4.

5.8 Διακοπή λειτουργίας ΑΠ ή ΑΕ

Διακόπτεται η λειτουργία της ΑΠ με τα ακόλουθα:
- απόφαση του Διοικητικού Συμβουλίου της ADACOM,
- απόφαση της αρχής η οποία εποπτεύει την παροχή της υπηρεσίας,
- δικαστική απόφαση,
- εκκαθάριση ή διακοπή των λειτουργιών της ADACOM.

Η ADACOM διασφαλίζει ότι ελαχιστοποιούνται οι πιθανές διαταραχές στους Συνδρομητές και τα Βασιζόμενα Μέρη λόγω της διακοπής των υπηρεσιών της ADACOM 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 μιας ΑΠ της ADACOM, η ADACOM καταβάλλει εύλογες από εμπορικής άποψης προσπάθειες ώστε να ειδοποιήσει τους Συνδρομητές, τα Βασιζόμενα Μέρη και άλλες οντότητες που επηρεάζονται από τη σχετική διακοπή πριν από τη διακοπή λειτουργίας της ΑΠ. Στην περίπτωση που η διακοπή λειτουργίας μίας ΑΠ κριθεί απαραίτητη, κατά περίπτωση, η ADACOM θα μεταβιβάσει τις υποχρεώσεις της σε άλλο ΠΥΕ και θα θέσει σε εφαρμογή το τεκμηριωμένο «Σχέδιο Διακοπής Εργασιών της ADACOM», ώστε να ελαχιστοποιήσει την αναστάτωση των Πελατών, των Συνδρομητών και των Βασιζόμενων Μερών. Το σχέδιο αυτό, προβλέπει, ανάλογα με την περίπτωση, τα ακόλουθα:
- την ειδοποίηση των μερών που επηρεάζονται από τη διακοπή λειτουργίας, όπως είναι οι Συνδρομητές, τα Βασιζόμενα Μέρη και οι Πελάτες, ενημερώνοντάς τους για την κατάσταση της ΑΠ,
- την αντιμετώπιση του κόστους της σχετικής ειδοποίησης,
- την ανάκληση του Πιστοποιητικού που εκδόθηκε στην ΑΠ από την ADACOM,
- τη διατήρηση των αρχείων και των εγγράφων της ΑΠ για τα χρονικά διαστήματα που απαιτούνται από την παρούσα ΠΠ/ΔΠΠ,
- τη συνεχή παροχή των υπηρεσιών υποστήριξης Συνδρομητή και του Πελατών,
- 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 τελικών χρηστών και των υφιστάμενων ΑΠ τα οποία δεν έχουν λήξει ή ανακληθεί, εφόσον είναι απαραίτητο,
- την επιστροφή χρημάτων (εφόσον κριθεί απαραίτητη) προς τους Συνδρομητές των οποίων τα Πιστοποιητικά δεν έχουν λήξει ή ανακληθεί, αλλά ανακλήθηκαν στα πλαίσια της διακοπής λειτουργίας ή εναλλακτικά την αντικατάσταση των Πιστοποιητικών εκδίδοντας νέα από διάδοχη ΑΠ,
- τη διάθεση 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 των αρμόδιων αρχών, όπως οι εποπτικοί φορείς,
- τη μεταφορά των υποχρεώσεων σε αξιόπιστο μέρος όσον αφορά τη διατήρηση όλων των πληροφοριών που είναι απαραίτητες για την απόδειξη της λειτουργίας των Υπηρεσιών Εμπιστοσύνης για ένα εύλογο χρονικό διάστημα, εκτός και εάν μπορεί να καταδειχθεί ότι η ADACOM δεν έχει στην κατοχή της τις σχετικές πληροφορίες,
- την υποβολή του αρχείου και των εγγράφων της ΑΠ της ADACOM σε άλλον συμβατικό Πάροχο Υπηρεσιών Πιστοποίησης όσον αφορά τα Εγκεκριμένα Πιστοποιητικά για τα χρονικά διαστήματα που απαιτούνται βάσει νομοθεσίας.

Με την παύση εργασιών της ADACOM ή παύση των υπηρεσιών της ΑΕ, για οποιοδήποτε λόγο, οι συμβάσεις ανάθεσης μέρους των αρμοδιοτήτων του ΠΥΕ σε τρίτα μέρη, λ.χ. εκχώρηση των αρμοδιοτήτων ταυτοποίησης σε Αρχή Εγγραφής, λήγουν αυτοδικαίως. Για το σκοπό αυτό, τα τρίτα μέρη θα πρέπει να διασφαλίζουν την παράδοση του αρχείου και των εγγράφων που σχετίζονται με τις εκχωρηθείσες αρμοδιότητες, σύμφωνα με την ισχύουσα νομοθεσία.

6. ΤΕΧΝΙΚΟΙ ΕΛΕΓΧΟΙ ΑΣΦΑΛΕΙΑΣ

6.1 Παραγωγή και εγκατάσταση ζεύγους κλειδιών

6.1.1 Παραγωγή ζεύγους κλειδιών

Η παραγωγή ζεύγους κλειδιών της ΑΠ διενεργείται από πολλαπλά, προεπιλεγμένα, εκπαιδευμένα και έμπιστα πρόσωπα, χρησιμοποιώντας αξιόπιστα συστήματα και διαδικασίες οι οποίες εγγυώνται την ασφάλεια και την απαραίτητη κρυπτογραφική ισχύ για τα παραγόμενα κλειδιά. Οι κρυπτογραφικές μονάδες που χρησιμοποιούνται για την παραγωγή κλειδιών πληρούν τις προδιαγραφές του επιπέδου 3 του FIPS 140-2.

Όλα τα ζεύγη κλειδιών της ΑΠ παράγονται σε προκαθορισμένες Διαδικασίες Παραγωγής Κλειδιών (Key Ceremonies) σύμφωνα με τις απαιτήσεις των εγγράφων του «Οδηγού Αναφοράς Διαδικασίας Παραγωγής Κλειδιών» (Key Ceremony Reference Guide και του «Οδηγού Χρήσης του Εργαλείου Διαχείρισης Κλειδιών της ΑΠ» (CA Key Management Tool User's Guide). Οι ενέργειες που πραγματοποιούνται σε κάθε διαδικασία παραγωγής κλειδιών καταγράφονται, αρχειοθετούνται και υπογράφονται από όλα τα εμπλεκόμενα πρόσωπα. Τα αρχεία αυτά τηρούνται για τους σκοπούς του ελέγχου και της ανίχνευσης για το χρονικό διάστημα που έχει κριθεί ως απαραίτητο από τη Διοίκηση της ADACOM.

Η παραγωγή ζεύγους κλειδιών Συνδρομητή τελικού χρήστη διενεργείται εν γένει από τον Συνδρομητή. Ο Συνδρομητής χρησιμοποιεί μια πιστοποιημένη κρυπτογραφική μονάδα ΕΔΔΥ η οποία συμμορφώνεται με τις απαιτήσεις του κανονισμού eIDAS.

Η παραγωγή, αποθήκευση και περαιτέρω χρήση των κλειδιών των εξ αποστάσεως Εγκεκριμένων Ψηφιακών Πιστοποιητικών γίνεται από την ADACOM χρησιμοποιώντας αποκλειστικά συσκευές πιστοποιημένες σύμφωνα με τις απαιτήσεις του άρθρου 30.3 του Κανονισμού 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 στον συνδρομητή

Όταν τα ζεύγη κλειδιών Συνδρομητή παράγονται σε ΕΔΔΥ από τον Συνδρομητή, δεν ισχύει η παράδοση ιδιωτικού κλειδιού στον Συνδρομητή.

Όταν τα ζεύγη κλειδιών παράγονται εκ των προτέρων από την ADACOM σε ΕΔΔΥ, η εν λόγω διάταξη παραδίδεται στον Συνδρομητή χρησιμοποιώντας την εμπορική υπηρεσία παράδοσης συστημένης επιστολής. Τα δεδομένα που απαιτούνται για την ενεργοποίηση της διάταξης κοινοποιούνται στον Συνδρομητή χρησιμοποιώντας μια εκτός ζώνης διαδικασία. Η διανομή των εν λόγω διατάξεων παρακολουθείται από την ADACOM.

Όταν τα ζεύγη κλειδιών παράγονται σε τοπική ΕΔΔΥ από τον Συνδρομητή, δεν ισχύει η παράδοση ιδιωτικού κλειδιού στον Συνδρομητή.
Όταν τα ζεύγη κλειδιών παράγονται σε εξ αποστάσεως ΕΔΔΥ από τον Συνδρομητή, η παράδοση ιδιωτικού κλειδιού στον Συνδρομητή πραγματοποιείται εντός της εξ αποστάσεως ΕΔΔΥ.

6.1.3 Παράδοση δημόσιου κλειδιού στον εκδότη του πιστοποιητικού

Οι Συνδρομητές υποβάλλουν ηλεκτρονικά το δημόσιο κλειδί τους στην ADACOM για πιστοποίηση με τη χρήση του Αιτήματος Υπογραφής Πιστοποιητικού (ΑΥΠ), κατά το πρότυπο PKCS # 10 ή

άλλη ηλεκτρονικά υπογεγραμμένη μορφή, σε ασφαλή σύνδεση μέσω SSL (Secure Socket Layer - Επιπέδου Ασφαλών Συνδέσεων). Όταν τα ζεύγη κλειδιών του Συνδρομητή παράγονται εκ των προτέρων από την ADACOM δεν εφαρμόζεται η εν λόγω απαίτηση.

6.1.4 Παράδοση δημόσιου κλειδιού της ΑΠ σε βασιζόμενα μέρη

Η ADACOM καθιστά διαθέσιμα τα Πιστοποιητικά ΑΠ Βάσης και Εκδότριας ΑΠ στους Συνδρομητές και τα Βασιζόμενα Μέρη μέσω του χώρου αποθήκευσής της.

Σε γενικές γραμμές, η ADACOM παρέχει την πλήρη αλυσίδα πιστοποιητικών της (συμπεριλαμβανομένων των εκδοτριών ΑΠ και οποιασδήποτε ΑΠ στην αλυσίδα) στον Συνδρομητή με την έκδοση του Πιστοποιητικού.

Οι Συνδρομητές, κατά τη διαδικασία λήψης του πιστοποιητικού, πραγματοποιούν αυτόματα τη λήψη και εγκαθιστούν στον υπολογιστή τους, τα δημόσια κλειδιά των ενδιάμεσων και εκδοτριών ΑΠ. Σε κάθε περίπτωση, εφόσον ένας χρήστης επιθυμεί να επαληθεύσει και/ή να πραγματοποιήσει τη λήψη του δημόσιου κλειδιού της ΑΠ, αυτό μπορεί να το κάνει προσπελάζοντας τον διαδικτυακό χώρο αποθήκευσης της ADACOM (https://pki.adacom.com/repository).

6.1.5 Μέγεθος κλειδιού

Τα ζεύγη κλειδιών θα 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 ADACOM όσον αφορά το ελάχιστο μέγεθος κλειδιών είναι η χρήση ενός ζεύγους κλειδιών ισχύος τουλάχιστον με 2048 bit RSA για τα πιστοποιητικά των ΑΠ και του Συνδρομητή.

Τα ζεύγη κλειδιών δημιουργούνται χρησιμοποιώντας ασφαλείς αλγορίθμους και παραμέτρους που βασίζονται σε ισχύοντα ερευνητικά και βιομηχανικά πρότυπα ακολουθώντας τις προτάσεις του ETSI TS 119 312 για την υπογραφή Πιστοποιητικών, ΚΑΠ και αποκρίσεων διακομιστή κατάστασης πιστοποιητικού.

6.1.6 Δημιουργία παραμέτρων και έλεγχος ποιότητας δημόσιων κλειδιών

Η ποιότητα των δημόσιων κλειδιών διασφαλίζεται με τη χρήση ασφαλούς δημιουργίας τυχαίων αριθμών και την on-board δημιουργία δημοσίων κλειδιών. Τα ζεύγη κλειδιών δημιουργούνται χρησιμοποιώντας ασφαλείς αλγόριθμους και παραμέτρους που βασίζονται σε τρέχοντα ερευνητικά και βιομηχανικά πρότυπα σύμφωνα με τις συστάσεις του προτύπου ETSI TS 119 312.

6.1.7 Σκοποί χρήσης κλειδιών (σύμφωνα με το πεδίο χρήσης κλειδιών X.509 v3)

Ανατρέξτε στην ενότητα 7.

6.2 Προστασία ιδιωτικού κλειδιού και μηχανικοί έλεγχοι κρυπτογραφικής μονάδας

Η ADACOM εφαρμόζει συνδυασμό φυσικών, λογικών, και διαδικαστικών μέτρων τα οποία εγγυώνται την ασφάλεια των ιδιωτικών κλειδιών των ΑΠ της. Επίσης, οι Συνδρομητές πρέπει να

λαμβάνουν τα μέτρα προφύλαξης ώστε να αποτρέψουν την απώλεια, την αποκάλυψη, την τροποποίηση, ή τη μη εξουσιοδοτημένη χρήση ιδιωτικών κλειδιών.

6.2.1 Πρότυπα και έλεγχοι για τις κρυπτογραφικές μονάδες

Για την παραγωγή ζεύγους κλειδιών της ΑΠ και την αποθήκευση ιδιωτικών κλειδιών της ΑΠ, η ADACOM χρησιμοποιεί κρυπτογραφικές μονάδες υλικού οι οποίες είναι πιστοποιημένες ή πληρούν τις προδιαγραφές του επιπέδου 3 του FIPS 140-2.

Τα ιδιωτικά κλειδιά του Συνδρομητή παράγονται σε ΕΔΔΥ που συμμορφώνεται με τις απαιτήσεις του κανονισμού eIDAS.

Η ADACOM 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 ADACOM θα παύσει να εκδίδει πιστοποιητικά σε αυτές τις συσκευές.

6.2.2 Έλεγχος του ιδιωτικού κλειδιού από πολλαπλά πρόσωπα (m από n)

Η ADACOM εφαρμόζει τεχνικούς και διαδικαστικούς μηχανισμούς οι οποίοι απαιτούν τη συμμετοχή πολλαπλών έμπιστων προσώπων για την εκτέλεση ευαίσθητων κρυπτογραφικών εφαρμογών της ΑΠ. Η ADACOM εφαρμόζει την πολιτική «Διαμοιρασμού Απορρήτου», διαχωρίζοντας τα δεδομένα ενεργοποίησης που είναι απαραίτητα για τη χρήση ενός ιδιωτικού κλειδιού ΑΠ σε διακριτά μέρη τα οποία καλούνται «Μερίδια Απορρήτου» και τα οποία βρίσκονται στην κατοχή εκπαιδευμένων και έμπιστων προσώπων που ονομάζονται «Κάτοχοι Μεριδίων». Απαιτείται ένας κατώτατος οριακός αριθμός Μεριδίων Απορρήτου (m) εκ του συνολικού αριθμού των Μεριδίων Απορρήτου που δημιουργήθηκαν και διανεμήθηκαν για μια συγκεκριμένη κρυπτογραφική μονάδα υλικού (n) ώστε να ενεργοποιηθεί το ιδιωτικό κλειδί της ΑΠ που είναι αποθηκευμένο στη μονάδα.

Ο κατώτατος αριθμός των Μεριδίων που απαιτούνται για να υπογραφεί ένα Πιστοποιητικό ΑΠ 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 ΠΠ/ΔΠΠ.

Κανένας έλεγχος πολλαπλών προσώπων δεν εφαρμόζεται στα ιδιωτικά κλειδιά του Συνδρομητή.

6.2.3 Παρακαταθήκη ιδιωτικού κλειδιού

Τα ιδιωτικά κλειδιά της ΑΠ της ADACOM και των Συνδρομητών δεν αρχειοθετούνται.

6.2.4 Δημιουργία αντίγραφου ασφαλείας ιδιωτικού κλειδιού

Η ADACOM δημιουργεί αντίγραφα ασφαλείας για τα ιδιωτικά κλειδιά της ΑΠ και τα ιδιωτικά κλειδιά των Συνδρομητών που δημιουργούνται και αποθηκεύονται από μία εξ αποστάσεως ΕΔΔΥ, για τους σκοπούς της τακτικής ανάκτησης και της αποκατάστασης από καταστροφή. Τα κλειδιά αυτά αποθηκεύονται σε κρυπτογραφημένη μορφή σε κρυπτογραφικές μονάδες υλικού και σε συσκευές που συνδέονται με την αποθήκευση κλειδιών. Οι κρυπτογραφικές μονάδες που χρησιμοποιούνται για την αποθήκευση των ιδιωτικών κλειδιών συμμορφώνονται με τις απαιτήσεις της παρούσας ΠΠ/ΔΠΠ. Τα ιδιωτικά κλειδιά αντιγράφονται σε εφεδρικές κρυπτογραφικές μονάδες υλικού σύμφωνα με την παρούσα ΠΠ/ΔΠΠ.

Οι μονάδες που περιέχουν τα αντίγραφα ασφαλείας των ιδιωτικών κλειδιών ΑΠ εντός του κύριου χώρου εγκαταστάσεων υπόκεινται στις προδιαγραφές της παρούσας ΠΠ/ΔΠΠ. Οι μονάδες που περιέχουν τα αντίγραφα ασφαλείας των ιδιωτικών κλειδιών ΑΠ όσον αφορά την αποκατάσταση από καταστροφή υπόκεινται στις προδιαγραφές της παρούσας ΠΠ/ΔΠΠ.

