ATHEX
Χρηματιστήριο Αθηνών

ΥΠΗΡΕΣΙΕΣ ΨΗΦΙΑΚΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ

Πολιτική/Κανονισμός για Αναγνωρισμένη Ηλεκτρονική Χρονοσήμανση

(CP/CPS for Qualified Electronic Time Stamps)

Έκδοση 1.0 - 15/06/2017

Εγκεκριμένη για τις ακόλουθες «Πολιτικές Πιστοποιητικών» του Χ.Α.:

---

1. Πολιτική Πιστοποιητικών για Πιστοποιητικά Χρονοσήμανσης
   OID 1.3.6.1.4.1.29402.1.1.4.1.1.0

1. ΕΙΣΑΓΩΓΗ

1.1 Επισκόπηση

Ο παρών Κανονισμός Πιστοποίησης (εφεξής «κανονισμός CPS») της ΕΛΛΗΝΙΚΑ ΧΡΗΜΑΤΙΣΤΗΡΙΑ - ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ Α.Ε. ΣΥΜΜΕΤΟΧΩΝ (εφεξής «Χ.Α.») παρουσιάζει τις αρχές και τις διαδικασίες που χρησιμοποιούνται από την ΕΛΛΗΝΙΚΑ ΧΡΗΜΑΤΙΣΤΗΡΙΑ - ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ Α.Ε. ΣΥΜΜΕΤΟΧΩΝ για την έκδοση και τη διαχείριση του κύκλου ζωής των Πιστοποιητικών Χρονοσήμανσης της ΕΛΛΗΝΙΚΑ ΧΡΗΜΑΤΙΣΤΗΡΙΑ - ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ Α.Ε. ΣΥΜΜΕΤΟΧΩΝ. Ο παρών κανονισμός CPS και όλες οι τροποποιήσεις του ενσωματώνονται δια παραπομπής σε όλα τα προαναφερθέντα πιστοποιητικά της ΕΛΛΗΝΙΚΑ ΧΡΗΜΑΤΙΣΤΗΡΙΑ - ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ Α.Ε. ΣΥΜΜΕΤΟΧΩΝ.

Ο κανονισμός (ΕΕ) αριθ. 910/2014 («κανονισμός eIDAS») περιλαμβάνει απαιτήσεις για τους Παρόχους Υπηρεσιών Εμπιστοσύνης (εφεξής «πάροχοι TSP») που παρέχουν υπηρεσίες στο κοινό, συμπεριλαμβανομένων των παρόχων TSP που εκδίδουν χρονοσημάνσεις. Επιπλέον, στον κανονισμό καθορίζονται πιο συγκεκριμένες απαιτήσεις για μια συγκεκριμένη κατηγορία παρόχων TSP που ονομάζονται «αναγνωρισμένοι πάροχοι TSP». Το Χ.Α. είναι αναγνωρισμένος πάροχος TSP.
Οι ηλεκτρονικές υπογραφές χρησιμοποιούνται για την αύξηση της ασφάλειας μέσω δημιουργίας μιας απαραβίαστης κρυπτογραφικής σφράγισης γύρω από ηλεκτρονικά δεδομένα. Μόλις υπογραφεί ένα δεδομένο, οποιαδήποτε αλλαγή στο περιεχόμενό του θα προκαλέσει την αποτυχία της ηλεκτρονικής υπογραφής, προειδοποιώντας τον χρήστη. Οι ηλεκτρονικές υπογραφές μπορούν να χρησιμοποιηθούν με διάφορους τρόπους:

- Οι μεμονωμένες ηλεκτρονικές υπογραφές υποστηρίζουν την ακεραιότητα των ηλεκτρονικών αρχείων, δηλώνοντας ΠΟΙΟΣ υπέγραψε ΤΙ (με άλλα λόγια, ποιος δημιούργησε το συγκεκριμένο περιεχόμενο ή τις αλλαγές).

- Οι χρονοσημάνσεις χρησιμοποιούν ηλεκτρονικές υπογραφές, ενσωματώνοντας τον χρόνο από μια ακριβή πηγή, για να επιβεβαιώσουν ΤΙ έγινε ΠΟΤΕ.

