



ADACOM

CYBER SECURITY

ADACOM

Πολιτική Πιστοποιητικού &
Δήλωση Πρακτικών Πιστοποίησης
Αρχής Χρονοσφραγίδας

Έκδοση 2.0

Ισχύει από 10 Φεβρουαρίου 2023

© 2023 ADACOM S.A. Με την επιφύλαξη παντός δικαιώματος

Πληροφορίες Κειμένου

Το παρόν έγγραφο δημιουργήθηκε από την ADACOM A.E και περιλαμβάνει τους όρους υπό τους οποίους η ADACOM λειτουργεί ως Εγκεκριμένος Πάροχος Υπηρεσιών Χρονοσφραγίδας (ΕΠΥΧ).

Το παρόν βασίζεται και είναι συμβατό με το Πρότυπο EN 319 421 (ESI) – Απαιτήσεις γενικής πολιτικής για παρόχους υπηρεσιών εμπιστοσύνης

Δικαιώματα Πνευματικής Ιδιοκτησίας

Τα πνευματικά δικαιώματα του παρόντος ανήκουν στην ADACOM. Όλα τα δικαιώματα διατηρούνται. Εκτός από τις κατωτέρω επιτρεπόμενες περιπτώσεις, κανένα τμήμα της παρούσας δημοσίευσης δεν δύναται να αναπαραχθεί, να αποθηκευτεί ή να εισαχθεί σε σύστημα ανάκτησης ή να μεταδοθεί σε οποιαδήποτε μορφή ή με οποιοδήποτε μέσο (μέσω ηλεκτρονικής, μηχανικής μετάδοσης, φωτοτύπησης, εγγραφής ή άλλου μέσου) χωρίς την πρότερη γραπτή άδεια της ADACOM A.E.

Τα αιτήματα για οποιαδήποτε άλλη άδεια αναπαραγωγής της παρούσας δημοσίευσης (καθώς και αιτήματα για χορήγηση αντιγράφων από την ADACOM A.E.) πρέπει να αποστέλλονται στην ADACOM A.E., Κρέοντος 25, Τ.Κ. 10442, Σεπόλια, Ελλάδα Υπόψη: Αρχή Διαχείρισης Πολιτικών. Τηλ.: +30 210 5193740, Email: practices@adacom.com.

Ιστορικό Εκδόσεων

| Ημερομηνία | Έκδοση | Μεταβολές |
|------------|--------|---|
| 10/01/2019 | 1.0 | Αρχικό έγγραφο |
| 25/01/2019 | 1.1 | Μικρές αλλαγές στην παρ. 7.4.7 |
| 15/02/2019 | 1.2 | Μικρές αλλαγές στην παρ. 4.2 |
| 10/02/2023 | 2.0 | Αλλαγές στις παρ. 1.1, 5.2 (προηγ. 6.2), 5.3 (προηγ. 6.3), 5.4 (προηγ. 6.4), 6.4.9 (προηγ. 7.4.9), Προσθήκη ενότητας 7, μετακίνηση του πίνακα ορισμών και συντομογραφιών στην ενότητα 8, νέα αρίθμηση |

Περιεχόμενα

| | |
|--|----|
| 1. Εισαγωγή | 5 |
| 1.1 Διαχείριση Πολιτικής..... | 5 |
| 1.2 Διαδικασία Έγκρισης | 6 |
| 2. Πηγές | 6 |
| 3. Γενικές Έννοιες | 6 |
| 3.1 Υπηρεσίες Χρονοσφραγίδας..... | 6 |
| 3.2 Αρχή Χρονοσφραγίδας | 7 |
| 3.3 Συνδρομητές..... | 7 |
| 3.3.1 Βασιζόμενα Μέρη | 8 |
| 3.3.2 Άλλοι Συμμετέχοντες | 8 |
| 3.3.3 Χρήση Χρονοσφραγίδων..... | 8 |
| 3.4 Πολιτική Χρονοσφραγίδας και Δήλωση Πρακτικών Αρχής Χρονοσφραγίδας..... | 8 |
| 3.4.1 Σκοπός | 8 |
| 3.4.2 Επίπεδο εξειδίκευσης | 8 |
| 3.4.3 Προσέγγιση..... | 9 |
| 4. Πολιτικές Χρονοσφραγίδας..... | 9 |
| 4.1 Επισκόπηση..... | 9 |
| 4.2 Αναγνώριση..... | 9 |
| 4.3 Κοινότητα Χρηστών και Εφαρμογή | 9 |
| 4.4 Συμμόρφωση | 9 |
| 5. Υποχρεώσεις και Ευθύνη | 10 |
| 5.1 Υποχρεώσεις Αρχής Χρονοσφραγίδας | 10 |
| 5.1.1 Γενικές Υποχρεώσεις..... | 10 |
| 5.1.2 Υποχρεώσεις Αρχής Χρονοσφραγίδας προς Συνδρομητές | 10 |
| 5.2 Υποχρεώσεις Συνδρομητών | 10 |
| 5.3 Υποχρεώσεις Βασιζόμενων Μερών | 11 |
| 5.4 Ευθύνη..... | 11 |
| 6. Πρακτικές Αρχής Χρονοσφραγίδας | 12 |
| 6.1 Δηλώσεις Πρακτικών και Κοινοποίησης..... | 12 |
| 6.1.1 Δήλωση Πρακτικών Αρχής Χρονοσφραγίδας..... | 12 |
| 6.1.2 Δήλωση Γνωστοποίησης Αρχής Χρονοσφραγίδας | 12 |
| 6.2 Κύκλος Ζωής Διαχείρισης Κλειδιού | 13 |
| 6.2.1 Δημιουργία Κλειδιού Αρχής Χρονοσφραγίδας..... | 13 |

| | | |
|--------|---|----|
| 6.2.2 | Προστασία Ιδιωτικού Κλειδιού MX..... | 13 |
| 6.2.3 | Διανομή Δημοσίου Κλειδιού MX | 13 |
| 6.2.4 | Επαναδημιουργία κλειδιού MX..... | 14 |
| 6.2.5 | Τέλος Κύκλου Ζωής Κλειδιού MX | 14 |
| 6.2.6 | Διαχείριση Κύκλου Ζωής της Κρυπτογραφικής Μονάδας που χρησιμοποιείται για την υπογραφή χρονοσφραγίδων | 14 |
| 6.3 | Χρονοσφράγιση | 14 |
| 6.3.1 | Διακριτικό Χρονοσφραγίδας (ΔΧ)..... | 14 |
| 6.3.2 | Συγχρονισμός Ρολογιού με UTC..... | 15 |
| 6.3.3 | Διαδικασία Χειρισμού Άλματος Δευτερολέπτου | 15 |
| 6.4 | Διαχείριση και Λειτουργία Αρχής Χρονοσφραγίδας..... | 15 |
| 6.4.1 | Διαχείριση Ασφάλειας..... | 15 |
| 6.4.2 | Ταξινόμηση και Διαχείριση Περιουσιακών Στοιχείων | 15 |
| 6.4.3 | Ασφάλεια Προσωπικού | 15 |
| 6.4.4 | Φυσικοί και Περιβαλλοντική Ασφάλεια | 17 |
| 6.4.5 | Επιχειρησιακή Διαχείριση | 18 |
| 6.4.6 | Εγκατάσταση και συντήρηση αξιόπιστων συστημάτων | 18 |
| 6.4.7 | Έκθεση σε κίνδυνο των Υπηρεσιών της Αρχής Χρονοσφραγίδας | 19 |
| 6.4.8 | Τερματισμός Αρχής Χρονοσφραγίδας | 19 |
| 6.4.9 | Συμμόρφωση με τη νομοθεσία..... | 19 |
| 6.4.10 | Καταγραφή πληροφοριών σχετικά με τη Λειτουργία των Υπηρεσιών Χρονοσφραγίδας..... | 20 |
| 7. | Άλλα Επιχειρησιακά και Νομικά Θέματα..... | 20 |
| 7.1 | Οικονομική υπευθυνότητα..... | 20 |
| 7.2 | Ισχύουσες συμφωνίες, ΠΠ, ΔΠΠ..... | 20 |
| 7.3 | Πολιτική Απορρήτου..... | 20 |
| 7.4 | Πολιτική επιστροφής χρημάτων | 21 |
| 7.5 | Άδειες Αποθηκευτικού Χώρου, Σήματα Αξιοπιστίας και Έλεγχος..... | 21 |
| 7.6 | Εφαρμοστέο δίκαιο, Καταγγελίες, Επίλυση διαφορών..... | 21 |
| 8. | Ορισμοί και συντομογραφίες | 21 |
| 8.1 | Ορισμοί..... | 21 |
| 8.2 | Συντομογραφίες | 24 |

1. Εισαγωγή

Το παρόν έγγραφο αποτελεί την Πολιτική Πιστοποιητικού & τη Δήλωση Πρακτικών Πιστοποίησης της Αρχής Χρονοσφραγίδας για Υπηρεσίες Εγκεκριμένης Χρονοσφραγίδας της ADACOM. Σκοπός του παρόντος είναι η περιγραφή των κανόνων και των λειτουργικών διαδικασιών που υιοθετεί η ADACOM ως Εγκεκριμένος Πάροχος Υπηρεσιών Εμπιστοσύνης (ΕΠΥΕ) για την παροχή των Εγκεκριμένων Υπηρεσιών Χρονοσφραγίδας, σύμφωνα με τον Κανονισμό (ΕΕ) Ν° 910/2014 [eIDAS].