Σε περίπτωση τοπικής ΕΔΔΥ τα ιδιωτικά κλειδιά του Συνδρομητή 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 ενός Πιστοποιητικού της ΑΠ της ADACOM, τα ζεύγη κλειδιών που συνδέονται με το πιστοποιητικό, διατηρούνται για χρονικό διάστημα τουλάχιστον 5 ετών με ασφαλή τρόπο χρησιμοποιώντας κρυπτογραφικές μονάδες υλικού οι οποίες πληρούν τις απαιτήσεις της παρούσας ΠΠ/ΔΠΠ. Τα συγκεκριμένα ζεύγη κλειδιών της ΑΠ δεν χρησιμοποιούνται για την υπογραφή κανενός συμβάντος μετά την ημερομηνία λήξης του αντίστοιχου Πιστοποιητικού ΑΠ, εκτός και εάν το σχετικό Πιστοποιητικό ΑΠ έχει ανανεωθεί σύμφωνα με του όρους της παρούσας ΠΠ/ΔΠΠ.

Τα ιδιωτικά κλειδιά του Συνδρομητή δεν μπορούν να εξαχθούν ή να αποκατασταθούν από την ΕΔΔΥ και δεν αρχειοθετούνται.

6.2.6 Μεταφορά ιδιωτικού κλειδιού προς/από την κρυπτογραφική μονάδα

Η ADACOM δημιουργεί ζεύγη κλειδιών της ΑΠ για τις κρυπτογραφικές μονάδες υλικού στις οποίες θα χρησιμοποιηθούν τα κλειδιά. Επίσης, η ADACOM δημιουργεί αντίγραφα των σχετικών ζευγών κλειδιών για τους σκοπούς της τακτικής αποκατάστασης και αποκατάστασης από καταστροφή. Όταν για τα ζεύγη κλειδιών των ΑΠ δημιουργούνται αντίγραφα ασφάλειας σε άλλες κρυπτογραφικές μονάδες υλικού, η μεταφορά τους μεταξύ των μονάδων πραγματοποιείται σε κρυπτογραφημένη μορφή.

Η ADACOM δημιουργεί ζεύγη κλειδιών Συνδρομητή στις κρυπτογραφικές μονάδες υλικού στις οποίες θα χρησιμοποιηθούν τα κλειδιά. η ADACOM δημιουργεί αντίγραφα των σχετικών ζευγών κλειδιών για σκοπούς υψηλής διαθεσιμότητας και αποκατάστασης από καταστροφή. 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

Όλοι οι Συνδρομητές της ADACOM είναι απαραίτητο να προστατεύουν τα δεδομένα ενεργοποίησης των ιδιωτικών τους κλειδιών έναντι απώλειας, κλοπής, τροποποίησης, μη εξουσιοδοτημένης γνωστοποίησης ή χρήσης.

Η παραγωγή των δεδομένων ενεργοποίησης περιγράφεται στην ενότητα 6.4.1

Τα ιδιωτικά κλειδιά των Συνδρομητών που δημιουργούνται και αποθηκεύονται σε τοπική ΕΔΔΥ, προστατεύονται από κωδικούς PIN. Ισχύουν οι ακόλουθοι κανόνες:

- Ο Συνδρομητής πρέπει να εισαγάγει τον κωδικό PIN στην ΕΔΔΥ για κάθε συναλλαγή.
- Ο Συνδρομητής υποχρεούται να αλλάξει τον κωδικό PIN και PUK πριν από την αρχική διαδικασία της εγγραφής.
- Σε περίπτωση που ο Συνδρομητής εισαγάγει λανθασμένα των κωδικό PIN 5 φορές συνεχόμενα, η ΕΔΔΥ μπλοκάρει.
- Το PIN μπορεί να ξεμπλοκάρει χρησιμοποιώντας των κωδικό PIN του διαχειριστή (admin).
- Η χρήση του κωδικού PIN του διαχειριστή θα μπλοκάρει μετά τις 3 συνεχόμενες λανθασμένες προσπάθειες.
- Ο χρήστης μπορεί να αλλάξει τους κωδικούς PIN και PUK.

Τα ιδιωτικά κλειδιά των Συνδρομητών που δημιουργούνται και αποθηκεύονται σε εξ αποστάσεως ΕΔΔΥ, προστατεύονται από κωδικό χρήστη, κωδικό πρόσβασης και κωδικό μιας χρήσης. Ισχύουν οι ακόλουθοι κανόνες:

- Ο Συνδρομητής πρέπει να εισαγάγει τον κωδικό χρήστη, κωδικό πρόσβασης, και κωδικό μιας χρήσης προκειμένου να αποκτήσει πρόσβαση στην εξ αποστάσεως ΕΔΔΥ για κάθε συναλλαγή.
- Σε περίπτωση που ο Συνδρομητής εισαγάγει λανθασμένα τον κωδικό χρήστη, κωδικό πρόσβασης, και κωδικό μιας χρήσης 5 φορές συνεχόμενα, η εξ αποστάσεως ΕΔΔΥ μπλοκάρει.
- Ο κωδικός πρόσβασης της εξ αποστάσεως ΕΔΔΥ δεν μπορεί να ανακτηθεί
- Ο Συνδρομητής μπορεί να αλλάξει τον κωδικό πρόσβασης

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 της ΑΠ της ADACOM απενεργοποιούνται με τη διακοπή της τροφοδοσίας της κρυπτογραφικής μονάδας.

Τα ιδιωτικά κλειδιά Συνδρομητών μπορούν να απενεργοποιηθούν μετά από κάθε λειτουργία, αποσυνδέοντας το σύστημά τους ή αφαιρώντας την τοπική ΕΔΔΥ από τον σταθμό εργασίας, ή κατά την αποσύνδεση από την εξ αποστάσεως ΕΔΔΥ. Σε κάθε περίπτωση, οι Συνδρομητές έχουν υποχρέωση να προστατεύουν επαρκώς το(τα) ιδιωτικό(-ά) κλειδί(-ιά) τους σύμφωνα με την παρούσα ΠΠ/ΔΠΠ.

6.2.10 Μέθοδος καταστροφής ιδιωτικού κλειδιού

Όταν απαιτείται, η ADACOM 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 ADACOM 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 φυσική καταστροφή ή πρόκληση φθοράς της ΕΔΔΥ.

6.2.11 Αξιολόγηση κρυπτογραφικής μονάδας

Ανατρέξτε στην ενότητα 6.2.1.

6.3 Άλλα θέματα διαχείρισης του ζεύγους κλειδιών

6.3.1 Αρχειοθέτηση δημόσιου κλειδιού

Για τα Πιστοποιητικά της ΑΠ, της ΑΕ και των Συνδρομητών της ADACOM δημιουργούνται αντίγραφα ασφαλείας τα οποία αρχειοθετούνται ως μέρος της τακτικής διαδικασίας δημιουργίας αντιγράφων της ADACOM.

Όλα τα δημόσια κλειδιά των Συνδρομητών φυλάσσονται στη βάση δεδομένων της ADACOM και μπορούν να αρχειοθετηθούν για τουλάχιστον επτά (7) ημέρες μετά τη λήξη της ΑΠ που έχει εκδώσει τα πιστοποιητικά.

6.3.2 Λειτουργικές περίοδοι πιστοποιητικών και περίοδος χρήσης ζεύγους κλειδιών

Η Λειτουργική Περίοδος ενός Πιστοποιητικού ολοκληρώνεται με τη λήξη ή την ανάκλησή του. Η Λειτουργική Περίοδος για ζεύγη κλειδιών είναι ίδια με τη Λειτουργική Περίοδο των συσχετιζόμενων Πιστοποιητικών, εκτός από το ότι τα ιδιωτικά κλειδιά μπορούν να συνεχίσουν να χρησιμοποιούνται για επαλήθευση υπογραφής. Οι μέγιστες Λειτουργικές Περίοδοι των Πιστοποιητικών της ADACOM για Πιστοποιητικά που εκδίδονται κατά ή μετά την ημερομηνία έναρξης ισχύος της παρούσας ΠΠ/ΔΠΠ παρατίθενται στον ακόλουθο Πίνακα.

Πιστοποιητικό που εκδόθηκε από:	***Χρήση Ιδιωτικού Κλειδιού***	***Περίοδος ισχύος***
ΑΠ βάσης	Δεν προβλέπεται	Συνήθως έως και 20 έτη
Εκδότρια ΑΠ	Δεν προβλέπεται	Συνήθως έως και 10 έτη
Πιστοποιητικά Μακράς Διάρκειας	Δεν προβλέπεται	Συνήθως 1-3 έτη
Πιστοποιητικά Σύντομης Διάρκειας	Δεν προβλέπεται	Συνήθως 24 - 72 ώρες

Επιπρόσθετα, οι ΑΠ της ADACOM παύουν να εκδίδουν νέα Πιστοποιητικά στην ανάλογη ημερομηνία (επιπλέον μέγιστη περίοδο ισχύος 60 ημερών των εκδοθέντων Πιστοποιητικών) πριν από τη λήξη του Πιστοποιητικού των ΑΠ, έτσι ώστε κανένα Πιστοποιητικό το οποίο εκδίδεται από ιεραρχικά Υφιστάμενη ΑΠ να μη λήγει μετά τη λήξη οποιουδήποτε Πιστοποιητικού της ιεραρχικά Ανώτερης ΑΠ. Η διάρκεια ζωής των πιστοποιητικών των Συνδρομητών δεν θα υπερβαίνει τη διάρκεια ζωής του πιστοποιητικού υπογραφής της ΑΠ.

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 τη διοίκηση της ADACOM.

6.4 Δεδομένα ενεργοποίησης

6.4.1 Παραγωγή και εγκατάσταση δεδομένων ενεργοποίησης

Τα δεδομένα ενεργοποίησης (Μερίδια Απορρήτου) που χρησιμοποιούνται για την προστασία των ΚΜΥ που περιέχουν τα ιδιωτικά κλειδιά των ΑΠ της ADACOM παράγονται σύμφωνα με τις απαιτήσεις της ενότητας 6.2.2 και του «Οδηγού Αναφοράς Διαδικασίας Παραγωγής Κλειδιών (Key Ceremony Reference Guide)». Η δημιουργία και η διανομή των σχετικών Μεριδίων Απορρήτου καταγράφεται.

Τα δεδομένα ενεργοποίησης που χρησιμοποιούνται (PIN) για την προστασία των τοπικών ΕΔΔΥ που περιέχουν τα ιδιωτικά κλειδιά του Υποκειμένου, παράγονται σύμφωνα με το εγχειρίδιο της ΕΔΔΥ.

- Όπου τα ζεύγη κλειδιών του Συνδρομητή παράγονται εκ των προτέρων από την ADACOM, τα δεδομένα ενεργοποίησης παραδίδονται στον Συνδρομητή χρησιμοποιώντας την εμπορική υπηρεσία παράδοσης συστημένης επιστολής.
- Όπου τα ζεύγη κλειδιών του Συνδρομητή παράγονται από τον Συνδρομητή, τα προκαθορισμένα δεδομένα ενεργοποίησης πρέπει να αλλάζουν αμέσως πριν από την παραγωγή κλειδιών.

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.
Η ADACOM θα μεταδίδει δεδομένα ενεργοποίησης μόνο μέσω κατάλληλα προστατευμένου καναλιού και σε χρόνο και τόπο που διαφέρει από την παράδοση της σχετικής κρυπτογραφικής μονάδας.

6.4.2 Προστασία δεδομένων ενεργοποίησης

Η ADACOM προστατεύει τα δεδομένα που χρησιμοποιούνται για την απενεργοποίηση ιδιωτικών κλειδιών από την αποκάλυψη χρησιμοποιώντας ένα συνδυασμό μηχανισμών ελέγχου.
Οι Κάτοχοι Μεριδίων της ADACOM πρέπει να διαφυλάσσουν τα προσωπικά τους Μερίδια Απορρήτου και τα Μερίδια Απορρήτου της εξ αποστάσεως ΕΔΔΥ και να υπογράψουν σύμβαση αναγνωρίζοντας τις αρμοδιότητες του Κατόχου Μεριδίων.

Το προσωπικό και οι Συνδρομητές της ADACOM λαμβάνουν οδηγίες να χρησιμοποιούν ισχυρούς κωδικούς πρόσβασης και να προστατεύουν τα PIN και τους κωδικούς πρόσβασης. Οι συνδρομητές πρέπει να απομνημονεύουν τα διαπιστευτήρια ενεργοποίησης (PIN, PUK, όνομα χρήστη, κωδικό πρόσβασης, OTP) και να μην τα αποκαλύπτουν σε κανέναν.

Η ADACOM εφαρμόζει την επαλήθευση ταυτότητας πολλαπλών παραγόντων (multi-factor authentication) για όλους τους λογαριασμούς που μπορούν να προκαλέσουν την έκδοση πιστοποιητικών ή λειτουργίες Αρχής Εγγραφής ή λειτουργίες εξουσιοδοτημένου τρίτου μέρους ή την εφαρμογή τεχνικών ελέγχων που εκτελούνται από την ΑΠ για περιορισμό της έκδοσης πιστοποιητικών μέσω του λογαριασμού σε περιορισμένο αριθμό προεγκεκριμένων τομέων ή διευθύνσεων ηλεκτρονικού ταχυδρομείου.

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 ADACOM καταστρέφει τα δεδομένα ενεργοποίησης αντικαθιστώντας τα με καινούργια και/ή μέσω της φυσικής καταστροφής τους.

6.5 Έλεγχοι ασφάλειας υπολογιστών

Η ADACOM εκτελεί όλες τις λειτουργίες των ΑΠ και ΑΕ χρησιμοποιώντας αξιόπιστα συστήματα που πληρούν τις απαιτήσεις του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System - ISMS) της ADACOM.

6.5.1 Ειδικές τεχνικές απαιτήσεις για την ασφάλεια των υπολογιστών

Η ADACOM διασφαλίζει ότι τα συστήματα που διατηρούν τα αρχεία δεδομένων και το λογισμικό της ΑΠ είναι αξιόπιστα συστήματα τα οποία είναι ασφαλή από τη μη εξουσιοδοτημένη πρόσβαση. Επιπλέον, η ADACOM περιορίζει την πρόσβαση στους διακομιστές παραγωγής εξουσιοδοτώντας μόνο τα άτομα που έχουν βάσιμο επαγγελματικό λόγο. Οι χρήστες γενικών εφαρμογών δεν διαθέτουν λογαριασμούς στους διακομιστές παραγωγής.

Το δίκτυο παραγωγής της ADACOM διαχωρίζεται λογικά από τα άλλα στοιχεία. Ο διαχωρισμός αυτός επιτρέπει την πρόσβαση στο δίκτυο μόνο μέσω καθορισμένων διαδικασιών εφαρμογών. Η ADACOM χρησιμοποιεί τείχη προστασίας (firewalls) για την προστασία του δικτύου παραγωγής από εσωτερική και εξωτερική διείσδυση, καθώς και για τον περιορισμό της φύσης και της πηγής των δραστηριοτήτων, οι οποίες θα μπορούσαν να προσπελάσουν τα συστήματα παραγωγής.

Όλα τα κρίσιμα στοιχεία λογισμικού εγκαθίστανται και ενημερώνονται μόνο από αξιόπιστες πηγές. Υπάρχουν επίσης και εσωτερικές διαδικασίες για την προστασία της ακεραιότητας των στοιχείων υπηρεσιών πιστοποίησης από ιούς, κακόβουλο και μη εξουσιοδοτημένο λογισμικό.

Επαληθεύεται η ταυτότητα των μελών του προσωπικού της ADACOM πριν από τη χρήση κρίσιμων εφαρμογών που σχετίζονται με τις υπηρεσίες. Δημιουργούνται λογαριασμοί χρηστών για το προσωπικό σε συγκεκριμένους ρόλους που απαιτούν πρόσβαση στο σχετικό σύστημα. Οι άδειες του συστήματος αρχείων, καθώς και άλλες διαθέσιμες δυνατότητες στο μοντέλο ασφάλειας του λειτουργικού συστήματος χρησιμοποιούνται για να αποτραπεί οποιαδήποτε άλλη χρήση. Οι λογαριασμοί χρηστών αφαιρούνται το συντομότερο δυνατό όταν το επιβάλει η αλλαγή των ρόλων. Οι κανόνες που αφορούν την ασφάλεια ελέγχονται ετησίως.

Η ADACOM απαιτεί τη χρήση κωδικών πρόσβασης με ελάχιστο αριθμό χαρακτήρων και συνδυασμό αλφαριθμητικών και ειδικών χαρακτήρων. Η ADACOM απαιτεί οι κωδικοί πρόσβασης να αλλάζουν σε περιοδική βάση.

Η άμεση πρόσβαση σε βάσεις δεδομένων της ADACOM που υποστηρίζουν τις Λειτουργίες της ΑΠ, είναι περιορισμένη σε Έμπιστα Πρόσωπα που έχουν βάσιμο επαγγελματικό λόγο για την πρόσβαση αυτή.

Η διαχείριση των στοιχείων του συστήματος υπηρεσιών πιστοποίησης της ADACOM διενεργείται σύμφωνα με τις καθορισμένες διαδικασίες διαχείρισης αλλαγών. Οι εν λόγω διαδικασίες περιλαμβάνουν τη δοκιμή του συστήματος σε ένα απομονωμένο περιβάλλον δοκιμής και την

απαίτηση ότι η αλλαγή πρέπει να εγκρίνεται από τον Υπεύθυνο Ασφάλειας. Η έγκριση τεκμηριώνεται για περαιτέρω αναφορά.

Όλα τα μέσα που περιέχουν τα δεδομένα και το λογισμικό του περιβάλλοντος παραγωγής, τις πληροφορίες για τον έλεγχο, το αρχείο ή τα αντίγραφα ασφαλείας αποθηκεύονται εντός της ADACOM με τους κατάλληλους ελέγχους λογικής και φυσικής πρόσβασης. Τα μέσα που περιέχουν Ευαίσθητες Πληροφορίες οι οποίες διαγράφονται με ασφάλεια όταν δεν είναι πλέον απαραίτητες.