Οι μεμονωμένες υπογραφές μπορούν να χρησιμοποιηθούν ανεξάρτητα –ή μαζί με χρονοσημάνσεις– προκειμένου να αυξηθεί η αξιοπιστία των ηλεκτρονικών αρχείων και συναλλαγών.

1.2 Όνομα και ταυτοποίηση εγγράφου

Το παρόν έγγραφο είναι ο Κανονισμός Πιστοποίησης της Ελληνικά Χρηματιστήρια – Χρηματιστήριο Αθηνών Α.Ε. Συμμετοχών για Πιστοποιητικά Χρονοσήμανσης. Οι τιμές του χαρακτηριστικού αναγνώρισης (OID) που αντιστοιχούν στην Πολιτική Πιστοποιητικών της Ελληνικά Χρηματιστήρια – Χρηματιστήριο Αθηνών Α.Ε. Συμμετοχών. είναι οι εξής:

1.3.6.1.4.1.29402.1.4.1.0	Ελληνικά Χρηματιστήρια – Χρηματιστήριο Αθηνών Α.Ε. Συμμετοχών

	Πολιτική/Κανονισμός Πιστοποίησης Πιστοποιητικών Χρονοσήμανσης

1.3.6.1.4.1.29402	Χαρακτηριστικό αναγνώρισης (OID) της Ελληνικά Χρηματιστήρια – Χρηματιστήριο Αθηνών Α.Ε.
1	Ανεξάρτητο τμήμα «Υπηρεσιών Δημόσιας Πιστοποίησης» της Ελληνικά Χρηματιστήρια –
4	***Πολιτική πιστοποιητικών για χρονοσήμανση***
1.0	***Πρώτο και δεύτερο ψηφίο του αριθμού έκδοσης της Πολιτικής Πιστοποιητικών/Κανονισμού Πιστοποίησης***

2. Πεδίο εφαρμογής

Η Αρχή Χρονοσήμανσης του Χ.Α. (εφεξής «αρχή TSA») χρησιμοποιεί υποδομή δημόσιων κλειδιών και αξιόπιστες χρονικές πηγές για την παροχή αξιόπιστων ηλεκτρονικών χρονοσημάνσεων βάσει προτύπων. Η παρούσα Πολιτική/Κανονισμός Χρονοσήμανσης του Χ.Α. (εφεξής «πολιτική TSP/PS του Χ.Α.») ορίζει τις λειτουργικές και διαχειριστικές πρακτικές του Χ.Α., ώστε οι Συνδρομητές και τα Τρίτα Βασιζόμενα Μέρη να μπορούν να αξιολογήσουν την εμπιστοσύνη τους στη λειτουργία των υπηρεσιών χρονοσήμανσης εγγράφων.

Η αρχή TSA του Χ.Α. στοχεύει στην παροχή υπηρεσιών χρονοσήμανσης εγγράφων σύμφωνα με τον κανονισμό eIDAS, καθώς και βάσει άλλων εφαρμοστέων εθνικών νόμων και κανονισμών. Ωστόσο, οι χρονοσημάνσεις του Χ.Α. μπορούν να χρησιμοποιηθούν εξίσου σε οποιαδήποτε εφαρμογή που απαιτεί απόδειξη ότι ένα δεδομένο υπήρχε πριν από μια συγκεκριμένη χρονική στιγμή.

Η δομή και το περιεχόμενο της παρούσας πολιτικής TSP/PS του Χ.Α. καθορίζονται σύμφωνα με το πρότυπο ETSI EN 319 421 - Ηλεκτρονικές Υπογραφές και Υποδομές (ESI): Απαιτήσεις πολιτικής και ασφάλειας για Παρόχους Υπηρεσιών Εμπιστοσύνης που εκδίδουν χρονοσημάνσεις. Η διαχείριση και έγκριση της πολιτικής TSP/PS του Χ.Α. γίνεται από την Αρχή Διαχείρισης Πολιτικών του Χ.Α. Η πολιτική πρέπει να διαβάζεται σε συνδυασμό με την τρέχουσα Πολιτική Πιστοποιητικών/Κανονισμό Πιστοποίησης (CP/CPS) του Χ.Α.