Οι Υπηρεσίες Εγκεκριμένης Χρονοσφραγίδας της ADACOM, ενισχύουν τον αποδεικτικό ισχυρισμό ότι ένα ηλεκτρονικό αρχείο υπήρχε πριν από ένα συγκεκριμένο χρονικό σημείο. Αυτές οι υπηρεσίες μπορούν να χρησιμοποιηθούν για να υποστηρίξουν υπηρεσίες μη αποκήρυξης, για να αποδείξουν ότι μια ηλεκτρονική υπογραφή είχε παραχθεί κατά τη διάρκεια της περιόδου ισχύος ενός πιστοποιητικού δημοσίου κλειδιού, για να υποστηρίξει μακροχρόνια ηλεκτρονική αρχειοθέτηση κτλ.

Οι Υπηρεσίες Εγκεκριμένης Χρονοσφραγίδας της ADACOM, είναι μέρος των υπηρεσιών Υποδομής Δημοσίου Κλειδιού (ΥΔΚ) της ADACOM.

Το παρόν έγγραφο, περιγράφει γενικούς κανόνες που εφαρμόζονται από την Αρχή Χρονοσφραγίδας (ΑΧ) για την έκδοση Διακριτικού Χρονοσφραγίδας (ΔΧ) και ορίζει τα εμπλεκόμενα μέρη, τις αρμοδιότητες τους, τα δικαιώματα τους και το εύρος εφαρμογής.

Η Αρχή Χρονοσφραγίδας της ADACOM είναι προσβάσιμη μέσω του <https://tts.adacom.com/qTTS/Timestamp>.

Η Αρχή Χρονοσφραγίδας δεν προβαίνει σε μακροχρόνια αρχειοθέτηση των Διακριτικών Χρονοσφραγίδας και η εφαρμογή που χρησιμοποιεί η ΑΧ θα πρέπει να αποθηκεύει το εκδοθέν διακριτικό για μελλοντική χρήση.

Οι Υπηρεσίες Εγκεκριμένης Χρονοσφραγίδας της ADACOM παρέχονται σύμφωνα με τα πρότυπα EN 319 421 και EN 319 422 και υπό την εποπτεία της ADACOM, ενεργώντας ως Εγκεκριμένος Πάροχος Υπηρεσιών Χρονοσφραγίδας.

Η Διοίκηση μπορεί να κάνει εξαιρέσεις σε αυτή την ΠΠ/ΔΠΠ ανά περίπτωση, για να μετριάσει ουσιαστικές, επικείμενες επιπτώσεις σε πελάτες, συνεργάτες, βασιζόμενα μέρη και/ή άλλους, όταν δεν υπάρχουν πρακτικές εναλλακτικές.

1.1 Διαχείριση Πολιτικής

Οργανισμός που Διαχειρίζεται το Έγγραφο

ADACOM A.E.

Κρέοντος 25

10442, Αθήνα

Ελλάδα

Υπεύθυνος Επικοινωνίας

Υπεύθυνος Πολιτικής ΥΔΚ

Αρχή Διαχείρισης Πολιτικών της ADACOM

Υπόψη ADACOM A.E.

Κρέοντος 25

10442, Αθήνα, Ελλάδα

Τηλέφωνο: +30 210 5193740

email: practices@adacom.com

1.2 Διαδικασία Έγκρισης

Η έγκριση της παρούσας ΠΠ/ΔΠΠ και των επακόλουθων τροποποιήσεων πραγματοποιούνται από την ΑΔΠ. Οι τροποποιήσεις πραγματοποιούνται είτε σε μορφή εγγράφου που περιλαμβάνει την τροποποιημένη έκδοση της 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 αντικείμενα των πολιτικών Πιστοποιητικού.

2. Πηγές

Τα παρακάτω έγγραφα σχετίζονται με την παρούσα ΠΠ & ΔΠΠ για Υπηρεσίες Εγκεκριμένης Χρονοσφραγίδας της ADACOM:

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

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

[3] ETSI EN 319 421: Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) - Policy and Security Requirements for Trust Service Providers issuing Time-Stamps". [3] ETSI EN 319 421: «Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) - Απαιτήσεις πολιτικής και ασφάλειας για τους παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν χρονοσφραγίδες»

[4] ETSI EN 319 422: «Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) — Πρωτόκολλο Χρονοσφραγίδας και προφίλ token Χρονοσφραγίδας και Time-stamping protocol and time-stamp token profiles".».

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

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

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

3. Γενικές Έννοιες

3.1 Υπηρεσίες Χρονοσφραγίδας

Οι Υπηρεσίες Εγκεκριμένων Χρονοσφραγίδων της ADACOM αποτελείται από τη διαχείριση της υποδομής και την παροχή Διακριτικών Χρονοσφραγίδας. Αυτές οι υπηρεσίες παρέχονται από την Αρχή Χρονοσφραγίδας της ADACOM (ΑΧ) στους Συνδρομητές, αποτελούν αναπόσπαστο μέρος της Υποδομής Δημοσίου Κλειδιού (ΥΔΚ) της ADACOM και είναι σύμφωνες με τον Κανονισμό eIDAS και το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI).

Οι Υπηρεσίες Εγκεκριμένων Χρονοσφραγίδων διασφαλίζουν την χρήση αξιόπιστης πηγής χρόνου και την κατάλληλη διαχείριση όλων των στοιχείων του συστήματος.

3.2 Αρχή Χρονοσφραγίδας

Η Αρχή Χρονοσφραγίδας της ADACOM είναι υπεύθυνη για την παροχή Υπηρεσιών Εγκεκριμένων Χρονοσφραγίδων όπως περιγράφεται στο παρόν έγγραφο. Έχει την ευθύνη για τη λειτουργία των σχετικών Μονάδων Χρονοσφραγίδας (MX) που δημιουργούνται και υπογράφονται εκ μέρους της AX. Η νομική οντότητα υπεύθυνη για την AX είναι η ADACOM A.E. ενεργούσα ως ΕΠΥΧ.

Η ADACOM εκδίδει Εγκεκριμένες Χρονοσφραγίδες κατά την παρακάτω ιεραρχία:

ΑΠ Βάσης (Root CA)

CN = ADACOM Global Qualified CA

O = ADACOM S.A.

2.5.4.97 = VATEL-099554476

OU = ADACOM Trust Services

C = GR

CA Αρχής Χρονοσφραγίδας (Time Stamping Authority CA)

CN = ADACOM Qualified Timestamping CA

O = ADACOM S.A.

2.5.4.97 = VATEL-099554476

OU = ADACOM Trust Services

C = GR

CA Μονάδας Χρονοσφραγίδας (Time Stamping Unit CA)

CN = ADACOM Qualified TSU 2018

O = ADACOM S.A.

2.5.4.97 = VATEL-099554476

OU = ADACOM Trust Services

C = GR

Οι χρονοσφραγίδες της AX της ADACOM εκδίδονται σύμφωνα με τις παρακάτω πολιτικές πιστοποιητικού:

- **OID 0.4.0.2042.1.2** itu-t(0) identified-organization(4) etsi(0) other-certificate-policies(2042) policy-identifiers(1) ncplus(2)
- **OID 0.4.0.2023.1.1:** itu-t(0) identifiedorganization(4) etsi(0) time-stamp-policy(2023) policy-identifiers(1) baseline-ts-policy (1).