Οι διαδικασίες διαχείρισης ευπάθειας και αντιμετώπισης συμβάντων τεκμηριώνονται σε εσωτερικό έγγραφο. Το σύστημα παρακολούθησης εντοπίζει και ειδοποιεί για μη αναμενόμενες δραστηριότητες του συστήματος που υποδεικνύουν πιθανή παραβίαση της ασφάλειας, συμπεριλαμβανομένης της εισβολής στο δίκτυο.

Τα έγγραφα και υλικά με Ευαίσθητες Πληροφορίες περνάνε σε καταστροφέα εγγράφων πριν από την απόρριψή τους. Τα μέσα που χρησιμοποιήθηκαν για τη συλλογή ή τη μεταβίβαση ευαίσθητων πληροφοριών καθίστανται μη αναγνώσιμα πριν από την απόρριψή τους.

Οι ΑΕ πρέπει να εξασφαλίζουν ότι τα συστήματα που διατηρούν λογισμικό και αρχεία δεδομένων είναι αξιόπιστα συστήματα, προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και είναι λογικά διαχωρισμένα από άλλα στοιχεία. Οι ΑΕ πρέπει να χρησιμοποιούν τείχη προστασίας για να προστατεύσουν το δίκτυο από εσωτερικές και εξωτερικές εισβολές και να περιορίσουν τη φύση και την πηγή των δραστηριοτήτων που μπορούν να έχουν πρόσβαση στα εν λόγω συστήματα και πληροφορίες.

6.5.2 Αξιολόγηση ασφάλειας υπολογιστών

Καμία διατύπωση.

6.6 Τεχνικοί έλεγχοι κατά τον κύκλο ζωής

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 ADACOM διαθέτει μηχανισμούς και/ή πολιτικές για τον έλεγχο και την παρακολούθηση της διαμόρφωσης των συστημάτων της ΑΠ.

Η ADACOM ακολουθεί τις κατευθυντήριες γραμμές για την ασφάλεια δικτύου της ενότητας 7.8 του ETSI EN 319 401. Η ADACOM ακολουθεί επίσης τις κατευθυντήριες γραμμές για την ασφάλεια «Απαιτήσεις Ασφαλείας Συστήματος Δικτύου και Πιστοποιητικών» του CA/Browser Forum.

Μετά την εγκατάσταση και, έκτοτε, σε περιοδική βάση, η ADACOM επιβεβαιώνει την ακεραιότητα των συστημάτων των ΑΠ της. Μόνο το λογισμικό που χρησιμοποιείται απευθείας για την εκτέλεση των εργασιών, χρησιμοποιείται για το πληροφοριακό σύστημα.

6.6.3 Έλεγχοι ασφάλειας κατά τον κύκλο ζωής του πιστοποιητικού

Οι πολιτικές και τα περιουσιακά στοιχεία της ADACOM 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 ADACOM ελέγχονται τουλάχιστον ετησίως για αλλαγές που παραβιάζουν τις πολιτικές ασφαλείας της ADACOM. Οι αλλαγές που έχουν αντίκτυπο στο επίπεδο της παρεχόμενης ασφάλειας εξετάζονται από τον Υπεύθυνο Ασφαλείας και εγκρίνονται από τη Διοίκηση.

Η ADACOM διαθέτει διαδικασίες για τη διασφάλιση 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 ουδεμίας ενημέρωσης κώδικα ασφαλείας θα τεκμηριώνονται.

Η ADACOM διαχειρίζεται την καταχώριση των πηγών πληροφοριών και ταξινομεί όλες τις πληγές πληροφοριών σύμφωνα με τα αποτελέσματα της τακτικής ανάλυσης για την ασφάλεια σχετικά με την αξιολόγηση κινδύνων.

6.7 Έλεγχοι ασφάλειας δικτύου

Η ADACOM εκτελεί όλες τις λειτουργίες των ΑΠ και ΑΕ της, χρησιμοποιώντας δίκτυα που είναι ασφαλή σύμφωνα με το ISMS της ADACOM για την αποτροπή της μη εξουσιοδοτημένης πρόσβασης και άλλων κακόβουλων ενεργειών. Η ADACOM προστατεύει την κοινοποίηση ευαίσθητων πληροφοριών μέσω της κρυπτογράφησης και των ψηφιακών υπογραφών.

Το επίπεδο ασφαλείας του εσωτερικού δικτύου και των εξωτερικών συνδέσεων παρακολουθείται συνέχεια προκειμένου να αποτραπεί η πρόσβαση σε πρωτόκολλα και υπηρεσίες που δεν απαιτούνται για τη λειτουργία των Υπηρεσιών Εμπιστοσύνης.

Η ADACOM εκτελεί μια αξιολόγηση για την τρωτότητα σε περιοδική βάση σε δημόσιες και ιδιωτικές διευθύνσεις IP για όσο διενεργεί δοκιμές διείσδυσης στα συστήματα πιστοποίησης.

6.8 Χρονοσήμανση

Τα Πιστοποιητικά, οι ΚΑΠ καθώς και οι άλλες καταχωρίσεις ανάκλησης στη βάση δεδομένων περιλαμβάνουν πληροφορίες σχετικά με την ώρα και την ημερομηνία.
Ο χρόνος συστήματος στους υπολογιστές της ADACOM ενημερώνεται χρησιμοποιώντας το πρωτόκολλο χρόνου δικτύου (Network Time Protocol - NTP) για συγχρονισμό των ρολογιών του συστήματος τουλάχιστον μία φορά κάθε μία ώρα.

7. ΠΡΟΦΙΛ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ, ΚΑΠ ΚΑΙ OCSP

7.1 Προφίλ Πιστοποιητικού

Το προφίλ του πιστοποιητικού είναι σύμφωνο με το X.509 έκδοση 3, το IETF RFC 5280 και την παράγραφο 6.6.1 του προτύπου ETSI EN 319 411-1.

7.1.1 Αριθμός Έκδοσης

Όλα τα πιστοποιητικά είναι X.509 έκδοση 3.

7.1.2 Επεκτάσεις Πιστοποιητικού

Κάθε πιστοποιητικό που εκδίδεται περιέχει επεκτάσεις όπως ορίζονται για τα X.509v3 Πιστοποιητικά.

Τα πιστοποιητικά της τεχνικά περιορισμένης Εκδότριας ΑΠ της ADACOM περιέχει επέκταση Extended Key Usage (EKU) η οποία εξειδικεύει όλες τις επεκτεινόμενες χρήσεις κλειδιού για τις οποίες το Πιστοποιητικό της Εκδότριας ΑΠ εξουσιοδοτείται να εκδίδει πιστοποιητικά. Το anyExtendedKeyUsage KeyPurposeId δεν εμφανίζεται στην επέκταση EKU των πιστοποιητικών της ADACOM.

Παρακάτω υπάρχει λίστα των επεκτάσεων που χρησιμοποιούνται από την ADACOM για κάθε τύπο πιστοποιητικού:

7.1.2.1 Για ΑΠ Βάσης

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**None**
Certificate Policies	Cert Policy ID	**1.3.6.1.4.1.15976.1.1**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.adacom.com/cps**
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Enhanced Key Usage	Server Authentication	**1.3.6.1.5.5.7.3.1**
	Client Authentication	**1.3.6.1.5.5.7.3.2**
	Code Signing	**1.3.6.1.5.5.7.3.3**
	Secure Email	**1.3.6.1.5.5.7.3.4**
	Time Stamping	**1.3.6.1.5.5.7.3.8**
	OCSP Signing	**1.3.6.1.5.5.7.3.9**

7.1.2.2 Για Εκδότριες ΑΠ για ηλεκτρονικές υπογραφές

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the*

		issuer's Certificate.
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**0**
Certificate Policies	Cert Policy ID	**1.3.6.1.4.1.15976.1.1.1**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.adacom.com/cps**
	Cert Policy ID	**0.4.0.194112.1.0**
	Cert Policy ID	**0.4.0.194112.1.2**
	Cert Policy ID	**0.4.0.2042.1.1**
	Cert Policy ID	**0.4.0.2042.1.2**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl.adacom.com/ca/qroot.crl**
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://repo.adacom.com/certs/root-qglobal.crt**
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Enhanced Key Usage	Secure Email	**1.3.6.1.5.5.7.3.4**
	Client Authentication	**1.3.6.1.5.5.7.3.2**
Subject Alternative Name	Directory Address	*This field contains the Key identification*

7.1.2.3 Για Εκδότριες ΑΠ για ηλεκτρονικές σφραγίδες

Κανονική Επέκταση	***Πεδίο***	***Τιμή***
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**0**
Certificate Policies	Cert Policy ID	**1.3.6.1.4.1.15976.1.1.2**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.adacom.com/cps**
	Cert Policy ID	**0.4.0.194112.1.1**
	Cert Policy ID	**0.4.0.194112.1.3**
	Cert Policy ID	**0.4.0.2042.1.1**
	Cert Policy ID	**0.4.0.2042.1.2**

CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl.adacom.com/ca/qroot.crl**
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://repo.adacom.com/certs/root-qglobal.crt**
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Enhanced Key Usage	Secure Email	**1.3.6.1.5.5.7.3.4**
	Client Authentication	**1.3.6.1.5.5.7.3.2**
Subject Alternative Name	Directory Address	*This field contains the Key identification*

Κανονική Επέκταση	***Πεδίο***	***Τιμή***
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**2.16.840.1.113733.1.7.23.2**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CPS Pointer)
	Cert Qualifier	**https://pki.adacom.com/cps**
	Cert Policy ID	**0.4.0.194112.1.3**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl.adacom.com/ ADACOMSALegalPersoneSeal/LatestCRL.crl**
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD	**0.4.0.1862.1.4 (N/A for advanced eSeals)**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location (en)	**https://pki.adacom.com/repository/PKIPDS-EN.pdf**
	PDS Location (el)	**https://pki.adacom.com/repository/PKIPDS-EL.pdf**
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEseal	**0.4.0.1862.1.6.2**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	**http://ocsp.adacom.com**
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**https://pki.adacom.com/repository/en/certs/production/file s/ca-eseal.crt**

Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Enhanced Key Usage	Client Authentication	**1.3.6.1.5.5.7.3.2**

7.1.2.4 Για ηλεκτρονικές υπογραφές Φυσικού Προσώπου

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.15976.1.1.0.x(version).y(sub-version)**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.adacom.com/cps**
	Cert Policy ID	**1.3.6.1.4.1.15976.1.1.1**
	Cert Policy ID	**0.4.0.194112.1.0** (QCP-n), or **0.4.0.194112.1.2** (QCP-n-qscd)
	Cert Policy ID (N/A for QCP-n)	**1.3.6.1.4.1.15976.1.1.1.3** (Local QSCD), or **1.3.6.1.4.1.15976.1.1.1.4** (Remote QSCD)
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl.adacom.com/ADACOMSAQSignServices/LatestCRL.crl**
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD (N/A for QCP-n)	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location (en)	**https://pki.adacom.com/repository/PKIPDS-EN.pdf**
	PDS Location (el)	**https://pki.adacom.com/repository/PKIPDS-EL.pdf**
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEsign	**0.4.0.1862.1.6.1**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	**http://ocsp.adacom.com**
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://repo.adacom.com/certs/ca-qsign-g1.crt**
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Enhanced Key Usage	Secure Email	**1.3.6.1.5.5.7.3.4**
	Client Authentication	**1.3.6.1.5.5.7.3.2**
Subject Alternative Name	RFC822 Name	*Email address of Subject*

7.1.2.5 Για ηλεκτρονικές υπογραφές Φυσικού Προσώπου που σχετίζεται με Νομικό Πρόσωπο

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.15976.1.1.0.x(version).y(sub-version)**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.adacom.com/cps**
	Cert Policy ID	**1.3.6.1.4.1.15976.1.1.1**
	Cert Policy ID	**0.4.0.194112.1.0** (QCP-n), or **0.4.0.194112.1.2** (QCP-n-qscd)
	Cert Policy ID (N/A for QCP-n)	**1.3.6.1.4.1.15976.1.1.1.3** (Local QSCD), or **1.3.6.1.4.1.15976.1.1.1.4** (Remote QSCD)
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl.adacom.com/ADACOMSAQSignServices/LatestCRL.crl**
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD (N/A for QCP-n)	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location (en)	**https://pki.adacom.com/repository/PKIPDS-EN.pdf**
	PDS Location (el)	**https://pki.adacom.com/repository/PKIPDS-EL.pdf**
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEsign	**0.4.0.1862.1.6.1**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	**http://ocsp.adacom.com**
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://repo.adacom.com/certs/ca-qsign-g1.crt**
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Enhanced Key Usage	Secure Email	**1.3.6.1.5.5.7.3.4**
	Client Authentication	**1.3.6.1.5.5.7.3.2**
Subject Alternative Name	RFC822 Name	*Email address of Subject*

7.1.2.6 Για ηλεκτρονικές σφραγίδες Νομικού Προσώπου

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.15976.1.1.0.x(version).y(sub-version)**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.adacom.com/cps**
	Cert Policy ID	**1.3.6.1.4.1.15976.1.1.2**
	Cert Policy ID	**0.4.0.194112.1.1** (QCP-l), or **0.4.0.194112.1.3** (QCP-l-qscd)
	Cert Policy ID (N/A for QCP-l)	**1.3.6.1.4.1.15976.1.1.2.3** (Local QSCD), or **1.3.6.1.4.1.15976.1.1.2.4** (Remote QSCD)
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl.adacom.com/ADACOMSAQSealServices/LatestCRL.crl**
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD (N/A for QCP-l)	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location (en)	**https://pki.adacom.com/repository/PKIPDS-EN.pdf**
	PDS Location (el)	**https://pki.adacom.com/repository/PKIPDS-EL.pdf**
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEseal	**0.4.0.1862.1.6.2**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	**http://ocsp.adacom.com**
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://repo.adacom.com/certs/ca-qseal-g1.crt**
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Enhanced Key Usage	Client Authentication	**1.3.6.1.5.5.7.3.2**

7.1.2.7 Για ηλεκτρονικές σφραγίδες PSD2

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*

Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.15976.1.1.0.x(version).y(sub-version)**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.adacom.com/cps**
	Cert Policy ID	**1.3.6.1.4.1.15976.1.1.2**
	Cert Policy ID	**0.4.0.194112.1.1** (QCP-l), or **0.4.0.194112.1.3** (QCP-l-qscd)
	Cert Policy ID (N/A for QCP-l)	**1.3.6.1.4.1.15976.1.1.2.3** (Local QSCD), or **1.3.6.1.4.1.15976.1.1.2.4** (Remote QSCD)
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl.adacom.com/ADACOMSAQSealServices/LatestCRL.crl**
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD (N/A for QCP-l)	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location (en)	**https://pki.adacom.com/repository/PKIPDS-EN.pdf**
	PDS Location (el)	**https://pki.adacom.com/repository/PKIPDS-EL.pdf**
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEseal	**0.4.0.1862.1.6.2**
	etsi-psd2-qcStatement	**0.4.0.19495.2**
	id-psd2-role-psp-as	**0.4.0.19495.1.1**
	id-psd2-role-psp-pi	**0.4.0.19495.1.2**
	id-psd2-role-psp-ai	**0.4.0.19495.1.3**
	id-psd2-role-psp-ic	**0.4.0.19495.1.4**
	NCAName	*NCA Long Name (English Language) Registered name*
	NCAId	*NCA Identifier composed of the same values as in the equivalent fields of the authorization number defined in ETSI TS 119 495 clause 5.2.1*
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	**http://ocsp.adacom.com**
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://repo.adacom.com/certs/ca-qseal-g1.crt**
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Enhanced Key Usage	Secure Email	**1.3.6.1.5.5.7.3.4**
	Client Authentication	**1.3.6.1.5.5.7.3.4**

7.1.3 Αναγνωριστικά Αντικειμένου Αλγορίθμου

Οι αλγόριθμοι υπογραφής ακολουθούν τις προδιαγραφές που περιγράφονται στις ενότητες 6.1.5 και 6.1.6. Όλοι οι αλγόριθμοι που χρησιμοποιούνται για τις ΑΠ και τον Συνδρομητή ακολουθούν τα ισχύοντα πρότυπα έρευνας και βιομηχανίας για την παροχή εύλογης ασφάλειας για τους επιδιωκόμενους σκοπούς που χρησιμοποιούνται.

7.1.4 Τύποι Ονομάτων

Κάθε πιστοποιητικό περιέχει έναν μοναδικό αύξοντα αριθμό που δεν επαναχρησιμοποιείται ποτέ. Το περιεχόμενο του πεδίου Issuer Distinguished Name αντιστοιχεί στο Subject DN της Εκδότριας ΑΠ για την υποστήριξη της αλυσιδωτής ονοματοδοσίας όπως ορίζεται στο RFC 5280, ενότητα 4.1.2.4.