3. Παραπομπές

Τα ακόλουθα έγγραφα περιέχουν διατάξεις σχετικές με την πολιτική TSP/PS του Χ.Α.:

[1] ETSI EN 319.412-2: Ηλεκτρονικές υπογραφές και υποδομές (ESI), Προφίλ πιστοποιητικών, Μέρος 2: Προφίλ πιστοποιητικού για πιστοποιητικά που εκδίδονται σε φυσικά πρόσωπα.
[2] ETSI EN 319 412-3: Ηλεκτρονικές υπογραφές και υποδομές (ESI), Προφίλ πιστοποιητικών, Μέρος 3: Προφίλ πιστοποιητικού για πιστοποιητικά που εκδίδονται σε νομικά πρόσωπα.
[3] ETSI EN 319.422: Ηλεκτρονικές υπογραφές και υποδομές (ESI), Πρωτόκολλο χρονοσήμανσης και προφίλ αδειοδοτικών χρονοσήμανσης.

[4] ETSI EN 319.421: Ηλεκτρονικές υπογραφές και υποδομές (ESI), Απαιτήσεις πολιτικής και ασφάλειας για Παρόχους Υπηρεσιών Εμπιστοσύνης που εκδίδουν χρονοσημάνσεις.
[5] ETSI TS 102.176.1: Αλγόριθμοι και παράμετροι για ασφαλείς ηλεκτρονικές υπογραφές, Μέρος 1: Συναρτήσεις σύνοψης και ασύμμετροι αλγόριθμοι.
[
[6] RFC 3126: Μορφές ηλεκτρονικής υπογραφής για μακροχρόνιες ηλεκτρονικές υπογραφές.
[7] RFC 3161: Πρωτόκολλο X.509 χρονοσήμανσης για υποδομή δημόσιων κλειδιών.
[8] 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 (κανονισμός eIDAS).

4. Ορισμοί και συντομογραφίες

4.1 Ορισμοί

Ως «Πολιτική Πιστοποιητικών/Κανονισμός Πιστοποίησης» ή «πολιτική CP/CPS» νοείται ένα έγγραφο που διατίθεται στο κοινό, το οποίο εξηγεί λεπτομερώς το σύστημα PKI του Χ.Α. και περιγράφει τις πρακτικές που χρησιμοποιούνται για την έκδοση Ψηφιακών Πιστοποιητικών.

Ως «Συντονισμένη Παγκόσμια Ώρα» ή «UTC» νοείται η χρονική κλίμακα, με βάση τα δευτερόλεπτα, όπως ορίζεται από τη σύσταση TF.460-5 της Διεθνούς Επιτροπής Τηλεπικοινωνιών - Τομέα ραδιοεπικοινωνιών (ITU-R) και αντιστοιχεί περίπου στη Μέση Ώρα Γκρίνουιτς (GMT).

Ως «ηλεκτρονική χρονοσήμανση» νοούνται τα δεδομένα σε ηλεκτρονική μορφή τα οποία συνδέουν άλλα δεδομένα σε ηλεκτρονική μορφή με μια συγκεκριμένη χρονική στιγμή, αποδεικνύοντας ότι τα τελευταία δεδομένα υπήρχαν εκείνη τη στιγμή.

Ως «αναγνωρισμένη ηλεκτρονική χρονοσήμανση» νοείται μια ηλεκτρονική χρονοσήμανση που πληροί τις ακόλουθες απαιτήσεις:
(α) συνδέει τα δεδομένα με την ημερομηνία και την ώρα κατά τρόπο που να αποκλείει ευλόγως τη δυνατότητα μεταβολής των δεδομένων χωρίς αυτό να γίνει αντιληπτό,
(β) βασίζεται σε ακριβή χρονική πηγή που συνδέεται με τη Συντονισμένη Παγκόσμια Ώρα και
(γ) υπογράφεται με προηγμένη ηλεκτρονική υπογραφή ή σφραγίζεται με προηγμένη ηλεκτρονική σφραγίδα του αναγνωρισμένου παρόχου υπηρεσιών εμπιστοσύνης ή με κάποια ισοδύναμη μέθοδο.