3.3 Συνδρομητές

Ο Συνδρομητής είναι το φυσικό ή νομικό πρόσωπο που κάνει αίτηση, στο οποίο παρέχεται η χρονοσφραγίδα και το οποίο συνάπτει σύμβαση με την ADACOM.

Ο Συνδρομητής μπορεί να είναι ένας οργανισμός που αποτελείται από πολλούς τελικούς χρήστες ή έναν μεμονωμένο τελικό χρήστη.

Όταν ο Συνδρομητής είναι ένας οργανισμός, ορισμένες από τις υποχρεώσεις που ισχύουν για τον εν λόγω οργανισμό θα πρέπει να ισχύουν και για τους τελικούς χρήστες. Σε κάθε περίπτωση, ο οργανισμός θα θεωρηθεί υπεύθυνος εάν οι υποχρεώσεις των τελικών χρηστών δεν εκπληρωθούν σωστά και επομένως ένας τέτοιος οργανισμός θα πρέπει να ενημερώσει δεόντως τους τελικούς χρήστες του.

Όταν ο Συνδρομητής είναι τελικός χρήστης, αυτός θα είναι άμεσα υπεύθυνος εάν οι υποχρεώσεις του δεν πληρούνται σωστά.

3.3.1 Βασιζόμενα Μέρη

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

3.3.2 Άλλοι Συμμετέχοντες

Δεν εφαρμόζεται.

3.3.3 Χρήση Χρονοσφραγίδων

Οι Χρονοσφραγίδες που εκδίδονται από την ADACOM, όπως ορίζεται στο παρόν έγγραφο, είναι εγκεκριμένες σύμφωνα με τον Κανονισμό eIDAS.

Οι Χρονοσφραγίδες θα χρησιμοποιούνται μόνο στο βαθμό που η χρήση τους είναι σύμφωνη με το εφαρμοστέο δίκαιο και εντός των ορίων και του περιεχομένου που καθορίζονται στο παρόν έγγραφο. Οποιαδήποτε χρήση εκτός των ορίων αυτών ή για παράνομους σκοπούς ή αντίθετα προς το δημόσιο συμφέρον ή για σκοπούς που ενδέχεται να βλάψουν την επιχείρηση ή τη φήμη της ADACOM. Ενδεικτικά, η χρήση των Χρονοσφραγίδων απαγορεύεται για οποιονδήποτε από τους ακόλουθους σκοπούς:

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

3.4 Πολιτική Χρονοσφραγίδας και Δήλωση Πρακτικών Αρχής Χρονοσφραγίδας

3.4.1 Σκοπός

Το παρόν έγγραφο καθορίζει τις απαιτήσεις πολιτικής και ασφάλειας που σχετίζονται με τις πρακτικές λειτουργίας και διαχείρισης της ADACOM ως Αρχή Χρονοσφραγίδας (ΑΧ) για την έκδοση Εγκεκριμένων Χρονοσφραγίδων. Αυτές μπορούν να χρησιμοποιηθούν ως υποστήριξη ηλεκτρονικών υπογραφών ή σε οποιαδήποτε εφαρμογή που απαιτεί απόδειξη ότι υπήρχε ένα δεδομένο πριν από μία συγκεκριμένη χρονική στιγμή.

Το παρόν έγγραφο μπορεί να χρησιμοποιηθεί από ανεξάρτητες οντότητες ως βάση για να επιβεβαιωθεί ότι η ΑΧ της ADACOM αποτελεί αξιόπιστη οντότητα για την έκδοση Εγκεκριμένων Χρονοσφραγίδων σύμφωνα με τον Κανονισμό eIDAS.

Το παρόν έγγραφο είναι διαθέσιμο στο κοινό. Η διανομή αυτού του εγγράφου υπόκειται σε περιορισμούς όπως περιγράφεται στην ενότητα «Δικαιώματα πνευματικής ιδιοκτησίας».

3.4.2 Επίπεδο εξειδίκευσης

Το παρόν έγγραφο περιγράφει μόνο τους γενικούς κανόνες έκδοσης και διαχείρισης των ΔΧ. Λεπτομερής περιγραφή της υποδομής και συναφείς επιχειρησιακές διαδικασίες περιγράφονται σε πρόσθετα έγγραφα που δεν δημοσιοποιούνται. Αυτά τα πρόσθετα έγγραφα είναι διαθέσιμα μόνο σε εξουσιοδοτημένο προσωπικό της ADACOM και, κατ' εξαίρεση, σε ελεγκτές των Υπηρεσιών Χρονοσφραγίδας.

3.4.3 Προσέγγιση

Το παρόν έγγραφο καθορίζεται από τις ειδικές λεπτομέρειες του λειτουργικού περιβάλλοντος, της οργανωτικής δομής, των λειτουργικών διαδικασιών, των εγκαταστάσεων και του περιβάλλοντος πληροφορικής της AX ADACOM.

4. Πολιτικές Χρονοσφραγίδας

4.1 Επισκόπηση

Η παρούσα Πολιτική ορίζει το σύνολο των κανόνων που χρησιμοποιούνται κατά την έκδοση ενός ΔΧ και ρυθμίζει το επίπεδο ασφάλειας της AX ADACOM. Η AX ADACOM εκδίδει ΔΧ σύμφωνα με το πρότυπο ETSI EN 319 422.

Τα ΔΧ εκδίδονται με ακρίβεια ενός (1) δευτερόλεπτου.

Οι Χρονοσφραγίδες ζητούνται μέσω Hypertext Transfer Protocol (HTTP), όπως περιγράφεται στο RFC 3161.

4.2 Αναγνώριση

Το Αναγνωριστικό Αντικειμένου (OID) της Πολιτικής Πιστοποιητικού και Δήλωσης Πρακτικών Πιστοποίησης για Υπηρεσίες Εγκεκριμένης Χρονοσφραγίδας της ADACOM είναι 1.3.6.1.4.1.15976.1.1.3:

| | |
|-------------------------|--|
| 1.3.6.1.4.1.15976 | Αναγνωριστικό Αντικειμένου (OID) της ADACOM, καταχωρημένο στο IANA |
| 1.3.6.1.4.1.15976.1 | Πάροχος Υπηρεσιών Πιστοποίησης |
| 1.3.6.1.4.1.15976.1.1 | Πολιτικές Εγκεκριμένου Πιστοποιητικού |
| 1.3.6.1.4.1.15976.1.1.3 | Υπηρεσίες Εγκεκριμένων Σφραγίδων |

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

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

4.3 Κοινότητα Χρηστών και Εφαρμογή

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

Η ADACOM δεν παρέχει δημόσιες Υπηρεσίες Χρονοσφραγίδας.

4.4 Συμμόρφωση

Η AX της ADACOM χρησιμοποιεί το αναγνωριστικό στο ΔΧ όπως αναφέρεται στην παράγραφο 5.2 «Αναγνώριση».

Η AX της ADACOM διασφαλίζει τη συμμόρφωση των παρεχόμενων υπηρεσιών με τους κανονισμούς που ορίζονται στην ενότητα 6.1 «Υποχρεώσεις AX» και διασφαλίζει την αξιοπιστία των μηχανισμών ελέγχου που περιγράφονται στην ενότητα 7 «Πρακτικές AX».

5. Υποχρεώσεις και Ευθύνη

5.1 Υποχρεώσεις Αρχής Χρονοσφραγίδας

5.1.1 Γενικές Υποχρεώσεις

Το παρόν κεφάλαιο περιλαμβάνει, άμεσα ή με παραπομπή, όλες τις υποχρεώσεις, εγγυήσεις και ευθύνες της ΑΧ της ADACOM, των Συνδρομητών της και των χρηστών των ΔΧ (Συνδρομητές και Βασιζόμενα Μέρη). Αυτές οι υποχρεώσεις και ευθύνες ρυθμίζονται από συμφωνίες αποδεκτές από όλα τα μέρη.

Η ADACOM έχει θέσει σε λειτουργία την ΑΧ ADACOM και αναλαμβάνει την ευθύνη ότι εφαρμόζονται οι απαιτήσεις της ενότητας 7 «Πρακτικές ΑΧ» του παρόντος εγγράφου - καθώς και οι διατάξεις του eIDAS, όπως ισχύουν κατά την ισχύουσα Πολιτική Πιστοποίησης & Δήλωση Πρακτικών Πιστοποίησης για Υπηρεσίες Χρονοσφραγίδας της ADACOM.