7.1.4.1 Για ΑΠ Βάσης και Εκδότριες ΑΠ

Πεδίο	**Τιμή**	
Issuer	*For Root CA it is the same as SubjectDN.* *For Issuing CAs it is the SubjectDN of the Root CA*	
Subject DN	Common Name	*Is used for user-friendly representation of the CA name to represent itself. This name does not need to be exact match of the fully registered organization name*
	Organization	**ADACOM S.A.** (for Root CA) **ADACOM ADVANCED INTERNET APPLICATIONS S.A.** (For Issuing CAs)
	OrganizationIdentifier	***VATEL-099554476***
	Organization Unit	*For Root CA it is "**ADACOM Trust Services**"* *For Issuing CAs it is "**ADACOM Qualified Trust Services**"*
	Country	**GR**
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**4096**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.4.2 Για ηλεκτρονικές υπογραφές Φυσικού Προσώπου

Πεδίο	**Τιμή**	
Issuer	*For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.*	
Subject DN	Common Name	*Space separated Person Given name and Surname.*
	givenName	*Person given name in UTF8 format according to RFC5280*
	sureName	*Person surename in UTF8 format according to RFC5280*
	serialNumber	*Tax Identification Number with the following semantics: "**TIN**GR-123456789"*
		*Social Security Number with the following semantics: "**PNO**GR-12345678"*

		*Personal Identification Card with the following semantics: "**IDC**GR-AK1234567"*
		*Passport Number with the following semantics: "**PAS**GR-1231232"*
		Random code as specified in clause 5.1.3 of ETSI EN 319 412-1
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.4.3 Για ηλεκτρονικές υπογραφές Φυσικού Προσώπου που συνδέεται με Νομικό Πρόσωπο

Πεδίο	Τιμή	
Issuer	*For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.*	
Subject DN	Common Name	*Space separated Person Given name and Surname.*
	givenName	*Person given name in UTF8 format according to RFC5280*
	sureName	*Person surename in UTF8 format according to RFC5280*
	serialNumber	*Tax Identification Number with the following semantics: "**TIN**GR-123456789"*
		*Social Security Number with the following semantics: "**PNO**GR-12345678"*
		*Personal Identification Card with the following semantics: "**IDC**GR-AK1234567"*
		*Passport Number with the following semantics: "**PAS**GR-1231232"*
		Random code as specified in clause 5.1.3 of ETSI EN 319 412-1
	Organization	*Issuer organization name who made subscriber identification.*
	Organizational Unit	*Issuer organization unit name (optional)*
	OrganizationIdentifier	*Legal Entity's Identification Number from a national trade register with the following semantics: "**NTR**GR-123456789".* *Legal Entity's Tax Identification Number with the following semantics: "**VAT**GR-123456789"*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.4.4 Για ηλεκτρονικές σφραγίδες Νομικού Προσώπου

Πεδίο	Τιμή	
Issuer	*For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.*	
	Common Name	*Legal Person's name*
Subject DN	Organization	*Issuer organization name who made subscriber identification.*
	Organizational Unit	*Issuer organization unit name (optional)*
	OrganizationIdentifier	*Legal Entity's Identification Number from a national trade register with the following semantics: "**NTR**GR-123456789".*
		*Legal Entity's Tax Identification Number with the following semantics: "**VAT**GR-123456789"*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.4.5 Για ηλεκτρονικές σφραγίδες PSD2

Πεδίο	Τιμή	
Issuer	*For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.*	
Subject DN	Common Name	*Legal Person's name*
	Organization	*Issuer organization name who made subscriber identification.*
	Organizational Unit	*Issuer organization unit name (optional)*
	OrganizationIdentifier	*PSD2 Authorization Number issued by the NCA encoded as defined in ETSI TS 119 495 clause 5.2.1*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.5 Περιορισμοί Ονομάτων

Η ADACOM μπορεί να συμπεριλάβει περιορισμού ονομάτων στο πεδίο nameConstraints όταν αυτό κριθεί κατάλληλο.
Εάν μια Εκδότρια ΑΠ συμπεριλάβει την επεκτεινόμενη χρήση κλειδιού "id-kp-emailProtection" θα θεωρείται ως τεχνικά περιορισμένη και θα ελέγχεται όπως περιγράφεται στην ενότητα 8.

7.1.6 Αναγνωριστικά Αντικειμένου Πολιτικής Πιστοποιητικού

Σύμφωνα με τον κάθε τύπο πιστοποιητικού, τα παρακάτω αναγνωρισμένα OIDs μπορούν να προστεθούν στην επέκταση certificatePolicies:

- **QCP-n**: 0.4.0.194112.1.0 όπως περιγράφεται στο ETSI EN 319 411-2
- **QCP-l**: 0.4.0.194112.1.1 όπως περιγράφεται στο ETSI EN 319 411-2
- **QCP-n-qscd**: 0.4.0.194112.1.2 όπως περιγράφεται στο ETSI EN 319 411-2
- **QCP-l-qscd**: 0.4.0.194112.1.3 όπως περιγράφεται στο ETSI EN 319 411-2
- **NCP**: 0.4.0.2042.1.1 όπως περιγράφεται στο ETSI EN 319 411-1
- **NCP+:** 0.4.0.2042.1.2 όπως περιγράφεται στο ETSI EN 319 411-1

Η ADACOM προσθέτει επίσης τα παρακάτω OIDs στην επέκταση των Πολιτικών Πιστοποιητικού (Certificate Policies extension) για να προσδιορίζει πότε το ιδιωτικό κλειδί ενός εγκεκριμένου πιστοποιητικού δημιουργείται σε Τοπική ΕΔΔΥ, της οποίας τη διαχείριση για τη δημιουργία του ιδιωτικού αυτού κλειδιού την έχει ο Συνδρομητής/Υποκείμενο, και πότε το ιδιωτικό κλειδί ενός εγκεκριμένου πιστοποιητικού δημιουργείται σε Εξ αποστάσεως ΕΔΔΥ, της οποίας τη διαχείριση για τη δημιουργία του ιδιωτικού αυτού κλειδιού την έχει ο ΕΠΥΕ για λογαριασμό του Συνδρομητή.

- Εγκεκριμένες ηλεκτρονικές υπογραφές:
  - **1.3.6.1.4.1.15976.1.1.1.3.** Το ιδιωτικό κλειδί βρίσκεται σε τοπική ΕΔΔΥ.
  - **1.3.6.1.4.1.15976.1.1.1.4.** Το ιδιωτικό κλειδί βρίσκεται σε Εξ αποστάσεως ΕΔΔΥ.
- Εγκεκριμένες ηλεκτρονικές σφραγίδες:
  - **1.3.6.1.4.1.15976.1.1.2.3.** Το ιδιωτικό κλειδί βρίσκεται σε τοπική ΕΔΔΥ.
  - **1.3.6.1.4.1.15976.1.1.2.4.** Το ιδιωτικό κλειδί βρίσκεται σε Εξ αποστάσεως ΕΔΔΥ

7.1.7 Χρήση Επέκτασης των Περιορισμών Πολιτικής

Δεν εφαρμόζεται.

7.1.1 Σύνταξη και σημασιολογία Προδιαγραφών Πολιτικής

Ο προσδιοριστής πολιτικής είναι η URL που παραπέμπει στη δημοσιευμένη ΠΠ/ΔΠΠ της ADACOM.

7.1.2 Επεξεργασία Σημασιολογίας για την Επέκταση των Κρίσιμων Πολιτικών Πιστοποιητικού

Δεν προβλέπεται.

7.2 Προφίλ ΚΑΠ (CRL)

Το προφίλ του ΚΑΠ είναι σύμφωνο με το X.509 έκδοση 2 και του IETF RFC 5280.

7.2.1 Αριθμός Έκδοσης

Η ADACOM εκδίδει ΚΑΠ version 2 που περιέχουν τα παρακάτω πεδία:

Πεδίο	Τιμή
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer Distinguished Name	ADACOM Issuing CA SubjectDN
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format.

Revoked Certificates List	List of revoked Certificates, including the serial number and revocation date
Signature	The signature algorithm MUST follow the requirements described in sections 6.1.5 and 6.1.6

7.2.2 Επεκτάσεις ΚΑΠ και Καταχωρίσεων ΚΑΠ

Οι ΚΑΠ έχουν τις παρακάτω επεκτάσεις:

Πεδίο	Τιμή
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the Certificate
Invalidity Date	Optional date in UTC format
Reason Code	Optional reason for revocation

7.3 Προφίλ OCSP

7.3.1 Αριθμός Έκδοσης

Οι αποκριτές OCSP της ADACOM συμμορφώνονται με την έκδοση 1 του RFC 6960.

7.3.2 Επεκτάσεις OCSP

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.15976.1.1.1** (for Signatures), or **1.3.6.1.4.1.15976.1.1.2** (for Seals)
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.adacom.com/cps**
Key Usage	Digital Signature	**Set**
OCSP No Revocation Checking	ocsp-nocheck	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://repo.adacom.com/certs/ca-qsign-g1.crt,** or **http://repo.adacom.com/certs/ca-qseal-g1.crt**
Enhanced Key Usage	OCSP Signing	**Set**
Subject Key Identifier	RFC822 Name	*This field contains the ID of the Certificate Holder's key.*

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**2.16.840.1.113733.1.7.23.2**

	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CPS Pointer)
	Cert Qualifier	**https://pki.adacom.com/cps**
	Cert Policy Qualifier ID	1.3.6.1.5.5.7.2.2 (User Notice)
Key Usage	Digital Signature	**Set**
OCSP No Revocation Checking	ocsp-nocheck	**Set**
Enhanced Key Usage	OCSP Signing	**Set**
Subject Key Identifier	RFC822 Name	*This field contains the ID of the Certificate Holder's key.*

8. ΕΛΕΓΧΟΣ ΣΥΜΜΟΡΦΩΣΗΣ ΚΑΙ ΑΛΛΕΣ ΑΞΙΟΛΟΓΗΣΕΙΣ

Η συμμόρφωση του πληροφοριακού συστήματος, των πολιτικών και των πρακτικών, των εγκαταστάσεων, του προσωπικού και των περιουσιακών στοιχείων της ADACOM αξιολογείται από έναν φορέα αξιολόγησης συμμόρφωσης σύμφωνα με τον κανονισμό eIDAS, την αντίστοιχη νομοθεσία, τις απαιτήσεις του CA/B Forum και πρότυπα ή όποτε συντελείται μια σημαντική αλλαγή στις λειτουργίες της Υπηρεσίας Εμπιστοσύνης, βάσει των προτύπων ETSI που αναφέρονται στην Ενότητα 9.15.

Πέρα από τους ελέγχους συμμόρφωσης, η ADACOM δικαιούται να διενεργεί και άλλες επιθεωρήσεις και έρευνες ώστε να διασφαλίσει την αξιοπιστία των Υπηρεσιών Πιστοποίησης της ADACOM. Η ADACOM δικαιούται να αναθέσει την εκτέλεση των εν λόγω ελέγχων, επιθεωρήσεων και ερευνών σε μια εξωτερική ελεγκτική εταιρεία.

Η ADACOM δικαιούται να διενεργεί δεύτερο κύκλο ελέγχων σε αναδόχους που έχουν συνάψει σχέση με την ADACOM για να λειτουργούν ως Τοπικές Αρχές Εγγραφής (ΤΑΕ).

8.1 Συχνότητα και συνθήκες αξιολόγησης

Οι Έλεγχοι Συμμόρφωσης της ADACOM 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/τυπικά προσόντα του αξιολογητή

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

- τους Εσωτερικούς Ελεγκτές,
- τον οργανισμό αξιολόγησης της συμμόρφωσης ο οποίος έχει διαπιστευθεί σύμφωνα με τον κανονισμό (ΕΚ) αριθ. 765/2008 και τα πρότυπα ETSI (π.χ. ETSI EN 319 403)
- τον Εποπτικό Φορέα.

8.3 Σχέση του αξιολογητή με την υπό αξιολόγηση οντότητα

Ο ελεγκτής του οργανισμού αξιολόγησης της συμμόρφωσης πρέπει να είναι ανεξάρτητος από την ADACOM και από τα συστήματα της ADACOM που αξιολογούνται.

Ο εσωτερικός ελεγκτής δεν ελέγχει τους τομείς της αρμοδιότητάς του.

8.4 Θέματα που καλύπτει η αξιολόγηση

Η αξιολόγηση της συμμόρφωσης καλύπτει τη συμμόρφωση του πληροφοριακού συστήματος, των πολιτικών και των πρακτικών, των εγκαταστάσεων, του προσωπικού και των περιουσιακών στοιχείων της ADACOM με τον κανονισμό eIDAS, την αντίστοιχη νομοθεσία και πρότυπα. Ο οργανισμός αξιολόγησης της συμμόρφωσης ελέγχει τα μέρη του πληροφοριακού συστήματος που χρησιμοποιούνται για την παροχή των Υπηρεσιών Εμπιστοσύνης.

Οι τομείς δραστηριότητας που υπάγονται στον εσωτερικό έλεγχο είναι οι εξής:

- η ποιότητα της υπηρεσίας,
- η ασφάλεια της υπηρεσίας,
- η ασφάλεια των λειτουργιών και των διαδικασιών,
- η προστασία των δεδομένων των Συνδρομητών και η πολιτική ασφάλειας,
- η εκτέλεση των διαδικασιών εργασιών και των συμβατικών υποχρεώσεων, καθώς και η συμμόρφωση με την ΠΠ και τις δηλώσεις πολιτικών και πρακτικών βάσει υπηρεσιών.

Ο Οργανισμός Αξιολόγησης της Συμμόρφωσης και ο Εσωτερικός Ελεγκτής ελέγχουν επίσης τα τμήματα του πληροφοριακού συστήματος, των πολιτικών και των πρακτικών, των εγκαταστάσεων, του προσωπικού και των περιουσιακών στοιχείων των υπεργολάβων που σχετίζονται με την παροχή Υπηρεσιών Εμπιστοσύνης της ADACOM (π.χ. συμπεριλαμβανομένων των ΤΑΕ).

8.5 Ανάληψη ενεργειών λόγω ανεπαρκειών

Όσον αφορά τους ελέγχους συμμόρφωσης των λειτουργιών της ADACOM, σημαντικές εξαιρέσεις ή ανεπάρκειες που έχουν εντοπιστεί κατά τη διενέργεια του Ελέγχου Συμμόρφωσης θα οδηγήσουν στον προσδιορισμό των ενεργειών που πρέπει να ληφθούν. Ο συγκεκριμένος προσδιορισμός πραγματοποιείται από τη διοίκηση της ADACOM με δεδομένα που προέρχονται από τον ελεγκτή. Η διοίκηση της ADACOM είναι υπεύθυνη για την ανάπτυξη και την υλοποίηση ενός σχεδίου λήψης διορθωτικών μέτρων. Σε περίπτωση που η ADACOM προσδιορίσει ότι οι εν λόγω εξαιρέσεις ή ανεπάρκειες απειλούν την ασφάλεια ή την ακεραιότητα των Υπηρεσιών Εμπιστοσύνης, θα αναπτυχθεί ένα σχέδιο ανάληψης διορθωτικών μέτρων εντός 30 ημερών και θα υλοποιηθεί εντός ενός ευλόγου από εμπορικής άποψης χρονικού διαστήματος. Για λιγότερο σημαντικές εξαιρέσεις ή ανεπάρκειες, η διοίκηση της ADACOM θα αξιολογεί τη σπουδαιότητα των σχετικών ζητημάτων και θα καθορίζει την ανάλογη πορεία δράσης.

Επιπλέον, σε περίπτωση που τα αποτελέσματα της αξιολόγησης του Οργανισμού Αξιολόγησης της Συμμόρφωσης καταδείξουν την ύπαρξη ανεπάρκειας, ο Εποπτικός Φορέας απαιτεί από την ADACOM να αποκαταστήσει τη μη τήρηση των απαιτήσεων εντός προθεσμίας (εάν ισχύει) που ορίζει ο Εποπτικός Φορέας. Η ADACOM καταβάλλει προσπάθειες να παραμένει συμμορφούμενη και να εκπληρώνει έγκαιρα όλες τις απαιτήσεις σχετικά με την ανεπάρκεια. Η διοίκηση της ADACOM είναι υπεύθυνη για την υλοποίηση ενός σχεδίου ανάληψης διορθωτικών μέτρων. Η ADACOM 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.

Όταν 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 Κοινοποιήσεις των αποτελεσμάτων

Τα συμπεράσματα των ελέγχων ή 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 eIDAS, την αντίστοιχη νομοθεσία και πρότυπα, δύνανται να δημοσιεύονται στον δικτυακό τόπο της ADACOM στη διεύθυνση: https://pki.adacom.com/repository.

Επιπλέον, η ADACOM υποβάλει τη σχετική έκθεση για την αξιολόγηση της συμμόρφωσης στον Εποπτικό Φορέα εντός τριών (3) εργάσιμων ημερών μετά τη λήψη της. Η ADACOM υποβάλλει τα συμπεράσματα του ελέγχου ή το(τα) πιστοποιητικό(ά) για την(τις) υπηρεσία(ες) εμπιστοσύνης στους υπαλλήλους συντήρησης προγραμμάτων περιήγησης (Root Browser) στα οποία συμμετέχει η ADACOM και άλλα ενδιαφερόμενα μέρη.

Τα αποτελέσματα των εσωτερικών ελέγχων των λειτουργιών της ADACOM δύνανται να δημοσιευτούν κατά τη διακριτική ευχέρεια της διοίκησης της ADACOM.

8.7 Εσωτερικοί Έλεγχοι

Η ADACOM πραγματοποιεί τακτικού εσωτερικούς ελέγχους ώστε να επιβεβαιώνει τη συμμόρφωση κατά την ενότητα 8.4.

9. ΑΛΛΑ ΕΠΙΧΕΙΡΗΣΙΑΚΑ ΚΑΙ ΝΟΜΙΚΑ ΘΕΜΑΤΑ

9.1 Τέλη

9.1.1 Τέλη έκδοσης ή ανανέωσης πιστοποιητικού

Η ADACOM χρεώνει τους Συνδρομητές για την έκδοση, τη διαχείριση και την επαναδημιουργία κλειδιών των Πιστοποιητικών.

9.1.2 Τέλη για την πρόσβαση σε πιστοποιητικό

Η ADACOM δεν χρεώνει τέλη για τη διαθεσιμότητα ενός Πιστοποιητικού σε χώρο αποθήκευσης ή την κατ΄ άλλον τρόπο διαθεσιμότητα των Πιστοποιητικών προς τα Βασιζόμενα Μέρη.