Ως «τρίτο βασιζόμενο μέρος» νοείται μια οντότητα (φυσικό πρόσωπο ή οργανισμός) που βασίζεται σε ένα αδειοδοτικό χρονοσήμανσης που παρέχεται από την αρχή TSA του Χ.Α.
Ως «Χ.Α.» νοείται η ΕΛΛΗΝΙΚΑ ΧΡΗΜΑΤΙΣΤΗΡΙΑ – ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ Α.Ε. ΣΥΜΜΕΤΟΧΩΝ.

Ως «συνδρομητής» νοείται μια οντότητα (φυσικό πρόσωπο ή οργανισμός) που αιτείται τις υπηρεσίες που παρέχονται από αρχή TSA και έχει συνάψει Συμφωνία Συνδρομητή με την αρχή TSA του Χ.Α.

Ως «αρχή χρονοσήμανσης» ή «αρχή TSA» νοείται μια αξιόπιστη αρχή που εκδίδει αδειοδοτικά χρονοσήμανσης.

Ως «πολιτική/κανονισμός χρονοσήμανσης» ή «πολιτική TSP/PS του Χ.Α.» (το παρόν έγγραφο) νοείται ένα σύνολο κανόνων που διέπουν τη δυνατότητα εφαρμογής ενός αδειοδοτικού χρονοσήμανσης σε ένα συγκεκριμένο σύνολο ή κατηγορία εφαρμογών με κοινές απαιτήσεις ασφαλείας.

Ως «αδειοδοτικό χρονοσήμανσης» ή «αδειοδοτικό TST» νοείται ένα αντικείμενο δεδομένων που συνδέει την αναπαράσταση ενός δεδομένου με μια συγκεκριμένη χρονική στιγμή χρησιμοποιώντας ψηφιακή υπογραφή, δημιουργώντας με αυτόν τον τρόπο ένα αποδεικτικό στοιχείο.

Ως «μονάδα χρονοσήμανσης» ή «μονάδα TSU» νοείται ένα σύνολο υλισμικού και λογισμικού που διοικείται ως μονάδα και έχει ένα μόνο ιδιωτικό κλειδί υπογραφής ενεργό κάθε φορά.

Ως «υπηρεσία εμπιστοσύνης» νοείται μια ηλεκτρονική υπηρεσία που ενισχύει την εμπιστοσύνη στις ηλεκτρονικές συναλλαγές.

Ως «πάροχος υπηρεσιών εμπιστοσύνης (πάροχος TSP)» νοείται μια οντότητα που παρέχει μία ή περισσότερες υπηρεσίες εμπιστοσύνης.

Ως «UTC(k)» νοείται μια χρονική κλίμακα που λαμβάνεται από ένα εργαστήριο «k», όπως ορίζεται στην εγκύκλιο T του Διεθνούς Γραφείου Μέτρων και Σταθμών (BIPM) και διατηρείται σε στενή συμφωνία με την UTC.

Πρόσθετοι ορισμοί παρέχονται στις πολιτικές CP/CPS.

4.2 Συντομογραφίες

5. Γενικές έννοιες

5.1 Υπηρεσίες χρονοσήμανσης εγγράφων

Οι υπηρεσίες χρονοσήμανσης εγγράφων αποτελούνται από τα ακόλουθα:

- Παροχή χρονοσήμανσης: η τεχνική υπηρεσία που εκδίδει τα αδειοδοτικά χρονοσήμανσης (αδειοδοτικά TST).

- Διαχείριση χρονοσήμανσης: η υπηρεσία που παρακολουθεί και ελέγχει τη λειτουργία της χρονοσήμανσης, συμπεριλαμβανομένου του συγχρονισμού με το σημείο αναφοράς χρόνου UTC, σύμφωνα με την πολιτική TSP/PS του Χ.Α.