Οι συμφωνίες της ADACOM με Συνδρομητές και Βασιζόμενα Μέρη περιγράφουν αμοιβαίες υποχρεώσεις και ευθύνες, συμπεριλαμβανομένων και οικονομικών υποχρεώσεων. Η Πολιτική Πιστοποίησης & Δήλωση Πρακτικών Πιστοποίησης για Υπηρεσίες Χρονοσφραγίδας της ADACOM αποτελούν αναπόσπαστο μέρος αυτών των συμφωνιών.

5.1.2 Υποχρεώσεις Αρχής Χρονοσφραγίδας προς Συνδρομητές

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

Η ADACOM αναλαμβάνει τις ακόλουθες υποχρεώσεις προς τους Συνδρομητές:

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

5.2 Υποχρεώσεις Συνδρομητών

Οι Συνδρομητές θα πρέπει να επαληθεύσουν τις υπογραφές που δημιουργήθηκαν από την ΑΧ ADACOM στο ΔΧ.

Ο Συνδρομητής των Υπηρεσιών Χρονοσφραγίδας πρέπει:

- α. να χρησιμοποιεί ασφαλείς κρυπτογραφικές λειτουργίες για να αιτηθεί χρονοσφραγίδες,

β. να ελέγχει ότι:

- το πιστοποιητικό της Μονάδας Χρονοσφραγίδας είναι της ADACOM,
- το πιστοποιητικό της Μονάδας Χρονοσφραγίδας δεν έχει ανακληθεί,
- εμφανίζεται η σήμανση ότι είναι εγκεκριμένο,
- το πιστοποιητικό της εκδότριας Αρχής Χρονοσφραγίδας δεν έχει ανακληθεί.

Επιπλέον υποχρεώσεις των Συνδρομητών δύναται να ορίζονται και στους Όρους και Προϋποθέσεις για Εγκεκριμένες Υπηρεσίες Εμπιστοσύνης της ADACOM.

5.3 Υποχρεώσεις Βασιζόμενων Μερών

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

Τα Βασιζόμενα μέρη των Υπηρεσιών Χρονοσφραγίδας πρέπει να ελέγχουν ότι:

- το πιστοποιητικό της Μονάδας Χρονοσφραγίδας είναι της ADACOM,
- το πιστοποιητικό της Μονάδας Χρονοσφραγίδας δεν έχει ανακληθεί,
- εμφανίζεται η σήμανση ότι είναι εγκεκριμένο,
- το πιστοποιητικό της εκδότριας Αρχής Χρονοσφραγίδας δεν έχει ανακληθεί.

Τα Βασιζόμενα Μέρη θα πρέπει να λαμβάνουν υπόψη τυχόν περιορισμούς στη χρήση της χρονοσφραγίδας που υποδεικνύεται από το παρόν έγγραφο. Εάν η επαλήθευση πραγματοποιηθεί μετά τη λήξη της περιόδου ισχύος του πιστοποιητικού, το Βασιζόμενο Μέρος θα πρέπει να ακολουθήσει τις οδηγίες που αναφέρονται στο Παράρτημα Δ΄ του ETSI EN 319 421.

Τα Βασιζόμενα Μέρη θα πρέπει να χρησιμοποιήσουν τον Κατάλογο Εμπιστοσύνης για να διαπιστώσουν αν η MX και η χρονοσφραγίδα είναι εγκεκριμένες. Εάν το δημόσιο κλειδί της MX παρατίθεται στον Κατάλογο Εμπιστοσύνης και η υπηρεσία που αντιπροσωπεύει είναι εγκεκριμένη υπηρεσία χρονοσφραγίδας, τότε οι χρονοσφραγίδες που εκδίδονται από αυτήν την MX μπορούν να θεωρηθούν εγκεκριμένες. Το qcStatement "esi4-qtstStatement-1" όπως ορίζεται στο ETSI EN 319 422 [4], παράγραφος 9.1, χρησιμοποιείται ως ένδειξη ότι η χρονοσφραγίδα είναι εγκεκριμένη.

5.4 Ευθύνη

Η ευθύνη της ADACOM που ενεργεί ως ΕΠΥΧ και των Συνδρομητών και Βασιζόμενων Μερών που συνδέονται με τις υπηρεσίες καθορίζεται στη σχετική συμφωνία ή όπως προβλέπεται στην ισχύουσα νομοθεσία.

Η ADACOM είναι υπεύθυνη για τυχόν ζημίες που υφίστανται άμεσα, εκ προθέσεως ή εξ αμελείας, σε οποιοδήποτε φυσικό ή νομικό πρόσωπο, λόγω μη συμμόρφωσης με τις υποχρεώσεις που ορίζονται στο παρόν έγγραφο και στον Κανονισμό (ΕΕ) Αρ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 23ης Ιουλίου 2014 (eIDAS).

Οι Όροι και Προϋποθέσεις της ADACOM για Εγκεκριμένες Υπηρεσίες Εμπιστοσύνης περιορίζουν την ευθύνη της ADACOM. Οι περιορισμοί ευθύνης περιλαμβάνουν αποκλεισμό έμμεσων, ειδικών, παρεπόμενων και επακόλουθων ζημιών. Περιλαμβάνουν επίσης ως ανώτατο όριο ευθύνης όσον αφορά τη συνολική ευθύνη της ADACOM προς οποιοδήποτε πρόσωπο σχετικά με τις Υπηρεσίες Χρονοσφραγίδας, η οποία περιορίζεται σε ποσό που δεν υπερβαίνει το ποσό της αντίστοιχης σύμβασης για την υπηρεσία χρονοσφραγίδας, το οποίο υπολογίζεται κατ' αναλογία και ως συνολικό μέγιστο ποσό των 500.000 ευρώ, ανεξάρτητα από τη φύση της ευθύνης και την κατηγορία, το ποσό ή την έκταση οποιασδήποτε ζημίας. Οι περιορισμοί ευθύνης είναι οι ίδιοι ανεξάρτητα από τον αριθμό των Χρονοσφραγίδων ή των αξιώσεων που σχετίζονται με αυτές.

Η AX της ADACOM δεν αποδέχεται οποιαδήποτε ευθύνη σχετικά με τη χρήση που γίνεται με τα ΔΧ που παραδίδει και υπογράφει.

6. Πρακτικές Αρχής Χρονοσφραγίδας

Η ΑΧ της ADACOM θα εφαρμόσει ελέγχους που ικανοποιούν τις απαιτήσεις των προτύπων ETSI EN 319 421 και ETSI EN 319 422.

6.1 Δηλώσεις Πρακτικών και Κοινοποίησης

6.1.1 Δήλωση Πρακτικών Αρχής Χρονοσφραγίδας

Η Πολιτική Πιστοποίησης & Δήλωση Πρακτικών Πιστοποίησης για υπηρεσίες Χρονοσφραγίδας της ADACOM καθορίζει τους γενικούς κανόνες σχετικά με τις τεχνικές, οργανωτικές και διαδικαστικές απαιτήσεις λειτουργίας της ΑΧ της ADACOM.

Η ADACOM διασφαλίζει ότι τα αρχεία καταγραφής συμβάντων της ΑΧ διατηρούνται για τουλάχιστον επτά (7) χρόνια μετά την παρουσία αυτών των συμβάντων. Τα πιστοποιητικά Χρονοσφραγίδας ισχύουν για δέκα (10) χρόνια, αλλά απαιτούν ανανέωση κάθε χρόνο. Ως εκ τούτου, τα αρχεία καταγραφής για τη Χρονοσφραγίδα διατηρούνται για ένα (1) έτος μετά τη λήξη του Πιστοποιητικού της Μονάδας Χρονοσφραγίδας.

Διεξάγεται τακτικά εκτίμηση κινδύνου προκειμένου να αξιολογούνται τα περιουσιακά στοιχεία της επιχείρησης και οι απειλές αυτών των περιουσιακών στοιχείων, προκειμένου να προσδιοριστούν οι αναγκαίοι έλεγχοι ασφάλειας και οι επιχειρησιακές διαδικασίες που έχουν ληφθεί.

Οι όροι και οι προϋποθέσεις σχετικά με τη χρήση των υπηρεσιών χρονοσφραγίδας της ADACOM, όπως περιγράφονται στους Όρους και Προϋποθέσεις για Εγκεκριμένες Υπηρεσίες Εμπιστοσύνης της ADACOM, κοινοποιούνται και τίθενται στη διάθεση όλων των Συνδρομητών και Βασιζόμενων Μερών, όπως ορίζεται στην παράγραφο 7.1.2 του παρόντος εγγράφου.