9.1.3 Τέλη για την πρόσβαση σε πληροφορίες ανάκλησης ή κατάστασης

Η ADACOM δεν χρεώνει τέλη ως προϋπόθεση για τις υπηρεσίες OCSP και τη διαθεσιμότητα των ΚΑΠ όπως απαιτείται από την παρούσα ΠΠ/ΔΠΠ σε χώρο αποθήκευσης ή την κατ΄ άλλον τρόπο διαθεσιμότητά τους προς τα Βασιζόμενα Μέρη. Η ADACOM δεν επιτρέπει την πρόσβαση σε πληροφορίες ανάκλησης ή πληροφορίες κατάστασης Πιστοποιητικού στους χώρους αποθήκευσής της σε τρίτους που παρέχουν προϊόντα ή υπηρεσίες που κάνουν χρήση των σχετικών πληροφοριών για την κατάσταση του Πιστοποιητικού χωρίς την πρότερη έγγραφη και ρητή συγκατάθεση της.

9.1.4 Τέλη για άλλες υπηρεσίες

Η ADACOM δεν χρεώνει τέλη για την πρόσβαση στην παρούσα ΠΠ/ΔΠΠ. Οποιαδήποτε χρήση γίνεται για σκοπούς άλλους, πέραν της απλής προβολής των εγγράφων αυτών, όπως είναι η

αναπαραγωγή, η αναδιανομή, η τροποποίηση ή η δημιουργία παράγωγων έργων, υπόκειται σε σύμβαση παραχώρηση σχετικής άδειας χρήσης με την ADACOM.

9.1.5 Πολιτική επιστροφής χρημάτων

9.1.5.1 Πωλήσεις εξ αποστάσεως

Σε περίπτωση που η πώληση του Πιστοποιητικού πραγματοποιηθεί μέσω διαδικτύου ή τηλεφώνου, ο Συνδρομητής έχει το δικαίωμα, σύμφωνα με το άρθρο 4 παράγραφος 10 του νόμου 2251/1994, όπως τροποποιήθηκε, να καταγγείλει τη σύμβαση πώλησης χωρίς να αναφέρει τους λόγους εντός του αποκλειστικού χρονικού ορίου των δεκατεσσάρων (14) ημερών από την ημερομηνία αγοράς. Η άσκηση του εν λόγω δικαιώματος μπορεί να γίνει γραπτώς από τον Συνδρομητή στην ADACOM μέσω της αποστολής μηνύματος ηλεκτρονικού ταχυδρομείου στη διεύθυνση: qc@adacom.com. Ακολούθως, και μετά την κοινοποίηση, η ADACOM υποχρεούται να επιστρέψει τα χρήματα που αντιστοιχούν στην αξία της σύμβασης πώλησης στον Συνδρομητή. Η πληρωμή της επιστροφής χρημάτων πραγματοποιείται με την ίδια μέθοδο όπως εκείνη της αρχικής πληρωμής και ο Συνδρομητής δεν έχει το δικαίωμα να χρησιμοποιήσει το Πιστοποιητικό. Μετά το πέρας της εν λόγω περιόδου, η ισχύς του δικαιώματος καταγγελίας λήγει και η ADACOM δεν έχει περαιτέρω υποχρέωση για τον παραπάνω λόγο.

9.1.5.2 Άλλες περιπτώσεις

Με την επιφύλαξη της ενότητας 9.1.5.1, η ADACOM χειρίζεται ξεχωριστά κάθε περίπτωση επιστροφής χρημάτων.
Για την υποβολή αίτησης επιστροφής χρημάτων, ο Συνδρομητής θα πρέπει αποστείλει μια έγγραφη αίτηση στην ADACOM. Η παρούσα πολιτική επιστροφής χρημάτων δεν αποτελεί αποκλειστικό μέσο ικανοποίησης και δεν περιορίζει άλλα σχετικά μέσα που δύνανται να είναι διαθέσιμα στους συνδρομητές.

9.2 Οικονομική Ευθύνη

9.2.1 Ασφαλιστική κάλυψη

Η ADACOM διατηρεί ένα εμπορικώς εύλογο επίπεδο ασφαλιστικής κάλυψης αστικής ευθύνης έναντι σφαλμάτων και παραλείψεων, μέσω ενός σχετικού προγράμματος ασφάλισης αστικής ευθύνης.
Το πιστοποιητικό του ασφαλιστήριου συμβολαίου είναι διαθέσιμο στον δημόσιο χώρο αποθήκευσης της ADACOM στη διεύθυνση https://pki.adacom.com/repository/en/insurance.

9.2.2 Άλλα περιουσιακά στοιχεία

Η ADACOM διαθέτει επαρκείς οικονομικούς πόρους προκειμένου να διατηρεί τις λειτουργίες της και να εκτελεί τα καθήκοντα της ενώ παράλληλα μπορεί ευλόγως να αντιμετωπίσει τον κίνδυνο ευθύνης απέναντι στους Συνδρομητές και τα Βασιζόμενα Μέρη. Αποδεικτικά στοιχεία των οικονομικών πόρων δεν δημοσιοποιούνται.

9.2.3 Ασφαλιστική ή εγγυητική κάλυψη για τελικούς χρήστες (οντότητες)

Ανατρέξτε στην ενότητα 9.2.1 της παρούσας ΠΠ/ΔΠΠ.

9.3 Εμπιστευτικότητα επιχειρηματικών Πληροφοριών

9.3.1 Πεδίο εφαρμογής εμπιστευτικών πληροφοριών

Όλες οι πληροφορίες που έχουν καταστεί γνωστές κατά την παροχή υπηρεσιών και δεν προορίζονται για δημοσίευση (πχ. πληροφορίες που ήταν γνωστές στην ADACOM λόγω λειτουργίας και παροχής Υπηρεσιών Εμπιστοσύνης) είναι εμπιστευτικές. Ο Συνδρομητής έχει το δικαίωμα να λαμβάνει πληροφορίες από την ADACOM σχετικά με εκείνον σύμφωνα με την ισχύουσα νομοθεσία.

9.3.2 Πληροφορίες που δεν εμπίπτουν στο πεδίο εφαρμογής των εμπιστευτικών πληροφοριών

Οποιαδήποτε πληροφορία που δεν αναφέρεται ως εμπιστευτική ή δεν προβλέπεται για εσωτερική χρήση, συνιστά δημόσια πληροφορία. Οι πληροφορίες που θεωρούνται δημόσιου χαρακτήρα στην ADACOM, αναφέρονται στην ενότητα 2.2. της παρούσας ΠΠ/ΔΠΠ.

Επιπλέον, τα μη εξατομικευμένα στατιστικά στοιχεία για τις υπηρεσίες της ADACOM θεωρούνται επίσης δημόσιες πληροφορίες. Η ADACOM δύναται να δημοσιεύσει μη εξατομικευμένα στατιστικά στοιχεία σχετικά με τις υπηρεσίες της.

9.3.3 Ευθύνη προστασίας εμπιστευτικών πληροφοριών

Η ADACOM προστατεύει τις εμπιστευτικές πληροφορίες καθώς και τις πληροφορίες που προορίζονται για εσωτερική χρήση ώστε να μην εκτίθενται σε κίνδυνο και να μη γνωστοποιούνται σε τρίτα μέρη μέσω της εφαρμογής διαφορετικών ελέγχων ασφαλείας.

Η γνωστοποίηση ή προώθηση εμπιστευτικών πληροφοριών σε τρίτους επιτρέπεται μόνο με τη γραπτή συγκατάθεση του νομικού κατόχου των πληροφοριών βάσει δικαστικής εντολής ή άλλων περιπτώσεων που προβλέπονται από τον νόμο.

9.4 Απόρρητο προσωπικών στοιχείων

9.4.1 Σχέδιο απορρήτου

Η ADACOM εφαρμόζει πολιτική απορρήτου η οποία βρίσκεται στην εξής διεύθυνση: http://pki.adacom.com/repository σε συμμόρφωση με την ισχύουσα νομοθεσία.

9.4.2 Πληροφορίες που αντιμετωπίζονται ως ιδιωτικές

Οποιαδήποτε πληροφορία σχετικά με τους Συνδρομητές δεν είναι δημόσια διαθέσιμη μέσω του περιεχομένου του εκδοθέντος πιστοποιητικού, η υπηρεσία καταλόγου του πιστοποιητικού και οι ΚΑΠ σε σύνδεση (online) αντιμετωπίζονται ως ιδιωτικοί.

9.4.3 Πληροφορίες που δεν θεωρούνται ιδιωτικές

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

9.4.4 Ευθύνη για την προστασία ιδιωτικών πληροφοριών

Η ADACOM διασφαλίζει τις ιδιωτικές πληροφορίες από την έκθεση σε κίνδυνο και τη γνωστοποίηση σε τρίτους και συμμορφώνεται με την ισχύουσα νομοθεσία περί απορρήτου.

9.4.5 Ειδοποίηση και συγκατάθεση για χρήση ιδιωτικών πληροφοριών

Εφόσον δεν ορίζεται διαφορετικά στην παρούσα ΠΠ/ΔΠΠ, η εφαρμόσιμη πολιτική απορρήτου ή, βάσει σύμβασης, οι ιδιωτικές πληροφορίες δεν θα χρησιμοποιούνται χωρίς τη συναίνεση του μέρους στο οποίο εφαρμόζονται οι εν λόγω πληροφορίες, σε συμμόρφωση με την ισχύουσα νομοθεσία περί απορρήτου.

9.4.6 Γνωστοποίηση πληροφοριών σύμφωνα με δικαστική ή διοικητική διαδικασία

Η ADACOM δικαιούται να γνωστοποιεί Εμπιστευτικές Πληροφορίες εάν η ADACOM, καλή τη πίστει, θεωρεί ότι:

- η γνωστοποίηση είναι απαραίτητη αναφορικά με δικαστικές κλητεύσεις και εντάλματα έρευνας,
- η γνωστοποίηση είναι απαραίτητη αναφορικά με δικαστικές, διοικητικές ή άλλες νομικές διαδικασίες κατά τη διερευνητική φάση σε αστικού ή διοικητικού χαρακτήρα αγωγές, όπως κλητεύσεις, ανακρίσεις, αιτήματα παραδοχής και αιτήματα για προσκόμιση τεκμηρίων.

Η παρούσα ενότητα υπόκειται στην εφαρμοστέα νομοθεσία περί απορρήτου.

9.4.7 Γνωστοποίηση κατόπιν αιτήματος κατόχου

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

9.4.8 Λοιπές συνθήκες γνωστοποίησης πληροφοριών

Καμία διατύπωση.

9.5 Δικαιώματα Πνευματικής Ιδιοκτησίας

Η απονομή των Δικαιωμάτων Πνευματικής Ιδιοκτησία ανάμεσα στους Συμμετέχοντες στην ADACOM, εκτός των Συνδρομητών και των Βασιζόμενων Μερών, διέπεται από τις ισχύουσες συμβάσεις μεταξύ των σχετικών Συμμετεχόντων στον Υποτομέα της ADACOM. Οι ακόλουθες υποενότητες αφορούν τα Δικαιώματα Πνευματικής Ιδιοκτησίας σε σχέση με τους Συνδρομητές και τα Βασιζόμενα Μέρη.

9.5.1 Δικαιώματα ιδιοκτησίας επί των πιστοποιητικών και των πληροφοριών ανάκλησης

Οι ΑΠ διατηρούν όλα τα Δικαιώματα Πνευματικής Ιδιοκτησίας σε και επί των Πιστοποιητικών και των πληροφοριών ανάκλησης που εκδίδουν. Η ADACOM χορηγεί την άδεια αναπαραγωγής και διανομής Πιστοποιητικών σε μη αποκλειστική βάση και άνευ υποχρέωσης καταβολής δικαιωμάτων, εφόσον αυτά αναπαράγονται πλήρως και η χρήση τους υπόκειται στους Γενικούς Όρους και Προϋποθέσεις που αναφέρονται στο Πιστοποιητικό. Η ADACOM χορηγεί άδεια για τη χρήση των πληροφοριών ανάκλησης προκειμένου να εκτελέσει τις λειτουργίες των Βασιζόμενων Μερών με την επιφύλαξη των Γενικών Όρων και Προϋποθέσεων ή οποιωνδήποτε άλλων εφαρμοστέων συμβάσεων.

9.5.2 Δικαιώματα ιδιοκτησίας επί της ΠΠ/ΔΠΠ

Οι Συνδρομητές αναγνωρίζουν ότι η ADACOM διατηρεί όλα τα Δικαιώματα Πνευματικής Ιδιοκτησίας σε και επί της παρούσας ΠΠ/ΔΠΠ.

9.5.3 Δικαιώματα ιδιοκτησίας επί των ονομάτων

Ο Αιτών Πιστοποιητικό διατηρεί όλα τα δικαιώματα που κατέχει (εάν υπάρχουν) επί οποιουδήποτε εμπορικού σήματος, σήματος παροχής υπηρεσιών ή εμπορικής επωνυμίας που περιλαμβάνεται σε οποιαδήποτε Αίτηση για Πιστοποιητικό και επί οποιουδήποτε διακριτικού ονόματος εντός οποιουδήποτε Πιστοποιητικού που έχει εκδοθεί για τον εν λόγω Αιτούντα Πιστοποιητικό.

9.5.4 Δικαιώματα ιδιοκτησίας επί των κλειδιών και του υλικού κλειδιών

Τα ζεύγη κλειδιών που αντιστοιχούν σε Πιστοποιητικά των ΑΠ και των Συνδρομητών αποτελούν ιδιοκτησία των ΑΠ και των Συνδρομητών οι οποίοι είναι τα αντίστοιχα Υποκείμενα των Πιστοποιητικών αυτών ανεξάρτητα από το φυσικό μέσο στο οποίο έχουν αποθηκευθεί και προστατεύονται και τα πρόσωπα αυτά διατηρούν όλα τα Δικαιώματα Πνευματικής Ιδιοκτησίας σε και επί των συγκεκριμένων ζευγών κλειδιών. Με την επιφύλαξη της γενικότητας των όσων ορίζονται προηγουμένως, τα δημόσια κλειδιά Βάσης (Root public Keys) της ADACOM και τα Πιστοποιητικά Βάσης (Root Certificates) που τα περιλαμβάνουν, καθώς και όλα τα δημόσια κλειδιά της ΠΑΠ και των αυτοϋπογεγραμμένων Πιστοποιητικών, αποτελούν ιδιοκτησία της ADACOM. Τέλος, τα Μερίδια Απορρήτου του ιδιωτικού κλειδιού μιας ΑΠ αποτελούν ιδιοκτησία της ΑΠ, η οποία διατηρεί όλα τα Δικαιώματα Πνευματικής Ιδιοκτησίας επί αυτών των Μεριδίων Απορρήτου, ακόμη και αν δεν μπορούν να αποκτήσουν φυσική κατοχή των μεριδίων αυτών ή της ΑΠ από την ADACOM.

9.5.5 Παραβίαση δικαιωμάτων Πνευματικής Ιδιοκτησίας

Η ADACOM δεν παραβιάζει εν γνώσει της τα δικαιώματα πνευματικής ιδιοκτησίας οποιουδήποτε τρίτου μέρους.

9.6 Δηλώσεις και Εγγυήσεις

9.6.1 Δηλώσεις και Εγγυήσεις της ΑΠ

Η ΑΠ της ADACOM εγγυάται ότι:

- παρέχει τις υπηρεσίες της σύμφωνα με τις απαιτήσεις και τις διαδικασίες που ορίζονται στην παρούσα ΠΠ/ΔΠΠ και τα σχετικά έγγραφα·
- συμμορφώνεται με τον κανονισμό eIDAS και τις σχετικές νομικές πράξεις που ορίζονται στην παρούσα ΠΠ/ΔΠΠ και τα σχετικά έγγραφα·
- δημοσιεύει την ΠΠ/ΔΠΠ και τα σχετικά έγγραφα και εγγυάται τη διαθεσιμότητά τους σε δημόσιο δίκτυο επικοινωνίας δεδομένων·
- δημοσιεύει και πληροί τις απαιτήσεις της σε ό,τι αφορά τους όρους και τις προϋποθέσεις για τους συνδρομητές και εγγυάται τη διαθεσιμότητα και πρόσβασή τους σε δημόσιο δίκτυο επικοινωνίας δεδομένων·
- διατηρεί την εμπιστευτικότητα των πληροφοριών για τις οποίες έχουν λάβει γνώση κατά τη διάρκεια της παροχής της υπηρεσίας και δεν υπόκεινται σε δημοσίευση·
- τηρεί λογαριασμό των εκδοθέντων από εκείνη Διακριτικών Υπηρεσιών Εμπιστοσύνης και της εγκυρότητάς τους και διασφαλίζει τη δυνατότητα ελέγχου της εγκυρότητας των πιστοποιητικών·

- εγγυάται την πρόσβαση σε ιδιωτικά κλειδιά σε εξ αποστάσεως ΕΔΔΥ, στον εξουσιοδοτημένο Συνδρομητή των κλειδιών·
- Εγγυάται την κατάλληλη διαχείριση και συμμόρφωση της εξ αποστάσεως ΕΔΔΥ·
- ενημερώνει τον Εποπτικό Φορέα για τυχόν αλλαγές σε ένα δημόσιο κλειδί που χρησιμοποιείται για την παροχή των Υπηρεσιών Εμπιστοσύνης·
- χωρίς αδικαιολόγητη καθυστέρηση αλλά, σε κάθε περίπτωση, εντός 24 ωρών αφού έχουν λάβουν γνώση από αυτή, ειδοποιεί τον Εποπτικό Φορέα και, κατά περίπτωση, άλλους σχετικούς φορείς, όπως η εθνική αρχή αντιμετώπισης ηλεκτρονικών επιθέσεων (Εθνικό CERT) ή επιθεώρηση δεδομένων για την απώλεια ασφάλειας ή ακεραιότητας που έχει σημαντικό αντίκτυπο στην παρεχόμενη Υπηρεσία Εμπιστοσύνης ή στα προσωπικά δεδομένα που διατηρούνται σε αυτή·
- όπου 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, ειδοποιεί το φυσικό ή νομικό πρόσωπο για την παραβίαση της ασφάλειας ή την απώλεια της ακεραιότητας χωρίς αδικαιολόγητη καθυστέρηση·
- διατηρεί όλη την τεκμηρίωση, τις εγγραφές και τα αρχεία καταγραφής που σχετίζονται με τις Υπηρεσίες Εμπιστοσύνης σύμφωνα με τις ενότητες 5.4 και 5.5·
- εξασφαλίζει την αξιολόγηση της συμμόρφωσης σύμφωνα με τις απαιτήσεις και προσκομίζει τα συμπεράσματα του οργανισμού αξιολόγησης της συμμόρφωσης στον Εποπτικό Φορέα προκειμένου να διασφαλιστεί η συνεχή κατάσταση των Υπηρεσιών Εμπιστοσύνης στον Κατάλογο Εμπιστοσύνης·
- διαθέτει την απαιτούμενη οικονομική σταθερότητα, καθώς και τους απαιτούμενους οικονομικούς πόρους για να λειτουργεί σύμφωνα με την παρούσα ΠΠ/ΔΠΠ·
- δημοσιεύει τους όρους του υποχρεωτικού ασφαλιστηρίου συμβολαίου και τα συμπεράσματα του οργανισμού αξιολόγησης της συμμόρφωσης σε δημόσιο δίκτυο επικοινωνίας δεδομένων·
- παρέχει πρόσβαση στις υπηρεσίες της για άτομα με ειδικές ανάγκες όπου είναι εφικτό·
- δεν υπάρχει καμία ψευδής δήλωση στοιχείων στο Πιστοποιητικό η οποία να είναι γνωστή ή να οφείλεται σε υπαιτιότητα των οντοτήτων που εγκρίνουν την Αίτηση για Πιστοποιητικό ή που εκδίδουν το Πιστοποιητικό·
- δεν υπάρχουν λάθη στα στοιχεία του Πιστοποιητικού τα οποία εισήχθηκαν από τις οντότητες που ενέκριναν την Αίτηση για Πιστοποιητικό ή που εξέδωσαν το Πιστοποιητικό ως αποτέλεσμα αποτυχίας να επιδείξουν εύλογη μέριμνα κατά τον χειρισμό της Αίτησης για Πιστοποιητικό ή τη δημιουργία του Πιστοποιητικού·
- Οι υπηρεσίες ανάκλησης και η χρήση του χώρου αποθήκευσης είναι σύμφωνες με την ισχύουσα ΠΠ/ΔΠΠ σε κάθε ουσιώδη πτυχή.