Το Χ.Α. τηρεί τα διεθνή πρότυπα που παρατίθενται στην ενότητα 3 («Παραπομπές») του παρόντος εγγράφου με σκοπό την αύξηση της αξιοπιστίας των υπηρεσιών χρονοσήμανσης εγγράφων τόσο για συνδρομητές όσο και για τρίτα βασιζόμενα μέρη.

5.2 Αρχή χρονοσήμανσης

Οι χρήστες (δηλαδή οι συνδρομητές και τα τρίτα βασιζόμενα μέρη) εμπιστεύονται την αρχή TSA για την έκδοση ασφαλών αδειοδοτικών TST. Η αρχή TSA του Χ.Α. αναλαμβάνει τη συνολική ευθύνη για την παροχή των υπηρεσιών χρονοσήμανσης εγγράφων που προσδιορίζονται στην ενότητα 5.1.

Η αρχή TSA του Χ.Α. έχει την ευθύνη για τη λειτουργία μίας ή περισσοτέρων μονάδων χρονοσήμανσης (εφεξής «μονάδα TSU») που δημιουργούν και υπογράφουν αδειοδοτικά TST για λογαριασμό της αρχής TSA. Κάθε μονάδα TSU έχει διαφορετικό κλειδί.

Στη συνέχεια παρουσιάζεται μια σύνοψη των σημερινών μονάδων TSU του Χ.Α. και των εκδοτών τους:

ATHEX TSU Subject Distinguished Name	TSU Issuer
CN = Athex Qualified Timestamping Authority O = Athens Stock Exchange C = GR	ATHEX Root CA G2

Το Χ.Α. λειτουργεί την αρχή TSA στο πλαίσιο της Υποδομής Δημόσιων Κλειδιών (εφεξής «σύστημα PKI»). Η αρχή TSA του Χ.Α. αναγνωρίζεται στα Ψηφιακά Πιστοποιητικά που χρησιμοποιούνται στην υπηρεσία χρονοσήμανσης εγγράφων.

5.3 Συνδρομητές και Τρίτα βασιζόμενα μέρη

Οι συνδρομητές είναι οντότητες που τηρούν σύμβαση παροχής υπηρεσιών με το Χ.Α. και έχουν συνάψει τη Συμφωνία Συνδρομητή με την Αρχή Χρονοσήμανσης του Χ.Α. Τρίτο βασιζόμενο μέρος είναι ένα φυσικό πρόσωπο ή μια οντότητα που βασίζεται σε ένα αδειοδοτικό TST που δημιουργείται ως αδειοδοτικό TST του Χ.Α. Το τρίτο βασιζόμενο μέρος δεν είναι απαραιτήτως συνδρομητής. Οι οργανισμοί που είναι συνδρομητές είναι υπεύθυνοι για τις δραστηριότητες των συνδεδεμένων χρηστών και των τρίτων βασιζόμενων μερών τους και πρέπει να τους ενημερώνουν για την ορθή χρήση των χρονοσημάνσεων και για τους όρους της πολιτικής TSP/PS του Χ.Α. Οι συνδρομητές πρέπει να χρησιμοποιούν για τη δημιουργία χρονοσημάνσεων μια μέθοδο ή ένα πακέτο εργαλείων λογισμικού που εγκρίνεται από το Χ.Α., εκτός εάν εξουσιοδοτηθούν εγγράφως από το Χ.Α να πράξουν διαφορετικά.

5.4 Πολιτική και πρακτικές της αρχής TSA

5.4.1 Σκοπός

Η Πολιτική Χρονοσήμανσης («τι τηρείται») και ο Κανονισμός Χρονοσήμανσης («πώς τηρείται») του Χ.Α., έχουν συγχωνευθεί σε ένα έγγραφο, την πολιτική TSP/PS του Χ.Α. Η εν λόγω πολιτική TSP/PS του Χ.Α καθορίζει μια πολιτική και έναν κανονισμό χρονοσήμανσης εγγράφων που καλύπτουν τις γενικές απαιτήσεις για υπηρεσίες εμπιστοσύνης όσον αφορά τη χρονοσήμανση.