Η Αρχή Διαχείρισης Πολιτικής της ADACOM είναι υπεύθυνη για τη διατήρηση και έγκριση όλων των πολιτικών και πρακτικών ΥΔΚ της ADACOM σύμφωνα με τους όρους της παραγράφου 1.1 «Διαχείριση Πολιτικής» του παρόντος εγγράφου. Η διοίκηση της ADACOM έχει την ευθύνη να διασφαλίσει ότι οι πρακτικές εφαρμόζονται σωστά.

6.1.2 Δήλωση Γνωστοποίησης Αρχής Χρονοσφραγίδας

Η ΑΧ της ADACOM κοινοποιεί σε όλους τους Συνδρομητές και τα πιθανά Βασιζόμενα Μέρη τους όρους και προϋποθέσεις σχετικά με τη χρήση των Υπηρεσιών Χρονοσφραγίδας της ADACOM.

Η Δήλωση Γνωστοποίησης της ΑΧ της ADACOM συμμορφώνεται με τις απαιτήσεις του ETSI EN 319 421 και συμπεριλαμβάνεται contains δηλώσεις σχετικά με τις πρακτικές της ΑΧ, καθώς επίσης και τα δικαιώματα και υποχρεώσεις των Συνδρομητών και Βασιζόμενων Μερών κατά τρόπο απλουστευμένο και περιεκτικό.

Κάποια στοιχεία της Δήλωσης Γνωστοποίησης της ΑΧ ADACOM αναφέρονται παρακάτω:

- Κάθε ΔΧ που εκδίδεται από την ΑΧ της ADACOM περιλαμβάνει το αναγνωριστικό πολιτικής που ορίζεται στην ενότητα 5.2 του παρόντος εγγράφου.
- Οι λειτουργίες κρυπτογραφικού κατακερματισμού (hashing) που χρησιμοποιούνται στη διαδικασία Χρονοσφραγίδας είναι σύμφωνες με τις κανονιστικές απαιτήσεις SHA-256 and SHA-512.
- Η αναμενόμενη περίοδος ισχύος της ΜΧ της ADACOM είναι μέχρι δέκα (10) έτη.
- Η ακρίβεια του χρόνου, που παρέχεται σε ένα ΔΧ ρυθμίζεται στην ενότητα 5.1 του παρόντος εγγράφου.
- Οι περιορισμοί στην εφαρμογή που σχετίζονται με το σύστημα της ΑΧ έχουν καθοριστεί στην ενότητα 5.3 του παρόντος εγγράφου.
- Η επαλήθευση του ΔΧ πρέπει να γίνεται με τη χρήση του κατάλληλου λογισμικού.
- Οι υποχρεώσεις των Συνδρομητών περιγράφονται στην ενότητα 6.2 του παρόντος εγγράφου.
- Οι υποχρεώσεις των Συνδρομητών περιγράφονται στην ενότητα 6.3 του παρόντος εγγράφου.

- Η ADACOM τηρεί ασφαλή αρχεία που σχετικά με τη λειτουργία της AX της ADACOM.
- Η ADACOM δύναται να χρεώσει για τις υπηρεσίες που παρέχονται από την AX της ADACOM.

6.2 Κύκλος Ζωής Διαχείρισης Κλειδιού

6.2.1 Δημιουργία Κλειδιού Αρχής Χρονοσφραγίδας

Προσωπικό σε αξιόπιστους ρόλους υπό διπλό έλεγχο εκτελεί την δημιουργία των κλειδιών υπογραφής της MX σε ένα φυσικά ασφαλές περιβάλλον. Το προσωπικό που είναι εξουσιοδοτημένο να εκτελεί τη λειτουργία αυτή περιορίζεται σε εκείνα τα πρόσωπα που απαιτούνται σύμφωνα με τις πρακτικές της AX.

Η δημιουργία των κλειδιών υπογραφής της MX πραγματοποιείται μέσα σε ασφαλή κρυπτογραφικές συσκευές, οι οποίες πληρούν τις προϋποθέσεις που ορίζονται στο FIPS 140-2 level 3.

Τα ζεύγη κλειδιών δημιουργούνται χρησιμοποιώντας ασφαλείς αλγόριθμους και παραμέτρους που βασίζονται σε τρέχοντα ερευνητικά και βιομηχανικά πρότυπα σύμφωνα με τις συστάσεις του ETSI TS 319 312.

Οι δραστηριότητες που εκτελούνται σε κάθε δημιουργία κλειδιού καταγράφονται, χρονολογούνται και υπογράφονται από όλα τα εμπλεκόμενα άτομα. Αυτά τα αρχεία διατηρούνται για σκοπούς επιθεώρησης και παρακολούθησης για χρονικό διάστημα που κρίνεται κατάλληλο από τη Διοίκηση της ADACOM.

6.2.2 Προστασία Ιδιωτικού Κλειδιού MX

Η ADACOM λαμβάνει απαραίτητα μέτρα ώστε να βεβαιωθεί ότι τα ιδιωτικά κλειδιά της MX παραμένουν εμπιστευτικά και διατηρούν την ακεραιότητά τους.

Τα ιδιωτικά κλειδιά της MX αποθηκεύονται σε μια ασφαλή Μονάδα Ασφάλειας Υλικού (HSM) για την εκτέλεση λειτουργιών υπογραφής κλειδιών, οι οποίες συμμορφώνονται τουλάχιστον με το FIPS 140-2 επίπεδο 3 ή ισοδύναμο EAL 4+ ή υψηλότερο σύμφωνα με τις προδιαγραφές ISO / IEC 15408. Υπάρχουν ειδικοί έλεγχοι για να διασφαλιστεί ότι το υλικό δεν έχει αλλοιωθεί και λειτουργεί σωστά.

Τα ιδιωτικά κλειδιά της MX δεν μπορούν να εξαχθούν σε οποιαδήποτε μορφή και δεν είναι προσβάσιμα εκτός της Μονάδας Ασφάλειας Υλικού.

Η ADACOM δημιουργεί αντίγραφα ασφαλείας των ιδιωτικών κλειδιών της MX, για σκοπούς ανάκτησης ρουτίνας και αποκατάστασης καταστροφών. Τέτοια κλειδιά αποθηκεύονται σε κρυπτογραφημένη μορφή μέσα σε κρυπτογραφικές μονάδες υλικού. Οι κρυπτογραφικές μονάδες που χρησιμοποιούνται για την αποθήκευση ιδιωτικών κλειδιών πληρούν τις απαιτήσεις της παρούσας ΔΠΠ. Τα ιδιωτικά κλειδιά αντιγράφονται σε κρυπτογραφικές μονάδες εφεδρικού υλικού. Η επαναφορά των αντιγράφων ασφαλείας των κλειδιών της MX απαιτεί διπλό έλεγχο σε ένα φυσικά ασφαλές περιβάλλον.

6.2.3 Διανομή Δημοσίου Κλειδιού MX

Τα Δημόσια κλειδιά της MX της διατίθενται σε Ψηφιακό Πιστοποιητικό.

Τα Πιστοποιητικά της MX της ADACOM διατίθενται για ασφαλή μεταφόρτωση μέσω του Αποθηκευτικού χώρου της ADACOM: <https://pki.adacom.com/repository>. Είναι επίσης διαθέσιμα στον κατάλογο εμπιστοσύνης παρόχων υπηρεσιών πιστοποίησης (Trusted List of Certification Service Providers) της Ευρωπαϊκής Ένωσης μέσω της Εθνικής Εποπτικής Αρχής (Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων).

6.2.4 Επαναδημιουργία κλειδιού ΜΧ

Η περίοδος λειτουργίας για τα ζεύγη κλειδιών της ΜΧ μπορεί να οριστεί ρυθμίζοντας μια περίοδο χρήσης ιδιωτικού κλειδιού στο πιστοποιητικό δημόσιου κλειδιού της ΜΧ.

Τα ΔΧ της ADACOM υπογράφονται με πιστοποιητικά της ΜΧ της ADACOM ισχύος δέκα (10) ετών. Τα πιστοποιητικά της ΜΧ της ADACOM ισχύος δέκα (10) ετών χρησιμοποιούνται μόνο για την υπογραφή ΔΧ κατά τη διάρκεια περιόδου χρήσης ενός (1) έτους.

Η διαδικασία επαναδημιουργίας της ΜΧ της ADACOM εκτελείται μετά τη λήξη της περιόδου χρήσης (1 έτους) του πιστοποιητικού της ΜΧ. Τα δημόσια κλειδιά αρχειοθετούνται για περίοδο τουλάχιστον δέκα (10) ετών από την ημερομηνία λήξης του πιστοποιητικού.