Οι Γενικοί Όροι και Προϋποθέσεις Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης της ADACOM δύνανται να περιλαμβάνουν πρόσθετες δηλώσεις και εγγυήσεις.

9.6.2 Δηλώσεις και Εγγυήσεις της ΑΕ

Η ΑΕ της ADACOM εγγυάται ότι:

- δεν υπάρχει καμία ψευδής δήλωση στοιχείων στο Πιστοποιητικό η οποία να είναι γνωστή ή να οφείλεται σε υπαιτιότητα των οντοτήτων που εγκρίνουν την Αίτηση για Πιστοποιητικό ή που εκδίδουν το Πιστοποιητικό·
- δεν υπάρχουν λάθη στα στοιχεία του Πιστοποιητικού τα οποία εισήχθηκαν από τις οντότητες που ενέκριναν την Αίτηση για Πιστοποιητικό ως αποτέλεσμα αποτυχίας να επιδείξουν εύλογη μέριμνα κατά τον χειρισμό της Αίτησης για Πιστοποιητικό·
- τα Πιστοποιητικά τους πληρούν όλες τις ουσιώδεις απαιτήσεις της παρούσας ΠΠ/ΔΠΠ και
- οι υπηρεσίες ανάκλησης (κατά περίπτωση) και η χρήση του χώρου αποθήκευσης είναι σύμφωνες με την ισχύουσα ΠΠ/ΔΠΠ σε κάθε ουσιώδη πτυχή.

Οι Γενικοί Όροι και Προϋποθέσεις Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης της ADACOM δύνανται να περιλαμβάνουν πρόσθετες δηλώσεις και εγγυήσεις.

9.6.3 Δηλώσεις και εγγυήσεις του Συνδρομητή

Οι Συνδρομητές εγγυώνται ότι:

- κάθε Εγκεκριμένη Ηλεκτρονική Υπογραφή ή Εγκεκριμένη Ηλεκτρονική Σφραγίδα που έχει δημιουργηθεί με τη χρήση ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί που αναφέρεται στο Εγκεκριμένο Πιστοποιητικό, είναι η Εγκεκριμένη Ηλεκτρονική Υπογραφή ή Εγκεκριμένη Ηλεκτρονική Σφραγίδα του Συνδρομητή και το Εγκεκριμένο Πιστοποιητικό έχει εγκριθεί και είναι σε ισχύ (δεν έχει λήξει ή ανακληθεί) κατά τον χρόνο που δημιουργείται η Εγκεκριμένη Ηλεκτρονική Υπογραφή ή Ηλεκτρονική Σφραγίδα
- Τα διαπιστευτήρια πρόσβασης (PIN, PUK, κωδικό χρήστη, κωδικό πρόσβασης και κωδικό μιας χρήσης) στο ιδιωτικό τους κλειδί προστατεύονται και ότι κανένα μη εξουσιοδοτημένο άτομο δεν έχει ποτέ πρόσβαση.
- η Εγκεκριμένη Ηλεκτρονική Υπογραφή δημιουργείται μόνο σε ΕΔΔΥ ενώ η Εγκεκριμένη Ηλεκτρονική Σφραγίδα δημιουργείται είτε σε ΕΔΔΥ είτε όχι·
- όλες οι δηλώσεις που πραγματοποιούνται από τον Συνδρομητή ο οποίος τις έχει υποβάλλει στην Αίτηση για Πιστοποιητικό, είναι αληθείς και ο Συνδρομητής είναι ενήμερος για το γεγονός ότι η ADACOM δύναται να αρνηθεί να παράσχει την υπηρεσία εάν ο Συνδρομητής έχει σκόπιμα παρουσιάσει ψευδείς, ανακριβείς ή ελλιπείς πληροφορίες στην αίτηση για την υπηρεσία·
- ο Συνδρομητής τηρεί της απαιτήσεις που προβλέπονται από την ADACOM στην παρούσα ΠΠ/ΔΠΠ και τα σχετικά έγγραφα·
- όλες οι πληροφορίες που παρέχονται από τον Συνδρομητή και περιλαμβάνονται στο Πιστοποιητικό είναι αληθείς και, σε περίπτωση αλλαγής στα δεδομένα που υποβλήθηκαν, ο Συνδρομητής κοινοποιεί τα ορθά δεδομένα σύμφωνα με τους κανόνες που έχουν οριστεί από την παρούσα ΠΠ/ΔΠΠ και τα σχετικά έγγραφα·
- το Πιστοποιητικό που χρησιμοποιείται αποκλειστικά για εξουσιοδοτημένους και νόμιμους σκοπούς, συμβατούς με την παρούσα ΠΠ/ΔΠΠ·
- Ο Συνδρομητής δεν είναι ΑΠ και δεν χρησιμοποιεί το ιδιωτικό κλειδί που αντιστοιχεί σε οποιοδήποτε δημόσιο κλειδί που αναφέρεται στο Πιστοποιητικό, για σκοπούς ψηφιακής υπογραφής οποιουδήποτε Πιστοποιητικού (ή άλλης μορφής πιστοποιημένου δημοσίου κλειδιού) ή ΚΑΠ, όπως μια ΑΠ ή άλλως·
- ο Συνδρομητής ειδοποιεί την ADACOM χωρίς καμία αδικαιολόγητη καθυστέρηση εάν το ιδιωτικό κλειδί του υποκειμένου ή ο έλεγχός του έχει απολεσθεί, κλαπεί και δυνητικά εκτεθεί σε κίνδυνο.

Οι Γενικοί Όροι και Προϋποθέσεις Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης της ADACOM δύνανται να περιλαμβάνουν πρόσθετες δηλώσεις και εγγυήσεις.

9.6.4 Δηλώσεις και εγγυήσεις βασιζόμενου μέρους

Οι Γενικοί Όροι και Προϋποθέσεις της ADACOM για τη χρήση των Εγκεκριμένων Πιστοποιητικών απαιτούν τα Βασιζόμενα Μέρη να αναγνωρίσουν ότι διαθέτουν επαρκείς πληροφορίες προκειμένου να λάβουν μια τεκμηριωμένη απόφαση ως προς τον βαθμό στον οποίο επιθυμούν να βασίζονται όσον αφορά τις πληροφορίες σε ένα Πιστοποιητικό, ότι μόνο αυτά είναι αρμόδια να αποφασίσουν κατά πόσο πρόκειται να βασιστούν ή όχι στις εν λόγω πληροφορίες και ότι αναλαμβάνουν τις νομικές συνέπειες της μη τήρησης των υποχρεώσεών τους ως Βασιζόμενα Μέρη σύμφωνα με της παρούσα ΠΠ/ΔΠΠ.

Οι Γενικοί Όροι και Προϋποθέσεις Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης της ADACOM δύνανται να περιλαμβάνουν πρόσθετες δηλώσεις και εγγυήσεις των Βασιζόμενων Μερών.

9.6.5 Δηλώσεις και εγγυήσεις άλλων συμμετεχόντων

Καμία διατύπωση.

9.7 Δηλώσεις αποποίησης ευθύνης εγγυήσεων

Στον βαθμό που επιτρέπεται από την ισχύουσα νομοθεσία, οι Γενικοί Όροι και Προϋποθέσεις για Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης, η ADACOM αποποιείται πιθανές εγγυήσεις, συμπεριλαμβανομένης οποιασδήποτε εγγύησης ως προς την εμπορευσιμότητα ή την καταλληλότητα για έναν συγκεκριμένο σκοπό.

ADACOM δεν φέρει ευθύνη για τα εξής:

- το απόρρητο των διαπιστευτηρίων πρόσβασης (PIN, PUK, κωδικός χρήστη, κωδικός πρόσβασης και κωδικό μιας χρήσης) στα ιδιωτικά κλειδιά των Συνδρομητών, την πιθανή εσφαλμένη χρήση των πιστοποιητικών ή των ανεπαρκών ελέγχων των πιστοποιητικών ή για τις εσφαλμένες αποφάσεις ενός Βασιζόμενου Μέρους ή οποιαδήποτε συνέπεια λόγω σφαλμάτων ή παραλείψεων στους ελέγχους ταυτοποίησης της Υπηρεσίας Εμπιστοσύνης·
- τη μη τήρηση των υποχρεώσεών της, εάν η εν λόγω μη τήρηση οφείλεται σε σφάλματα ή προβλήματα ασφαλείας του Εποπτικού Φορέα, τον Κατάλογο Εμπιστοσύνης ή οποιαδήποτε άλλη δημόσια αρχή·
- τη μη τήρηση των υποχρεώσεων που απορρέουν από την παρούσα ΠΠ/ΔΠΠ και τα σχετικά έγγραφα, εάν η εν λόγω μη τήρηση προκύπτει λόγω Ανωτέρας Βίας.

9.8 Περιορισμοί Ευθύνης

Η ADACOM παρέχει περιορισμένες εγγυήσεις και αποποιείται κάθε άλλης εγγύησης, συμπεριλαμβανομένων εγγυήσεων εμπορευσιμότητας ή καταλληλότητας για συγκεκριμένο σκοπό, περιορίζει την ευθύνη και αποκλείει κάθε ευθύνη, εξαιρουμένου δόλου ή βαριάς αμέλειας, για τυχόν απώλεια κερδών, απώλεια δεδομένων, ή άλλη έμμεση, παρεπόμενη ή ποινική ζημία που προκύπτει από ή σε σχέση με τη χρήση, παράδοση, άδεια, εκπλήρωση, μη εκπλήρωση ή μη διαθεσιμότητα πιστοποιητικών, ηλεκτρονικών υπογράφων, ηλεκτρονικών σφραγίδων, χρονοσφραγίδων ή οποιωνδήποτε άλλων συναλλαγών ή υπηρεσιών που παρέχονται ή αναφέρονται στο παρόν, ακόμα και αν η ADACOM έχει ενημερωθεί για την πιθανότητα τέτοιων ζημίων. Σε καμία περίπτωση η συνολική ευθύνη της ADACOM A.E. έναντι όλων των μερών δεν θα υπερβαίνει το ισχύον ανώτατο όριο ευθύνης για γι' αυτό το εγκεκριμένο πιστοποιητικό όπως αναφέρεται παρακάτω:
η συνολική ευθύνη της ADACOM έναντι οποιουδήποτε και όλων των προσώπων σχετικά με ένα συγκεκριμένο εγκεκριμένο πιστοποιητικό περιορίζεται σε ποσό που δεν υπερβαίνει τα πεντακόσια (500,00) ευρώ ανά πιστοποιητικό και συνολικό ανώτατο όριο απαιτήσεων ύψους πεντακοσίων χιλιάδων (500.000) ευρώ, ανεξάρτητα από τη φύση της ευθύνης και την κατηγορία, το ποσό ή την έκταση οποιασδήποτε ζημίας που υπέστη. Οι περιορισμοί ευθύνης που προβλέπονται στην παρούσα παράγραφο είναι οι ίδιοι ανεξάρτητα από τον αριθμό των πιστοποιητικών, συναλλαγών ή απαιτήσεων που σχετίζονται με το εν λόγω πιστοποιητικό.

Η ευθύνη (και/ή ο περιορισμός αυτής) των Συνδρομητών και των Βασιζόμενων Μερών είναι αυτή που ορίζεται στους ισχύοντες Γενικούς Όρους και Προϋποθέσεις για τη χρήση των Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης.

9.9 Αποζημιώσεις

9.9.1 Αποζημίωση από πλευράς συνδρομητών

Στον βαθμό που το επιτρέπει η ισχύουσα νομοθεσία, οι Συνδρομητές υποχρεούνται να αποζημιώσουν την ADACOM για τα εξής:

- ανακρίβειες ή ψευδείς δηλώσεις στοιχείων από τον Συνδρομητή στην Αίτηση του για Πιστοποιητικό·
- αποτυχία του Συνδρομητή να γνωστοποιήσει κάποιο ουσιώδες στοιχείο στην Αίτηση για Πιστοποιητικό, εφόσον η ψευδής δήλωση ή η παράλειψη έγινε από αμέλεια ή με πρόθεση να εξαπατήσει οποιοδήποτε μέρος·
- αποτυχία του Συνδρομητή να προστατεύσει το ιδιωτικό του κλειδί, να χρησιμοποιήσει ένα Αξιόπιστο Σύστημα ή άλλως να λάβει απαραίτητα προληπτικά μέτρα προκειμένου να αποτραπεί η έκθεση σε κίνδυνο, η απώλεια, η αποκάλυψη, η τροποποίηση ή η μη εξουσιοδοτημένη χρήση του ιδιωτικού κλειδιού του Συνδρομητή ή για
- χρήση ονόματος από τον Συνδρομητή (συμπεριλαμβανομένων ενδεικτικά του κοινού ονόματος, ονόματος τομέα ή διεύθυνσης ηλεκτρονικού ταχυδρομείου) που παραβιάζει τα Δικαιώματα περί Πνευματικής Ιδιοκτησίας οποιουδήποτε τρίτου μέρους.

Οι Γενικοί Όροι και Προϋποθέσεις Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης δύνανται να περιλαμβάνουν πρόσθετες υποχρεώσεις σχετικά με την αποζημίωση.

9.9.2 Αποζημίωση από πλευράς βασιζόμενων μερών

Στον βαθμό που το επιτρέπει η ισχύουσα νομοθεσία, οι Γενικοί Όροι και Προϋποθέσεις Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης της ADACOM υποχρεώνουν τα Βασιζόμενα Μέρη να αποζημιώνουν την ADACOM για τα εξής:

- αποτυχία του Βασιζόμενου Μέρους να εκτελεί τις υποχρεώσεις του ως Βασιζόμενο Μέρος·
- στήριξη του Βασιζόμενου Μέρους σε Πιστοποιητικό που δεν είναι εύλογο σύμφωνα με τις περιστάσεις ή
- αποτυχία του Βασιζόμενου Μέρους να ελέγξει την κατάσταση του σχετικού Πιστοποιητικού ώστε να προσδιορίσει εάν το Πιστοποιητικό έχει λήξει ή ανακληθεί.

Οι Γενικοί Όροι και Προϋποθέσεις Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης δύνανται να περιλαμβάνουν πρόσθετες υποχρεώσεις σχετικά με την αποζημίωση.

9.10 Διάρκεια και λήξη ισχύος

9.10.1 Διάρκεια ισχύος

Η ΠΠ/ΔΠΠ τίθεται σε ισχύ με τη δημοσίευσή της στον χώρο αποθήκευσης της ADACOM. Οι τροποποιήσεις της εν λόγω ΠΠ/ΔΠΠ τίθενται σε ισχύ με τη δημοσίευσή τους στον χώρο αποθήκευσης της ADACOM.

9.10.2 Λήξη ισχύος

Η παρούσα ΠΠ/ΔΠΠ, όπως, κατά διαστήματα, έχει τροποποιηθεί, παραμένει σε ισχύ έως ότου αντικατασταθεί με μια νέα έκδοση.

9.10.3 Έναρξη ισχύος λήξης και μετενέργεια

Με τη λήξη ισχύος της παρούσας ΠΠ/ΔΠΠ, οι Συμμετέχοντες στον Υποτομέα της ADACOM εξακολουθούν εντούτοις να δεσμεύονται από τους όρους της όσον αφορά όλα τα πιστοποιητικά που εκδόθηκαν για το υπόλοιπο των περιόδων ισχύος των σχετικών πιστοποιητικών.