Για περισσότερες λεπτομέρειες σχετικά με την αρχή TSA του Χ.Α., ανατρέξτε στην ενότητα 8.1 («Πρακτικές και δηλώσεις γνωστοποίησης») του παρόντος εγγράφου. Όλες οι πολιτικές και πρακτικές του Χ.Α. υπόκεινται στον έλεγχο της Αρχής Διαχείρισης Πολιτικών του Χ.Α.

5.4.2 Βαθμός ειδικού χαρακτήρα

Η παρούσα πολιτική TSP/PS του Χ.Α. επεκτείνει την πολιτική CP/CPS που ρυθμίζει τη λειτουργία του Χ.Α. και των συναφών υπηρεσιών χωρίς τη δυνατότητα αποκήρυξης (non-repudiation). Η πολιτική TSP/PS και η πολιτική CP/CPS του Χ.Α. είναι δημόσια έγγραφα και μπορούν να ληφθούν στη διεύθυνση: http://www.athexgroup.gr/digital-certificates-pki-regulations.

5.4.3 Προσέγγιση

Η πολιτική TSP/PS του Χ.Α. καθορίζει τους γενικούς κανόνες λειτουργίας της αρχής TSA του Χ.Α. Πρόσθετα εσωτερικά έγγραφα ορίζουν τον τρόπο με τον οποίον το Χ.Α. πληροί τις τεχνικές, οργανωτικές και διαδικαστικές απαιτήσεις που προσδιορίζονται στην πολιτική TSP/PS του Χ.Α. Τα εν λόγω έγγραφα επιτρέπεται να παρασχεθούν μόνο υπό αυστηρά ελεγχόμενες συνθήκες.

6. Πολιτική χρονοσήμανσης

6.1 Επισκόπηση

Η παρούσα πολιτική TSP ορίζει ένα σύνολο διαδικασιών για την αξιόπιστη δημιουργία αδειοδοτικών χρονοσήμανσης σύμφωνα με το πρότυπο ETSI EN 319 421. Τα ιδιωτικά κλειδιά και οι μονάδες TSU πληρούν τις τεχνικές προδιαγραφές των προτύπων ETSI EN 319 422 και RFC 3161.

Η αρχή TSA του Χ.Α. υπογράφει χρονοσημάνσεις χρησιμοποιώντας ιδιωτικά κλειδιά που προορίζονται αποκλειστικά για τον σκοπό αυτό. Κάθε αδειοδοτικό TST περιέχει ένα αναγνωριστικό που παραπέμπει στην ισχύουσα πολιτική και τα αδειοδοτικά εκδίδονται με ακρίβεια χρόνου ± 1 δευτερολέπτου έναντι της UTC.

Αιτήσεις για χρονοσημάνσεις υποβάλλονται είτε μέσω του Πρωτοκόλλου Ελέγχου Μετάδοσης (TCP) είτε μέσω του Πρωτοκόλλου Υπερκειμενικής Μεταφοράς (HTTP), όπως περιγράφεται στο πρότυπο RFC 3161.

Η διεύθυνση URL για την πολιτική TSP/PS του Χ.Α. είναι:
http://www.athexgroup.gr/digital-certificates-pki-regulations

6.2 Ταυτοποίηση

Το χαρακτηριστικό αναγνώρισης (OID) της πολιτικής χρονοσήμανσης του Χ.Α. είναι: **1.3.6.1.4.1.29402.1.4.1.0**.

Αυτό το OID αναφέρεται σε κάθε χρονοσήμανση που εκδίδεται από το Χ.Α., ενώ η πολιτική TSP/PS του Χ.Α. διατίθεται τόσο σε συνδρομητές όσο και σε τρίτα βασιζόμενα μέρη.
Η παρούσα πολιτική χρονοσήμανσης του Χ.Α. βασίζεται στην πολιτική βέλτιστων πρακτικών του προτύπου ETSI BTSP για χρονοσημάνσεις (OID 0.4.0.2023.1.1).