6.2.5 Τέλος Κύκλου Ζωής Κλειδιού ΜΧ

Η ΑΧ της ADACOM TSA διασφαλίζει ότι τα ιδιωτικά κλειδιά υπογραφής της ΜΧ δεν χρησιμοποιούνται πέρα από το τέλος του κύκλου ζωής τους. Ειδικότερα, έχουν εφαρμόζονται λειτουργικές και τεχνικές διαδικασίες για να εξασφαλιστεί ότι ένα νέο κλειδί θα τεθεί σε εφαρμογή όταν λήξει η περίοδος χρήσης του κλειδιού της ΜΧ και ότι τα ιδιωτικά κλειδιά της ΜΧ ή οποιοδήποτε μέρος τους, συμπεριλαμβανομένων τυχόν αντιγράφων, καταστρέφονται κατά τρόπο ώστε να μην μπορεί να ανακτηθεί το ιδιωτικό κλειδί.

Το σύστημα δημιουργίας ΔΧ θα απορρίπτει κάθε απόπειρα έκδοσης ενός ΔΧ, εάν έχει λήξει το ιδιωτικό κλειδί υπογραφής ή εάν έχει λήξει η περίοδος χρήσης του ιδιωτικού κλειδιού υπογραφής.

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

Η ADACOM εξασφαλίζει την ασφάλεια της Μονάδας Ασφάλειας Υλικού (HSM) καθ' όλη τη διάρκεια του κύκλου ζωής της.

Η ADACOM έχει διαδικασίες για να εξασφαλίσει ότι:

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

6.3 Χρονοσφράγιση

6.3.1 Διακριτικό Χρονοσφραγίδας (ΔΧ)

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

- αναπαράσταση του δεδομένου που φέρει τη χρονοσφραγίδα όπως παρασχέθηκε από τον αιτούντα
- έναν μοναδικό αύξοντα αριθμό που μπορεί να χρησιμοποιηθεί τόσο για την παραγγελία του ΔΧ όσο και για την αναγνώριση του συγκεκριμένου ΔΧ
- ένα μοναδικό αναγνωριστικό της πολιτικής όπως περιγράφεται στην ενότητα 5.2 του παρόντος εγγράφου
- μια ηλεκτρονική υπογραφή που παράγεται χρησιμοποιώντας ένα κλειδί που χρησιμοποιείται αποκλειστικά για Χρονοσφράγιση
- αναγνωριστικό για την ΑΧ και την ΜΧ
- τιμή ημερομηνίας και ώρας που μπορεί να ανιχνευθεί στην πραγματική τιμή χρόνου UTC

- αλγόριθμος υπογραφής που χρησιμοποιείται στο ΔΧ όπως ορίζεται στην ενότητα 7.2 του παρόντος εγγράφου.

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

6.3.2 Συγχρονισμός Ρολογιού με UTC

Η ΑΧ της ADACOM εξασφαλίζει ότι η ώρα της συγχρονίζεται με το UTC εντός της δηλωμένης ακρίβειας με πολλαπλές ανεξάρτητες πηγές ώρας. Η ΑΧ της ADACOM ενσωματώνει το χρόνο στο ΔΧ με την ακρίβεια που περιγράφεται στην ενότητα 5.1 του παρόντος εγγράφου.

Τα αρχεία ελέγχου και βαθμονόμησης του συγχρονισμού τηρούνται από την ADACOM. Η ΑΧ της ADACOM διασφαλίζει ότι εάν ο χρόνος που θα υποδεικνύεται σε ένα ΔΧ μετακινείται εκτός του συγχρονισμού με το UTC, αυτό θα ανιχνευθεί. Εάν το ρολόι της ΜΧ παρασυρθεί εκτός της δηλωμένης ακρίβειας και ο επαναβαθμονόμος αποτύχει, η ΑΧ δεν θα εκδώσει χρονοσφραγίδες μέχρι να αποκατασταθεί ο σωστός χρόνος.

Η ADACOM εφαρμόζει ελέγχους ασφαλείας που εμποδίζουν τη μη εξουσιοδοτημένη λειτουργία, με σκοπό τη βαθμονόμηση της ώρας εκτός λειτουργίας.

6.3.3 Διαδικασία Χειρισμού Άλματος Δευτερολέπτου

Το άλμα δευτερολέπτου είναι μια προσαρμογή στο UTC παρακάμπτοντας ή προσθέτοντας ένα επιπλέον δευτερόλεπτο στο τελευταίο δευτερόλεπτο ενός μήνα UTC. Πρώτη προτίμηση δίνεται στο τέλος του Δεκεμβρίου και Ιουνίου και δεύτερη προτίμηση δίνεται στο τέλος του Μαρτίου και Σεπτεμβρίου.

Η ADACOM παρακολουθεί ότι ο συγχρονισμός διατηρείται όταν εμφανιστεί ένα άλμα δευτερολέπτου.

6.4 Διαχείριση και Λειτουργία Αρχής Χρονοσφραγίδας

6.4.1 Διαχείριση Ασφάλειας

Η ΑΧ της ADACOM TSA διασφαλίζει ότι εφαρμόζονται διοικητικές και διαχειριστικές διαδικασίες που είναι επαρκείς και ανταποκρίνονται στις αναγνωρισμένες βέλτιστες πρακτικές.

Η ADACOM εκτελεί όλες τις λειτουργίες της ΑΧ χρησιμοποιώντας αξιόπιστα συστήματα που πληρούν τις απαιτήσεις του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (ISMS) της.

6.4.2 Ταξινόμηση και Διαχείριση Περιουσιακών Στοιχείων

Η ADACOM διατηρεί απογραφή όλων των περιουσιακών στοιχείων και αναθέτει ταξινόμηση για τις απαιτήσεις προστασίας για τα εν λόγω στοιχεία σύμφωνα με την ανάλυση κινδύνου.

6.4.3 Ασφάλεια Προσωπικού

Η ADACOM διατηρεί τους κατάλληλους ελέγχους προσωπικού που πληρούν τις βέλτιστες πρακτικές ασφαλείας και απαιτήσεις των σχετικών προτύπων.

Το διευθυντικό και το επιχειρησιακό προσωπικό διαθέτει τις κατάλληλες δεξιότητες και γνώσεις σχετικά με τη Χρονοσφραγίση, τις ψηφιακές υπογραφές και τις Υπηρεσίες Εμπιστοσύνης, καθώς και τις διαδικασίες ασφαλείας για το προσωπικό με αρμοδιότητες στον τομέα της ασφάλειας, την ασφάλεια των πληροφοριών και την αξιολόγηση των κινδύνων.

Τα Έμπιστα Πρόσωπα περιλαμβάνουν όλους τους υπαλλήλους που έχουν πρόσβαση ή ελέγχουν τις κρυπτογραφικές διαδικασίες. Τα Έμπιστα Πρόσωπα περιλαμβάνουν, αλλά δεν περιορίζονται σε:

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

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.

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.

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.

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.

6.4.4 Φυσικοί και Περιβαλλοντική Ασφάλεια

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. Η Πολιτική Φυσικής Ασφάλειας της ADACOM περιέχει ευαίσθητες πληροφορίες για την ασφάλεια και διατίθεται μόνο κατόπιν συμφωνίας με την ADACOM.

Οι λειτουργίες των ΑΠ και ΑΧ 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

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 ασφαλείας. 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 ασφαλείας 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 ασφαλείας.

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 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 αφαιρούμενα μέσα αποθήκευσης (ψηφιακά και έντυπα), τα οποία περιέχουν ευαίσθητα δεδομένα απλού κειμένου σχετικά με τις λειτουργίες της.

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

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.

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).

Τα ευαίσθητα έγγραφα και υλικά περνάνε σε καταστροφή 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.

6.4.5 Επιχειρησιακή Διαχείριση

Η AX της ADACOM TSA διασφαλίζει ότι οι διαδικασίες και η υποδομή συμμορφώνονται με την επιχειρησιακή διαχείριση, τις απαιτήσεις διαδικαστικής ασφάλειας, τη διαχείριση πρόσβασης στο σύστημα, την αξιόπιστη εγκατάσταση και συντήρηση συστημάτων, τη διαχείριση της συνέχειας της επιχείρησης και την διαχείριση περιστατικών όπως ορίζεται στο ETSI EN 319 421.