9.11 Ατομικές ειδοποιήσεις και κοινοποιήσεις με συμμετέχοντες

Έκτος αν η συμφωνία μεταξύ των μερών ορίζει διαφορετικά, οι Συμμετέχοντες στον Υποτομέα της ADACOM οφείλουν να χρησιμοποιούν εμπορικά εύλογες μεθόδους για την μεταξύ τους επικοινωνία, λαμβάνοντας υπόψη την κρισιμότητα και το αντικείμενο της επικοινωνίας.

Η παράγραφος 1.5.1 παρέχει όλους τους διαθέσιμους τρόπους επικοινωνίας.

9.12 Τροποποιήσεις

9.12.1 Διαδικασία τροποποίησης

Τροποποιήσεις της παρούσας ΠΠ/ΔΠΠ πραγματοποιούνται από την Αρχή Διαχείρισης Πολιτικών (ΑΔΠ) της ADACOM. Οι τροποποιήσεις είναι είτε υπό μορφή εγγράφου που περιέχει την τροποποιημένη μορφή της ΠΠ/ΔΠΠ είτε με τη μορφή ενημέρωσης. Οι τροποποιημένες εκδόσεις ή ενημερώσεις είναι συνδεδεμένες με τον Χώρο Αποθήκευσης της ADACOM στη διεύθυνση: https://pki.adacom.com/repository. Οι νέες ενημερωμένες εκδόσεις υπερισχύουν έναντι οποιωνδήποτε καθορισμένων ή συγκρουόμενων διατάξεων της αναφερόμενης έκδοσης της ΠΠ/ΔΠΠ. Η ΑΔΠ προσδιορίζει εάν οι αλλαγές στην ΠΠ/ΔΠΠ απαιτούν ή όχι αλλαγές στα αναγνωριστικά αντικειμένου των πολιτικών Πιστοποιητικού.

9.12.2 Μηχανισμός και χρονική περίοδος ειδοποίησης

Η ΑΔΠ της ADACOM διατηρεί το δικαίωμα να τροποποιήσει την παρούσα ΠΠ/ΔΠΠ χωρίς ειδοποίηση, για επουσιώδεις αλλαγές, συμπεριλαμβανομένων, ενδεικτικά, των διορθώσεων τυπογραφικών λαθών και των αλλαγών των δικτυακών κόμβων (URL) ή των αλλαγών στα στοιχεία επικοινωνίας. Ο χαρακτηρισμός των τροποποιήσεων ως ουσιωδών ή επουσιωδών εναπόκειται στην αποκλειστική διακριτική ευχέρεια της ΑΔΠ της ADACOM.

Οι προτεινόμενες τροποποιήσεις στην ΠΠ/ΔΠΠ είναι συνδεδεμένες με τον Χώρο Αποθήκευσης της ADACOM στη διεύθυνση: https://pki.adacom.com/repository.

Έκτος αν ορίζεται διαφορετικά στην παρούσα ΠΠ/ΔΠΠ, εάν η ΑΔΠ της ADACOM θεωρεί ότι ουσιώδεις τροποποιήσεις στην παρούσα ΠΠ/ΔΠΠ είναι άμεσα απαραίτητες, προκειμένου να διακοπεί ή να προληφθεί μία παραβίαση της ασφάλειας του ΠΥΕ ή οποιουδήποτε τμήματός του, η ADACOM δικαιούται να προχωρήσει στις συγκεκριμένες τροποποιήσεις προβαίνοντας στη δημοσίευσή τους στον Αποθηκευτικό χώρο της ADACOM. Οι εν λόγω τροποποιήσεις θα τεθούν αμέσως σε ισχύ με τη δημοσίευσή τους. Μέσα σε εύλογο χρονικό διάστημα μετά τη δημοσίευση, η ADACOM ειδοποιεί σχετικά με τις εν λόγω τροποποιήσεις στους Συμμετέχοντες στον Υποτομέα της ADACOM.
Κατ' ελάχιστον, η ADACOM και ΑΔΠ θα ενημερώνουν την παρούσα ΠΠ/ΔΠΠ σε ετήσια βάση ακολουθώντας τις κατευθυντήριες οδηγίες της ΑΠ/ του Φόρουμ Φυλλομετρητών (CA/Browser Forum).

Οι τροποποιήσεις που δεν αλλάζουν τη σημασία της παρούσας ΠΠ/ΔΠΠ, όπως τυπογραφικές διορθώσεις, μεταφραστικές ενέργειες και ενημερώσεις των στοιχείων επικοινωνίας, τεκμηριώνονται στην ενότητα «Ιστορικό εκδόσεων» του παρόντος εγγράφου. Στην περίπτωση αυτή, το ο δεκαδικός αριθμός της έκδοσης αυξάνεται.

Σε περίπτωση σημαντικών αλλαγών, η νέα έκδοση της ΠΠ/ΔΠΠ είναι σαφώς διακριτή από τις προηγούμενες και ο αριθμός έκδοσης αυξάνεται κατά ένα.

9.12.3 Συνθήκες υπό τις οποίες επιβάλλεται τροποποίηση του αναγνωριστικού αντικειμένου (OID)

Εάν η ΑΔΠ αποφασίσει ότι είναι απαραίτητη κάποια αλλαγή στο αναγνωριστικό αντικειμένου που αντιστοιχεί στην Πολιτική Πιστοποιητικού, η αλλαγή αυτή θα περιλαμβάνει νέα αναγνωριστικά αντικειμένου για τις Πολιτικές Πιστοποιητικών. Διαφορετικά, οι τροποποιήσεις δεν θα πρέπει να απαιτούν αλλαγή στο αναγνωριστικό αντικειμένου της Πολιτικής Πιστοποιητικού.

9.13 Διατάξεις περί επίλυσης διαφορών

9.13.1 Διαφορές μεταξύ της ADACOM, των συνδεδεμένων εταιρειών και των πελατών

Οι διαφορές ανάμεσα στους Συμμετέχοντες στην ΥΔΚ της ADACOM επιλύονται σύμφωνα με τους διατάξεις των εφαρμοστέων συμβάσεων που έχουν συναφθεί μεταξύ των μερών.

9.13.2 Διαφορές με συνδρομητές ή βασιζόμενα μέρη

Οι Γενικοί Όροι και Προϋποθέσεις Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης της ADACOM περιλαμβάνουν ρήτρα για την επίλυση διαφορών. Οι διαφορές που αφορούν την ADACOM απαιτούν αρχική περίοδο διαπραγμάτευσης εξήντα (60) ημερών πριν από τη δικαστική αντιδικία η οποία θα επιλύεται στα δικαστήρια της Αθήνας, στην Ελλάδα.

9.14 Εφαρμοστέο δίκαιο

Η εκτελεστότητα, η ερμηνεία και η εγκυρότητα της παρούσας ΠΠ/ΔΠΠ διέπεται από την κείμενη ελληνική νομοθεσία, χωρίς να λαμβάνονται υπόψη συμβάσεις ή άλλες επιλογές διατάξεων δικαίου και χωρίς την απαίτηση θεμελίωσης εμπορικού δεσμού με την Ελλάδα. Η ανωτέρω επιλογή του εφαρμοστέου δικαίου στοχεύει στη διασφάλιση ομοιόμορφων διαδικασιών και ερμηνείας για το σύνολο των Συμμετεχόντων στον Υποτομέα της ADACOM, ανεξάρτητα από την τοποθεσία τους.

Η παρούσα διάταξη περί εφαρμοστέου δικαίου ισχύει μόνο για την παρούσα ΠΠ/ΔΠΠ. Οι Συμβάσεις που ενσωματώνουν τη ΠΠ/ΔΠΠ με παραπομπή, δύνανται να περιέχουν διαφορετικές διατάξεις περί εφαρμοστέου δικαίου, υπό την προϋπόθεση ότι η παρούσα διάταξη της ενότητας 9.14 διέπει την εκτελεστότητα, την ερμηνεία και την εγκυρότητα των όρων της ΠΠ/ΔΠΠ, ανεξάρτητα από τις λοιπές διατάξεις οποιωνδήποτε σχετικών συμβάσεων που υπόκεινται σε οποιονδήποτε περιορισμό προβλέπεται από την ισχύουσα νομοθεσία.

9.15 Συμμόρφωση με την ισχύουσα νομοθεσία

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

- του eIDAS - Κανονισμού (ΕΕ) αριθ. 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·
- των κανονισμών της ΕΕ και νόμων περί προσωπικών δεδομένων·
- των σχετικών ευρωπαϊκών προτύπων:
    a. ETSI EN 319 401 Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) – Απαιτήσεις γενικής πολιτικής για παρόχους υπηρεσιών εμπιστοσύνης·

b. 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·
c. 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·
d. ETSI TS 119 495 Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) – Ειδικές απαιτήσεις ανά τομέα – Προφίλ Εγκεκριμένων Πιστοποιητικών και Απαιτήσεις πολιτικής για παρόχους υπηρεσιών εμπιστοσύνης κατά την Οδηγία (ΕΕ) 2015/2366 σχετικά με υπηρεσίες πληρωμών

- CA/Browser Forum Baseline Requirements.

9.16 Λοιπές διατάξεις

9.16.1 Σύνολο σύμβασης

Δεν εφαρμόζεται.

9.16.2 Εκχώρηση

Οποιαδήποτε οντότητα που δραστηριοποιείται δυνάμει της παρούσας ΠΠ/ΔΠΠ δεν δύνανται να εκχωρήσει τα δικαιώματα ή τις υποχρεώσεις της χωρίς την πρότερη έγγραφη συγκατάθεση της ADACOM. Εκτός εάν άλλως ορίζεται σε σύμβαση με ένα μέρος, η ADACOM δεν κοινοποιεί την εκχώρηση.

9.16.3 Διαχωρισμός Όρων

Σε περίπτωση που ένα άρθρο ή μια διάταξη της παρούσας ΠΠ/ΔΠΠ κριθεί μη εκτελεστέο από δικαστήριο ή άλλη δικαστική αρχή, το υπόλοιπο της ΠΠ/ΔΠΠ παραμένει σε ισχύ.

9.16.4 Εφαρμογή (αμοιβές δικηγόρων και παραίτηση από δικαιώματα)

Η ADACOM δύναται να απαιτήσει αποζημίωση και αμοιβές δικηγόρων από ένα μέρος για ζημίες, απώλειες και έξοδα που σχετίζονται με τη συμπεριφορά του εν λόγω μέρους. Η αδυναμία της ADACOM να εφαρμόσει μια διάταξη της παρούσας ΠΠ/ΔΠΠ δεν αποτελεί παραίτηση της ADACOM από το δικαίωμά της να εφαρμόσει την ίδια διάταξη αργότερα ή το δικαίωμά της να εφαρμόσει μια οποιαδήποτε άλλη διάταξη της παρούσας ΠΠ/ΔΠΠ. Για να τεθεί σε ισχύ, η παραίτηση από δικαίωμα πρέπει να πραγματοποιείται εγγράφως και να υπογράφεται από την ADACOM.

9.16.5 Ανωτέρα βία

Η μη τήρηση των υποχρεώσεων που απορρέουν από την παρούσα ΠΠ/ΔΠΠ και/ή τα σχετικά έγγραφα δεν θεωρείται παράβαση, εάν η εν λόγω μη τήρηση προκύπτει λόγω Ανωτέρας Βίας. Κανένα από τα μέρη δεν δύναται να αξιώσει οποιαδήποτε μορφή αποζημίωσης από τα έτερα μέρη για καθυστερήσεις και/ή τη μη τήρηση της παρούσας ΠΠ/ΔΠΠ και/ή των σχετικών εγγράφων λόγω Ανωτέρας Βίας.

9.17 Άλλες διατάξεις

Δεν εφαρμόζεται.

Παράρτημα Α. Πίνακας ακρωνυμίων και ορισμών

Πίνακας ακρωνυμίων

Διάρκεια ισχύος	Ορισμός
ΑΔΠ	Αρχή Διαχείρισης Πολιτικών
ΑΕ	Αρχή Εγγραφής
ΑΕΑ	Αρμόδια Εθνική Αρχή
ΑΠ	Αρχή Πιστοποίησης
ΑΥΠ	Αίτημα Υπογραφής Πιστοποιητικού
ΔΠΠ	Δήλωση Πρακτικών Πιστοποίησης
ΔΠΠ	Δήλωση Πρακτικών Πιστοποίησης
ΕΑΤ	Ευρωπαϊκή Αρχή Τραπεζών
ΕΔΔΥ	Εγκεκριμένη Διάταξη Δημιουργίας Ηλεκτρονικής Υπογραφής/Σφραγίδας
ΚΑΠ	Κατάλογος Ανακληθέντων Πιστοποιητικών
ΠΑΠ	Πρωτεύουσα Αρχή Πιστοποίησης
ΠΠ	Πολιτική Πιστοποιητικού
ΠΥΕ	Πάροχος Υπηρεσίας Εμπιστοσύνης
ΠΥΠ	Πάροχος Υπηρεσιών Πληρωμής
ΤΑΕ	Τοπική Αρχή Εγγραφή
ΥΔΚ	Υποδομή Δημόσιου Κλειδιού
FIPS	Ομοσπονδιακά Πρότυπα Επεξεργασίας Πληροφοριών των Ηνωμένων Πολιτειών
NCP	Κανονικοποιημένη Πολιτική Πιστοποιητικού
NCP+	Εκτεταμένη Κανονικοποιημένη Πολιτική Πιστοποιητικού
OCSP	Πρωτόκολλο κατάστασης πιστοποιητικού μέσω σύνδεσης
OID	Αναγνωριστικό αντικειμένου, μοναδικός κωδικός αναγνώρισης αντικειμένου
PDS	Γνωστοποίηση ΥΔΚ
PIN	Προσωπικός αναγνωριστικός αριθμός
PKCS	Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού
PSD2	Οδηγία (ΕΕ) 2015/2366 σχετικά με τις υπηρεσίες πληρωμών
PSP_AS	Πάροχος Υπηρεσιών Πληρωμής_Εξυπηρέτηση λογαριασμού (Account Servicing)
PSP_PI	Πάροχος Υπηρεσιών Πληρωμής Εκκίνησης πληρωμής (Payment Initiation)
PSP_AI	Πάροχος Υπηρεσιών Πληρωμής Πληροφορίες Λογαριασμού (Account Information)
PSP_IC	Πάροχος Υπηρεσιών Πληρωμής Έκδοση μέσων πληρωμής με κάρτα (Issuing of card-based payment instruments_
RFC	Αίτηση για σχολιασμό
SSL	Επίπεδο Ασφαλών Συνδέσεων

Ορισμοί

Διάρκεια ισχύος	Ορισμός
Αίτημα Υπογραφής Πιστοποιητικού (ΑΥΠ)	Μήνυμα που μεταφέρει αίτημα για έκδοση Πιστοποιητικού.
Αίτηση για πιστοποιητικό	Το αίτημα από τον Αιτών για Πιστοποιητικό προς μια ΑΠ για την έκδοση ενός Πιστοποιητικού.
Αιτών Πιστοποιητικό	Το φυσικό πρόσωπο ή ένας οργανισμός που ζητά την έκδοση Πιστοποιητικού από μια ΑΠ.
Αλυσίδα πιστοποιητικού	Ο κατάλογος κατά σειρά κατάταξης των Πιστοποιητικών που περιλαμβάνει ένα Πιστοποιητικό Συνδρομητή, Πιστοποιητικά της ΑΠ και καταλήγει σε ένα Πιστοποιητικό Βάσης (Root).