6.3 Κοινότητα χρηστών και εφαρμοσιμότητα

Η κοινότητα χρηστών για τις χρονοσημάνσεις του Χ.Α. περιλαμβάνει μόνο τους συνδρομητές και τα τρίτα βασιζόμενα μέρη τους. Όλοι οι συνδρομητές θεωρούνται

αυτόματα ως τρίτα βασιζόμενα μέρη. Το Χ.Α. δεν παρέχει δημόσιες υπηρεσίες χρονοσήμανσης εγγράφων.
Οι χρονοσημάνσεις του Χ.Α. μπορούν να εφαρμοστούν σε οποιαδήποτε εφαρμογή που απαιτεί απόδειξη ότι ένα δεδομένο υπήρχε πριν από μια συγκεκριμένη χρονική στιγμή.

6.4 Συμμόρφωση

Το Χ.Α. αναφέρει σε όλες τις χρονοσημάνσεις το χαρακτηριστικό αναγνώρισης πολιτικής που αναγράφεται στην ενότητα 6.2 («Ταυτοποίηση») του παρόντος εγγράφου για να δηλώσει τη συμμόρφωση με την παρούσα πολιτική. Το Χ.Α. υπόκειται σε περιοδικές ανεξάρτητες εσωτερικές και εξωτερικές αναθεωρήσεις για να αποδείξει ότι η αρχή TSA του Χ.Α. ανταποκρίνεται στις υποχρεώσεις που ορίζονται στην ενότητα 7.1 («Υποχρεώσεις αρχής TSA») και έχει εφαρμόσει τους κατάλληλους ελέγχους σύμφωνα με την ενότητα 8 («Πρακτικές αρχής TSA»). Ανατρέξτε στη διεύθυνση http://www.athexgroup.gr/digital-certificates-pki-regulations για τον κατάλογο των ελέγχων και των διαπιστεύσεων του Χ.Α.

7. Υποχρεώσεις και ευθύνη

7.1 Υποχρεώσεις αρχής TSA

7.1.1 Γενικές υποχρεώσεις

Η λειτουργία της αρχής TSA εναπόκειται στο Χ.Α., το οποίο αναλαμβάνει την ευθύνη τήρησης των απαιτήσεων της ενότητας 8 («Πρακτικές αρχής TSA») του παρόντος εγγράφου - καθώς και των διατάξεων του κανονισμού eIDAS, όπως εφαρμόζονται στην επιλεγμένη πολιτική αξιόπιστης χρονοσήμανσης.
Το Χ.Α. είναι συμβαλλόμενο μέρος στις αμοιβαίες συμφωνίες και υποχρεώσεις μεταξύ της αρχής TSA, των συνδρομητών και των τρίτων βασιζόμενων μερών. Οι πολιτικές TSP/PS και CP/CPS του Χ.Α. αποτελούν αναπόσπαστα στοιχεία αυτών των συμφωνιών.

7.1.2 Υποχρεώσεις της αρχής TSA προς τους συνδρομητές

Το Χ.Α. αναλαμβάνει τις ακόλουθες υποχρεώσεις προς τους συνδρομητές της αρχής TSA:

- Να λειτουργεί σύμφωνα με την παρούσα πολιτική TSP/PS του Χ.Α., την πολιτική CP/CPS και άλλες σχετικές λειτουργικές πολιτικές και διαδικασίες.
- Να διασφαλίζει ότι οι μονάδες TSU διατηρούν ελάχιστη χρονική ακρίβεια ± 1 δευτερολέπτου έναντι της UTC.
- Να υποβάλλεται σε εσωτερικές και εξωτερικές αναθεωρήσεις προκειμένου να διασφαλίζεται η συμμόρφωσή του με τη σχετική νομοθεσία και τις εσωτερικές πολιτικές και διαδικασίες του Χ.Α.
- Να παρέχει υψηλό βαθμό διαθεσιμότητας πρόσβασης στα συστήματα της αρχής TSA του Χ.Α. εκτός από την περίπτωση προγραμματισμένων τεχνικών διακοπών και απώλειας συγχρονισμού χρόνου.