Οι διαδικασίες επιχειρησιακής διαχείρισης για την AX της ADACOM ενσωματώνονται στις γενικές εσωτερικές διαδικασίες διαχείρισης λειτουργιών της ADACOM.

6.4.6 Εγκατάσταση και συντήρηση αξιόπιστων συστημάτων

Η ADACOM διασφαλίζει ότι τα συστήματα που διατηρούν λογισμικό της AX και αρχεία δεδομένων είναι αξιόπιστα συστήματα, ασφαλή από μη εξουσιοδοτημένη πρόσβαση και τροποποίηση. Επιπλέον, η ADACOM περιορίζει την πρόσβαση σε διακομιστές παραγωγής σε άτομα που έχουν έγκυρο επιχειρηματικό λόγο για τέτοια πρόσβαση. Οι χρήστες γενικών εφαρμογών δεν διαθέτουν λογαριασμούς στους διακομιστές παραγωγής.

6.4.7 Έκθεση σε κίνδυνο των Υπηρεσιών της Αρχής Χρονοσφραγίδας

Σε περίπτωση έκθεσης σε κίνδυνο της λειτουργία της ΜΧ (π.χ. μείζονος έκθεσης σε κίνδυνο του κλειδιού της ΜΧ), πιθανολογούμενης έκθεσης σε κίνδυνο ή απώλειας βαθμονόμησης, η ΜΧ δεν θα εκδίδει χρονοσφραγίδες μέχρις ότου ληφθούν μέτρα για την αποκατάστασή της. Σε περίπτωση ή πιθανολογούμενης έκθεσης σε κίνδυνο ή απώλειας βαθμονόμησης κατά την έκδοση χρονοσφραγίδων, η ADACOM θα θέσει στη διάθεση όλων των Συνδρομητών και των Βασιζόμενων Μερών περιγραφή του συμβάντος.

Σε περίπτωση μείζονος έκθεσης σε κίνδυνο της λειτουργίας της ΜΧ, η ADACOM θα θέσει στη διάθεση όλων των Συνδρομητών και Βασιζόμενων Μερών πληροφορίες που μπορούν να χρησιμοποιηθούν για τον προσδιορισμό των χρονοσφραγίδων που ενδέχεται να επηρεάστηκαν, εκτός εάν αυτό παραβιάζει το απόρρητο των χρηστών της ΜΧ ή την ασφάλεια των υπηρεσιών της ΜΧ.

6.4.8 Τερματισμός Αρχής Χρονοσφραγίδας

Η λειτουργία της ΑΧ τερματίζεται με:

- απόφαση του Διοικητικού Συμβουλίου ή του Διευθύνοντα Συμβούλου της ADACOM
- απόφαση της αρχής που ασκεί την εποπτεία της παροχής της υπηρεσίας
- δικαστική απόφαση
- εκκαθάριση ή τον 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 ΑΧ της ADACOM, η ADACOM καταβάλλει εύλογες από εμπορικής άποψης προσπάθειες ώστε να ειδοποιήσει τους Συνδρομητές και τα Βασιζόμενα Μέρη πριν από τη διακοπή λειτουργίας της ΑΧ.

Η ΑΧ της ADACOM ανακαλεί τα πιστοποιητικά των ΜΧ όταν τερματίζει τις υπηρεσίες της.

6.4.9 Συμμόρφωση με τη νομοθεσία

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

- του Κανονισμού 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].
- του Γενικού Κανονισμού για την Προστασία των Δεδομένων (ΓΚΠΔ/GDPR) [Κανονισμός (ΕΕ) αριθ. 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών και την κατάργηση της οδηγίας 95/46/ΕΚ] καθώς και της εθνικής νομοθεσίας 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 EN 319 421 Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) - Απαιτήσεις πολιτικής και ασφάλειας για παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν Χρονοσφραγίδες.
- e. ETSI EN 319 422 Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) – Πρωτόκολλο Χρονοσφραγίδας και Προφίλ Διακριτικών Χρονοσφραγίδας

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

6.4.10 Καταγραφή πληροφοριών σχετικά με τη Λειτουργία των Υπηρεσιών Χρονοσφραγίδας

Η ΑΧ της ADACOM διασφαλίζει ότι όλες οι σχετικές πληροφορίες σχετικά με τις λειτουργίες των Υπηρεσιών Χρονοσφραγίδας της ADACOM καταγράφονται για καθορισμένο χρονικό διάστημα, ιδίως για την παροχή αποδεικτικών στοιχείων για σκοπούς δικαστικών διαδικασιών.

Η ADACOM διατηρεί αρχείο για όλες τις πληροφορίες σχετικά με τη λειτουργία την ΑΧ της ADACOM για περίοδο επτά (7) ετών.

Η ΑΧ της ADACOM τηρεί αρχεία για:

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

7. Άλλα Επιχειρησιακά και Νομικά Θέματα

7.1 Οικονομική υπευθυνότητα

Η ΑΧ της ADACOM εξασφαλίζει ότι η επιχείρησή της είναι αξιόπιστη, όπως απαιτείται στο ETSI EN 319 421. Η ADACOM έχει τη χρηματοοικονομική σταθερότητα και τους πόρους που απαιτούνται για να λειτουργήσει σύμφωνα με την τρέχουσα Πολιτική Πιστοποίησης & Δήλωση Πρακτικών Πιστοποίησης.

7.2 Ισχύουσες συμφωνίες, ΠΠ, ΔΠΠ

Σχετικές συμφωνίες, πολιτικές και δηλώσεις πρακτικών είναι:

- Η Πολιτική Πιστοποιητικού και Δήλωση Πρακτικών Πιστοποίησης για Εγκεκριμένες Υπηρεσίες Χρονοσφραγίδας της ADACOM
- Όροι και Προϋποθέσεις Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης της ADACOM.

Οι τελευταίες εκδόσεις όλων των εφαρμοστέων εγγράφων είναι διαθέσιμες στον [Αποθηκευτικό χώρο](#) της ADACOM.

7.3 Πολιτική Απορρήτου

Η ADACOM επεξεργάζεται προσωπικά δεδομένα σύμφωνα με την ισχύουσα νομοθεσία για την προστασία τους. Για περισσότερες λεπτομέρειες, παρακαλούμε να ανατρέξετε στη [Δήλωση Απορρήτου](#) της ADACOM.

7.4 Πολιτική επιστροφής χρημάτων

Η ADACOM καταβάλλει προσπάθειες ώστε να διασφαλίζει το μέγιστο επίπεδο ποιότητας των υπηρεσιών της. Σε περίπτωση που η πώληση της Χρονοσφραγίδας πραγματοποιηθεί μέσω διαδικτύου ή τηλεφωνικά, ο Συνδρομητής έχει το δικαίωμα να υπαναχωρήσει από την παραγγελία. Η άσκηση του εν λόγω δικαιώματος γίνεται γραπτώς από τον Συνδρομητή προς την ADACOM, μέσω της αποστολής μηνύματος ηλεκτρονικού ταχυδρομείου στη διεύθυνση qc@adacom.com.

7.5 Άδειες Αποθηκευτικού Χώρου, Σήματα Αξιοπιστίας και Έλεγχος

Οι Υπηρεσίες Εμπιστοσύνης της ADACOM για τις Εγκεκριμένες Ηλεκτρονικές Υπογραφές και τις Εγκεκριμένες Ηλεκτρονικές Σφραγίδες είναι καταχωρημένες στο [Μητρώο παρόχων υπηρεσιών εμπιστοσύνης](#) της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ) και στη σχετική [Ευρωπαϊκή Λίστα Εμπιστοσύνης](#).

Τα συμπεράσματα των ελέγχων ή τα πιστοποιητικά, τα οποία βασίζονται σε αποτελέσματα ελέγχου αξιολόγησης της συμμόρφωσης που διενεργείται σύμφωνα με τον κανονισμό eIDAS, την αντίστοιχη νομοθεσία και τα πρότυπα, δημοσιεύονται στον [Αποθηκευτικό χώρο](#) της ADACOM.

7.6 Εφαρμοστέο δίκαιο, Καταγγελίες, Επίλυση διαφορών

Τυχόν διαφορές που σχετίζονται με τις υπηρεσίες εμπιστοσύνης που παρέχονται από την ADACOM, διέπονται από τη νομοθεσία της Ελλάδας. Ο Συνδρομητής πρέπει να ενημερώσει την ADACOM σχετικά με οποιαδήποτε αξίωσή του, το αργότερο εντός τριάντα (30) ημερολογιακών ημερών από τη θεμελίωση της αξίωσης, εκτός εάν προβλέπεται διαφορετικά από τον νόμο. Εάν η διαφορά δεν επιλυθεί εντός εξήντα (60) ημερών μετά την αρχική ειδοποίηση, τότε οποιοδήποτε μέρος μπορεί να προσφύγει σε δικαστική επίλυση. Τα δικαστήρια της Αθήνας στην Ελλάδα έχουν αποκλειστική δικαιοδοσία και είναι αρμόδια για την επίλυση της εν λόγω διαφοράς.