Διάρκεια ισχύος	Ορισμός
Αξιόπιστο Σύστημα	Το υλικό υπολογιστή, το λογισμικό και οι διαδικασίες, τα οποία είναι ασφαλή σε λογικά πλαίσια από εισβολές και κακή χρήση. Παρέχει ένα επίπεδο διαθεσιμότητας, αξιοπιστίας και ορθής λειτουργίας σε λογικά πλαίσια. Είναι κατά το δυνατόν κατάλληλο για την εκτέλεση των προβλεπόμενων λειτουργιών του και υλοποιεί την ισχύουσα πολιτική ασφάλειας. Ένα αξιόπιστο σύστημα δεν αποτελεί απαραίτητα ένα «σύστημα εμπιστοσύνης», όπως αναγνωρίζεται στην ταξινομημένη κρατική ονοματολογία.
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.
ΑΠ εκτός σύνδεσης (offline)	Οι εκδότριες ΑΠ Βάσης και άλλες καθορισμένες διατηρούνται εκτός σύνδεσης για λόγους ασφάλειας προκειμένου να προστατευθούν έναντι πιθανών επιθέσεων από εισβολείς μέσω του δικτύου. Οι εν λόγω ΑΠ δεν υπογράφουν απευθείας τα Πιστοποιητικά Συνδρομητών τελικού χρήστη.
ΑΠ σε σύνδεση (online)	Οι ΑΠ που υπογράφουν Πιστοποιητικά Συνδρομητών τελικού χρήστη διατηρούνται σε σύνδεση προκειμένου να παρέχουν συνέχεια υπηρεσίες υπογραφής.
Αποθηκευτικός χώρος της ADACOM	Η βάση δεδομένων της ADACOM όσον αφορά τα Πιστοποιητικά και άλλες σχετικές πληροφορίες της ADACOM που είναι προσβάσιμες διαδικτυακά (online).
Αρμόδια Εθνική Αρχή (ΑΕΑ)	Αρχή που διασφαλίζει την αποτελεσματική συμμόρφωση με την Οδηγία (ΕΕ) 2015/2366 (Οδηγία Υπηρεσιών Πληρωμών ΙΙ).
Αρχή Διαχείρισης Πολιτικών (ΑΔΠ)	Ο οργανισμός εντός της ADACOM που είναι υπεύθυνος για την έκδοση της παρούσας πολιτικής.
Αρχή Εγγραφής (ΑΕ)	Πρόκειται για μια οντότητα που έχει εγκριθεί από μια ΑΠ και είναι υπεύθυνη για την ταυτοποίηση και την επαλήθευση της ταυτότητας των υποκειμένων των πιστοποιητικών. Επιπλέον, μια ΑΕ μπορεί να συνδράμει στη διαδικασία υποβολής αιτήσεων για πιστοποιητικό ή στη διαδικασία ανάκλησης ή και στις δύο διαδικασίες.
Αρχή Πιστοποίησης (ΑΠ)	Οντότητα που έχει εξουσιοδοτηθεί να δημιουργήσει και να αναθέτει πιστοποιητικά.
Βασιζόμενο Μέρος	Ένα φυσικό πρόσωπο ή οργανισμός που ενεργεί βασιζόμενος σε ένα πιστοποιητικό.
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 ADACOM παρέχει τις αντίστοιχες Υπηρεσίες Εμπιστοσύνης.
Δήλωση Πρακτικών Πιστοποίησης (ΔΠΠ)	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.
Διαμοιρασμός Απορρήτου	Η πρακτική του διαχωρισμού ενός ιδιωτικού κλειδιού της ΑΠ ή των δεδομένων ενεργοποίησής του προκειμένου να λειτουργήσει το ιδιωτικό κλειδί της ΑΠ ώστε να ενισχύσει τον έλεγχο πολλαπλών ατόμων επί των λειτουργιών του ιδιωτικού κλειδιού της ΑΠ.
Διαχειριστής	Πρόκειται για ένα Έμπιστο Πρόσωπο εντός του οργανισμού που πραγματοποιεί την επικύρωση και άλλες λειτουργίες της ΑΠ ή της ΑΕ.
Δικαιώματα Πνευματικής	Δικαιώματα επί ενός ή περισσοτέρων από τα ακόλουθα: οποιοδήποτε

Διάρκεια ισχύος	Ορισμός
Ιδιοκτησίας	δικαίωμα δημιουργού, δίπλωμα ευρεσιτεχνίας, εμπορικό μυστικό, εμπορικό σήμα, καθώς και κάθε άλλο δικαίωμα πνευματικής ιδιοκτησίας.
Εγκεκριμένη διάταξη δημιουργίας υπογραφής ή σφραγίδας (ΕΔΔΥ)	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.
Εγκεκριμένη ηλεκτρονική σφραγίδα	Πρόκειται για μια προηγμένη ηλεκτρονική σφραγίδα που δημιουργείται από εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής σφραγίδας και βασίζεται σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής σφραγίδας.
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 και το οποίο έχει διαπιστευτεί και εποπτεύεται από αρχές που ορίζονται από κράτος μέλος της ΕΕ και πληροί τις απαιτήσεις του κανονισμού eIDAS.
Εγκεκριμένο Πιστοποιητικό για ηλεκτρονική υπογραφή	Πιστοποιητικό ηλεκτρονικής υπογραφής που εκδίδεται από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης και πληροί τις οριζόμενες στο παράρτημα III απαιτήσεις του eIDAS·
Εγκεκριμένο Πιστοποιητικό για ηλεκτρονική σφραγίδα	Πιστοποιητικό ηλεκτρονικής σφραγίδας που εκδίδεται από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης και πληροί τις οριζόμενες στο παράρτημα III απαιτήσεις του 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.
Έγκυρο Πιστοποιητικό	Πιστοποιητικό που πέρασε με επιτυχία τη διαδικασία ταυτοποίησης η οποία προσδιορίζεται στο RFC 5280.
Έκθεση σε κίνδυνο	Η παραβίαση (ή υποτιθέμενη παραβίαση) μιας πολιτικής ασφαλείας, κατά την οποία μπορεί να έχει συμβεί μη εξουσιοδοτημένη αποκάλυψη ή απώλεια του ελέγχου επί διαβαθμισμένων πληροφοριών. Όσον αφορά τα ιδιωτικά κλειδιά, η Έκθεση σε Κίνδυνο αποτελεί η απώλεια, η κλοπή, η γνωστοποίηση, η τροποποίηση, η μη εξουσιοδοτημένη χρήση ή κάθε άλλη έκθεση της ασφάλειας του ιδιωτικού αυτού κλειδιού σε κίνδυνο.
Έλεγχος συμμόρφωσης	Ο περιοδικός έλεγχος στον οποίο υποβάλλεται ένας ΠΥΕ, Κέντρο Επεξεργασίας, το Κέντρο Υπηρεσιών ή Πελάτης της υπηρεσίας Managed PKI ώστε να προσδιοριστεί η συμμόρφωσή του με τη νομοθεσία, τις πολιτικές και τα πρότυπα που ισχύουν σε αυτό.
Έμπιστο πρόσωπο	Ένας υπάλληλος, ανάδοχος ή σύμβουλος μιας οντότητας, ο οποίος είναι υπεύθυνος για τη διαχείριση της αξιοπιστίας της υποδομής της οντότητας, των προϊόντων, των υπηρεσιών, των εγκαταστάσεων και/ή των πρακτικών της.
Ενδιάμεση Αρχή Πιστοποίησης (Ενδιάμεση ΑΠ)	Η Αρχή Πιστοποίησης της οποίας το Πιστοποιητικό βρίσκεται εντός της Αλυσίδας Πιστοποιητικών μεταξύ του Πιστοποιητικού της ΑΠ Βάσης (Root) και του Πιστοποιητικού της Αρχής Πιστοποίησης που εξέδωσε το Πιστοποιητικό Συνδρομητή τελικού χρήστη.
Εξ αποστάσεως ΕΔΔΥ	Εγκεκριμένη Διάταξη Δημιουργίας Υπογραφής Εξ αποστάσεως που πληροί τις απαιτήσεις του Παραρτήματος II του Κανονισμού eIDAS
Εξ αποστάσεως ταυτοποίηση	Η μέθοδος/διαδικασία μέσω της οποίας ο Συνδρομητής ταυτοποιείται μέσω ζωντανής βιντεοκλήσης και είναι ισοδύναμη με ταυτοποίηση μέσω φυσικής παρουσίας.
Επίπεδο Ασφαλών Συνδέσεων (SSL)	Η πρότυπη μέθοδος του κλάδου για την προστασία των Διαδικτυακών επικοινωνιών η οποία αναπτύχθηκε από τη Netscape Communications Corporation. Το πρωτόκολλο ασφαλείας SSL παρέχει κρυπτογράφηση των δεδομένων, επαλήθευση ταυτότητας διακομιστή (server), ακεραιότητα μηνύματος, και προαιρετικά επαλήθευση ταυτότητας χρήστη (client) για σύνδεση Transmission Control Protocol/Internet Protocol (Πρωτοκόλλου Ελέγχου Μετάδοσης/ Πρωτοκόλλου Διαδικτύου).

Διάρκεια ισχύος	Ορισμός
Εποπτικός φορέας	Η αρχή που ορίζεται από κράτος μέλος για να διενεργεί τις εποπτικές δραστηριότητες σχετικά με τις Υπηρεσίες Εμπιστοσύνης και τους Παρόχους Υπηρεσιών Εμπιστοσύνης δυνάμει του κανονισμού eIDAS εντός της επικράτειας του εν λόγω κράτους μέλους.
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.
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.
Θέση Εμπιστοσύνης	Οι θέσεις εντός της ADACOM τις οποίες πρέπει να κατέχει Έμπιστο Πρόσωπο.
Ιδιωτικό Κλειδί	Το κλειδί ενός ζεύγους κλειδιών το οποίο διατηρείται κρυφό από τον κάτοχο του ζεύγους κλειδιών και το οποίο χρησιμοποιείται για τη εγκεκριμένων πιστοποιητικών ή για την αποκρυπτογράφηση ηλεκτρονικών αρχείων ή φακέλων που έχουν κρυπτογραφηθεί με το αντίστοιχο δημόσιο κλειδί.
Κατάλογος Ανακληθέντων Πιστοποιητικών (ΚΑΠ)	Ο υπογεγραμμένος κατάλογος που αναφέρει ένα σύνολο πιστοποιητικών που έχουν ανακληθεί από τον εκδότη των πιστοποιητικών.
Κέντρο Επεξεργασίας	Ο χώρος της ADACOM που δημιουργεί μια ασφαλή εγκατάσταση που στεγάζει, μεταξύ άλλων, τις κρυπτογραφικές μονάδες που χρησιμοποιούνται για την έκδοση των Πιστοποιητικών.
Κωδικός μιας χρήσης	Τυχαίος κωδικός που παράγεται από εφαρμογή και χρησιμοποιείται μια φορά
Λειτουργική περίοδος	Το χρονικό διάστημα το οποίο ξεκινά την ημερομηνία και τον χρόνο έκδοσης ενός Πιστοποιητικού (ή σε μεταγενέστερη καθορισμένη ημερομηνία και χρόνο εάν δηλώνεται στο Πιστοποιητικό) και τερματίζει με την ημερομηνία και τον χρόνο κατά τον οποίο λήγει ή πρόωρα ανακαλείται το Πιστοποιητικό.
Μερίδιο Απορρήτου	Ένα τμήμα του ιδιωτικού κλειδιού μιας ΑΠ ή ένα τμήμα των δεδομένων ενεργοποίησης που είναι απαραίτητα για τη λειτουργία ενός ιδιωτικού κλειδιού της ΑΠ σύμφωνα με το σχέδιο του Διαμοιρασμού Απορρήτου.
Μη αποκήρυξη	Το χαρακτηριστικό μιας επικοινωνίας που παρέχει προστασία έναντι ενός μέρους που συμμετέχει στην επικοινωνία και το οποίο αρνείται ψευδώς για την προέλευσή της, αρνείται ότι υποβλήθηκε ή επιδόθηκε. Η άρνηση της προέλευσης περιλαμβάνει την άρνηση ότι η επικοινωνία προερχόταν από την ίδια πηγή στα πλαίσια μιας σειράς ενός ή περισσοτέρων προγενέστερων μηνυμάτων, ακόμα και αν η ταυτότητα που σχετίζεται με τον αποστολέα είναι άγνωστη. Σημείωση: μόνο η απόφαση δικαστηρίου, οργάνου διαιτησίας ή άλλου δικαστικού σώματος μπορεί να αποτρέψει τελικώς την αποκήρυξη. Για παράδειγμα, μια ψηφιακή υπογραφή που επαληθεύεται κατ' αναφορά σε ένα Εγκεκριμένο Πιστοποιητικό μπορεί να αποτελεί αποδεικτικό στοιχείο προς υποστήριξη δικαστικής απόφασης περί μη αποκήρυξης, ενώ η ίδια δεν συνιστά από μόνη της μη αποκήρυξη.
Μη αυτόματη επαλήθευση ταυτότητας	Διαδικασία με την οποία οι Αιτήσεις για Πιστοποιητικό ελέγχονται και εγκρίνονται με αυτόματο τρόπο (manually), μία προς μία, από έναν Διαχειριστή που χρησιμοποιεί διεπαφή που βασίζεται στο Web.
Πάροχος Υπηρεσίας Εμπιστοσύνης	Οντότητα που παρέχει μία ή περισσότερες Υπηρεσίες Εμπιστοσύνης.
Περίοδος ισχύος	Η χρονική περίοδος που υπολογίζεται από την ημερομηνία έκδοσης του Πιστοποιητικού έως την ημερομηνία λήξης ισχύος.
Πιστοποιητικό	Πρόκειται για το δημόσιο κλειδί ενός χρήστη μαζί με ορισμένες άλλες πληροφορίες οι οποίες παραδίδονται μη παραποιημένες βάσει κρυπτογράφησης με το ιδιωτικό κλειδί της αρχής πιστοποίησης που το εξέδωσε.
Πιστοποιητικό Διαχειριστή	Πρόκειται για ένα Πιστοποιητικό που εκδίδεται σε έναν Διαχειριστή το οποίο μπορεί να χρησιμοποιηθεί μόνο για την εκτέλεση των λειτουργιών της ΑΠ ή της ΑΕ.
Πιστοποιητικό μακράς διάρκειας	Το εγκεκριμένο πιστοποιητικό που ισχύει για 1 έως και 3 έτη.

Διάρκεια ισχύος	Ορισμός
Πιστοποιητικό σύντομης διάρκειας	Το εγκεκριμένο πιστοποιητικό που έχει ισχύ για 24 έως 72 ώρες και χρησιμοποιείται για μία συναλλαγή.
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 σφραγίδα	Μια προηγμένη ηλεκτρονική σφραγίδα πληροί τις ακόλουθες απαιτήσεις: • συνδέεται κατά τρόπο μοναδικό με τον υπογράφοντα· • είναι ικανή να ταυτοποιεί τον 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.
Προηγμένη ηλεκτρονική υπογραφή	Μια προηγμένη ηλεκτρονική υπογραφή πληροί τις ακόλουθες απαιτήσεις: • συνδέεται κατά τρόπο μοναδικό με τον υπογράφοντα· • είναι ικανή να ταυτοποιεί τον 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.
Πρωτεύουσα Αρχή Πιστοποίησης ΠΑΠ)	Μια ΑΠ που ενεργεί ως ΑΠ Βάσης (Root) και εκδίδει Πιστοποιητικά σε ΑΠ που είναι ιεραρχικά υφιστάμενές της.
Πρωτόκολλο κατάστασης πιστοποιητικού μέσω σύνδεσης (OCSP)	Το πρωτόκολλο που χρησιμοποιείται για να παρέχει στα Βασιζόμενα Μέρη πληροφορίες σε πραγματικό χρόνο σχετικά με την κατάσταση των Πιστοποιητικών.
Συμμετέχων	Φυσικό πρόσωπο ή οργανισμός που είναι είτε η ADACOM, Πελάτης, Αρχή Πιστοποίησης, Αρχή Έγγραφής, Συνδρομητής ή Βασιζόμενο Μέρος.
Συνδρομητής	Μια οντότητα που είναι εγγεγραμμένη στον Πάροχο Υπηρεσιών Εμπιστοσύνης, η οποία δεσμεύεται νομικά από τυχόν υποχρεώσεις του Συνδρομητή.
Συνθηματική φράση	Η μυστική φράση που επιλέγει ο Αιτών Πιστοποιητικό κατά την εγγραφή για ένα Πιστοποιητικό. Κατά την έκδοση του Πιστοποιητικού, ο Αιτών Πιστοποιητικό καθίσταται Συνδρομητής και η ΑΠ ή η ΑΕ μπορεί να χρησιμοποιήσει τη Συνθηματική Φράση για την επαλήθευση της ταυτότητας του Συνδρομητή όταν αυτός ζητά την ανάκληση ή την ανανέωση του Πιστοποιητικού του.
Τοπική ΕΔΔΥ	Εγκεκριμένη διάταξη τύπου USB (token) ή έξυπνης κάρτας
Υπηρεσία Εμπιστοσύνης	Πρόκειται για την ηλεκτρονική υπηρεσία για τα ακόλουθα: • τη δημιουργία, την εξακρίβωση και την επικύρωση ψηφιακών υπογραφών και σχετικών πιστοποιητικών· • τη δημιουργία, την εξακρίβωση και την επικύρωση χρονοσφραγίδων και σχετικών πιστοποιητικών· • τη συστημένη παράδοση και τα πιστοποιητικά που σχετίζονται με την υπηρεσία αυτή· • τη δημιουργία, την εξακρίβωση και την επικύρωση πιστοποιητικών για επαλήθευση της ταυτότητας ιστότοπων, ή • τη διαφύλαξη ψηφιακών υπογραφών ή πιστοποιητικών που σχετίζονται με τις υπηρεσίες αυτές.
Υποδομή Δημόσιου Κλειδιού (ΥΔΚ)	Η αρχιτεκτονική, η οργανωτική δομή, οι τεχνικές, οι κανονισμοί, και οι διαδικασίες που στο σύνολό τους υποστηρίζουν την εφαρμογή και τη λειτουργία του κρυπτογραφικού συστήματος δημοσίου κλειδιού που βασίζεται σε Πιστοποιητικό. Η ΥΔΚ της ADACOM αποτελείται από συστήματα που συνεργάζονται για την παροχή και την υλοποίηση της ΥΔΚ της ADACOM.
Υποκείμενο	Το Υποκείμενο μπορεί να είναι:

Διάρκεια ισχύος	Ορισμός
	α) ένα φυσικό πρόσωπο· β) ένα φυσικό πρόσωπο που προσδιορίζεται σε σχέση με ένα νομικό πρόσωπο· γ) ένα νομικό πρόσωπο (που μπορεί να είναι ένας Οργανισμός ή μια μονάδα ή τμήμα που προσδιορίζεται σε σχέση με έναν Οργανισμό)·
Υφιστάμενη ΑΠ	Η αρχή πιστοποίησης της οποίας το Πιστοποιητικό υπογράφεται από την ΑΠ Βάσης ή άλλης ιεραρχικά υφιστάμενης ΑΠ. Μια ιεραρχικά υφιστάμενη ΑΠ συνήθως εκδίδει είτε πιστοποιητικά τελικού χρήστη είτε άλλα πιστοποιητικά της ιεραρχικά υφιστάμενης ΑΠ.
eIDAS	Κανονισμός (ΕΕ) αριθ. 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.
PKCS #10	Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού (Public−Key Cryptography Standard) #10 που έχει αναπτυχθεί από την RSA Security Inc. και το οποίο καθορίζει τη δομή του Αιτήματος Υπογραφής Πιστοποιητικού.
PKCS #12	Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού (Public−Key Cryptography Standard) #12 που έχει αναπτυχθεί από την RSA Security Inc. και το οποίο καθορίζει το ασφαλές μέσο για τη μεταβίβαση των ιδιωτικών κλειδιών.
RSA	Κρυπτογραφικό σύστημα δημοσίου κλειδιού που επινοήθηκε από τους Rivest, Shamir και Adelman.