8. Ορισμοί και συντομογραφίες

8.1 Ορισμοί

| Όρος | 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 βάση | Η αρχή πιστοποίησης η οποία βρίσκεται στο υψηλότερο επίπεδο εντός του τομέα του ΠΥΕ και η οποία χρησιμοποιείται για να υπογράψει ιεραρχικά υφιστάμενες ΑΠ. |
| Αποθηκευτικός χώρος ADACOM | Η βάση δεδομένων πιστοποιητικών της ADACOM και άλλες σχετικές πληροφορίες για την ADACOM που είναι προσβάσιμες στο διαδίκτυο. |
| Αρχή Διαχείρισης Πολιτικής (ΑΔΠ) | Ο οργανισμός εντός της ADACOM που είναι υπεύθυνος για την έκδοση της παρούσας πολιτικής. |
| Αρχή Πιστοποίησης (ΑΠ) | Οντότητα που έχει εξουσιοδοτηθεί να δημιουργήσει και να αναθέτει πιστοποιητικά. |

| | |
|--|---|
| Αρχή Χρονοσφραγίδας (ΑΧ) | Η Αρχή των Υπηρεσιών Χρονοσφραγίδας που εκδίδει Διακριτικά Χρονοσφραγίδας. |
| Βασιζόμενο Μέρος | Ένα φυσικό πρόσωπο ή οργανισμός που ενεργεί βασιζόμενος σε ένα πιστοποιητικό. |
| Δήλωση Γνωστοποίησης ΑΧ | Σύνολο δηλώσεων σχετικά με τις πολιτικές και τις πρακτικές μιας ΑΧ που απαιτούν ιδιαίτερη προσοχή ή κοινοποίηση σε Συνδρομητές και Βασιζόμενα Μέρη. |
| Δήλωση Πρακτικών ΑΧ | Δήλωση σχετικά με τις πρακτικές που εφαρμόζει η ΑΧ κατά την έκδοση Διακριτικών Χρονοσφραγίδας. |
| 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. |
| Διακριτικό Χρονοσφραγίδας (ΔΧ) | Αντικείμενο δεδομένων που δεσμεύει μια αναπαράσταση ενός δεδομένου σε μια συγκεκριμένη χρονική στιγμή, αποδεικνύοντας έτσι ότι το δεδομένο υπήρχε πριν από το συγκεκριμένο χρόνο. |
| Δικαιώματα Πνευματικής Ιδιοκτησίας | Δικαιώματα επί ενός ή περισσότερων από τα ακόλουθα: οποιοδήποτε δικαίωμα δημιουργού, δίπλωμα ευρεσιτεχνίας, εμπορικό μυστικό, εμπορικό σήμα, καθώς και κάθε άλλο δικαίωμα πνευματικής ιδιοκτησίας. |
| Εγκεκριμένη ηλεκτρονική χρονοσφραγίδα | Δεδομένα σε ηλεκτρονική μορφή τα οποία συνδέουν άλλα δεδομένα σε ηλεκτρονική μορφή με ένα συγκεκριμένο χρονικό σημείο, τεκμηριώνοντας ότι τα εν λόγω δεδομένα υπήρχαν κατά το χρονικό σημείο εκείνο, κατά τέτοιο τρόπο ώστε να αποκλείεται η δυνατότητα τροποποίησης των δεδομένων, βασίζεται σε χρονική πηγή ακρίβειας συνδεδεμένη με τη Συντονισμένη Παγκόσμια Ωρα και φέρει προηγμένη ηλεκτρονική υπογραφή ή σφραγίδα του Εγκεκριμένου Παρόχου Υπηρεσιών Εμπιστοσύνης. |
| 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. |
| 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. |
| 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 ασφαλείας του ιδιωτικού αυτού κλειδιού σε κίνδυνο. |
| Έλεγχος συμμόρφωσης | Ο περιοδικός έλεγχος στον οποίο υποβάλλεται ένα Κέντρο Επεξεργασίας, το Κέντρο Υπηρεσιών ή Πελάτης της υπηρεσίας Managed PKI ώστε να προσδιοριστεί η συμμόρφωσή του με τα Πρότυπα του STN που ισχύουν αντίστοιχα για τα ανωτέρω. |

| | |
|---|--|
| Εμπιστο 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. |
| Εξ αποστάσεως ΕΔΔΥ | Εγκεκριμένη Διάταξη Δημιουργίας Υπογραφής Εξ αποστάσεως που πληροί τις απαιτήσεις του Παραρτήματος II του Κανονισμού eIDAS |
| 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. |
| 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. |
| Κανονισμός 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. |
| Κατάλογος Εμπιστοσύνης | Κατάλογος με πληροφορίες σχετικά με τους εγκεκριμένους παρόχους υπηρεσιών εμπιστοσύνης στην ΕΕ, καθώς και πληροφορίες σχετικά με τις υπηρεσίες εμπιστοσύνης που παρέχουν. |
| Μονάδα Χρονοσφραγίδας (ΜΧ) | Σύνολο υλικού και λογισμικού που διαχειρίζεται ως μονάδα και έχει ένα κλειδί υπογραφής Διακριτικού Χρονοσφραγίδας ενεργό κάθε φορά. |
| Πιστοποιητικό | Πρόκειται για το δημόσιο κλειδί της TSA μαζί με ορισμένες άλλες πληροφορίες οι οποίες παραδίδονται μη παραποιημένες βάσει κρυπτογράφησης με το ιδιωτικό κλειδί της αρχής πιστοποίησης που το εξέδωσε. |
| 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. |
| Συνδρομητής | Μια οντότητα που υποβάλλει αίτηση για υπηρεσία Χρονοσφραγίδας και είναι νομικά δεσμευμένη ως προς οποιεσδήποτε υποχρεώσεις Συνδρομητή. |
| Συντονισμένη παγκόσμια ώρα (UTC) | Χρονική κλίμακα βασισμένη στο δευτερόλεπτο όπως ορίζεται στη Σύσταση ITU-R TF.460-5 |
| Σύστημα ΑΧ | Σύνθεση προϊόντων και εξαρτημάτων πληροφορικής που οργανώνονται για την υποστήριξη της παροχής υπηρεσιών Χρονοσφραγίδας |
| Υπηρεσία Εμπιστοσύνης | Πρόκειται για την ηλεκτρονική υπηρεσία για τα ακόλουθα: <ul style="list-style-type: none"> • τη δημιουργία, την εξακρίβωση και την επικύρωση ηλεκτρονικών υπογραφών/σφραγίδων· • τη δημιουργία, την εξακρίβωση και την επικύρωση χρονοσφραγίδων. |
| 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 του STN αποτελείται από |

| | |
|--|---|
| | συστήματα που συνεργάζονται για την παροχή και την υλοποίηση του STN. |
|--|---|

8.2 Συντομογραφίες

| Συντομογραφία | Έννοια |
|---------------|--|
| ΑΠ | Αρχή Πιστοποίησης |
| ΑΧ | Αρχή Χρονοσφραγίδας |
| ΠΠ | Πολιτική Πιστοποιητικού |
| ΔΠΠ | Δήλωση Πρακτικών Πιστοποίησης |
| ΔΧ | Διακριτικό Χρονοσφραγίδας |
| ΕΠΥΕ | Εγκεκριμένος Πάροχος Υπηρεσιών Εμπιστοσύνης |
| ΕΠΥΧ | Εγκεκριμένος Πάροχος Υπηρεσιών Χρονοσφραγίδας |
| ΜΧ | Μονάδα Χρονοσφραγίδας |
| CSU | Κρυπτογραφημένη Μονάδα Υπογραφής |
| HSM | Hardware Security Module (Μονάδα Ασφάλειας Υλικού) |
| IETF | Internet Engineering Task Force |
| ISO | Διεθνής Οργανισμός Τυποποίησης |
| ITU | Διεθνής Ένωση Τηλεπικοινωνιών |
| OID | Αναγνωριστικό αντικειμένου |
| UTC | Coordinated Universal Time |