7.2 Υποχρεώσεις συνδρομητών

Οι συνδρομητές πρέπει να επαληθεύουν ότι το αδειοδοτικό χρονοσήμανσης φέρει τη σωστή υπογραφή και να ελέγχουν ότι το ιδιωτικό κλειδί που χρησιμοποιήθηκε για την υπογραφή του αδειοδοτικού χρονοσήμανσης δεν έχει παραβιαστεί. Οι συνδρομητές πρέπει να χρησιμοποιούν ασφαλείς κρυπτογραφικές λειτουργίες για αιτήματα χρονοσήμανσης. Οι συνδρομητές πρέπει να ενημερώνουν τους τελικούς τους χρήστες (συμπεριλαμβανομένων των τυχόν εμπλεκόμενων τρίτων βασιζόμενων μερών) σχετικά με τις πολιτικές TSP/PS και CP/CPS του Χ.Α. Οι υποχρεώσεις των συνδρομητών ορίζονται επίσης στη Συμφωνία Συνδρομητή της Αρχής Χρονοσήμανσης.

7.3 Υποχρεώσεις τρίτων βασιζόμενων μερών

Πριν εμπιστευτούν κάποια χρονοσήμανση, με την επιφύλαξη της ενότητας 8.1.2 («Δήλωση γνωστοποίησης αρχής TSA») του παρόντος εγγράφου, τα τρίτα βασιζόμενα μέρη πρέπει να επαληθεύσουν ότι το αδειοδοτικό TST φέρει τη σωστή υπογραφή και ότι το ιδιωτικό κλειδί που χρησιμοποιείται για την υπογραφή του αδειοδοτικού TST δεν έχει ανακληθεί. Το τρίτο βασιζόμενο μέρος θα πρέπει να λαμβάνει υπόψη τυχόν περιορισμούς στη χρήση της χρονοσήμανσης που υποδεικνύονται στην παρούσα πολιτική TSP/PS του Χ.Α. και οποιεσδήποτε άλλες προφυλάξεις που καθορίζονται στην παρούσα συμφωνία ή στην αίτηση Σύμβαση Συνδρομητή. Κατά την περίοδο ισχύος του πιστοποιητικού TSU, η κατάσταση του ιδιωτικού κλειδιού μπορεί να ελεγχθεί χρησιμοποιώντας τη σχετική λίστα ανακληθέντων πιστοποιητικών («λίστα CRL») του Χ.Α. Τα πιστοποιητικά που εκδίδονται από το Χ.Α., τα πιστοποιητικά TSU και οι σχετικές λίστες CRL δημοσιεύονται στη διεύθυνση www.athexgroup.gr/digital-certificates-repository. Εάν αυτή η επαλήθευση πραγματοποιηθεί μετά τη λήξη της περιόδου ισχύος του πιστοποιητικού, το τρίτο βασιζόμενο μέρος θα πρέπει να ακολουθήσει τις οδηγίες που αναφέρονται στο παράρτημα Δ του προτύπου ETSI EN 319 421.

Το πρότυπο ETSI EN 319 421 περιέχει ορισμένες πρόσθετες απαιτήσεις για τις αναγνωρισμένες ηλεκτρονικές χρονοσημάνσεις σύμφωνα με τον κανονισμό eIDAS.
Το πρότυπο ETSI EN 319 421 αναφέρει:

«Το τρίτο βασιζόμενο μέρος αναμένεται να χρησιμοποιήσει έναν κατάλογο εμπιστοσύνης για να διαπιστώσει εάν η μονάδα χρονοσήμανσης και η χρονοσήμανση είναι κατάλληλες. Εάν το δημόσιο κλειδί της μονάδας TSU περιλαμβάνεται στον κατάλογο εμπιστοσύνης και η υπηρεσία που αντιπροσωπεύει είναι υπηρεσία αναγνωρισμένης χρονοσήμανσης, τότε οι χρονοσημάνσεις που εκδίδονται με αυτήν τη μονάδα TSU μπορούν να θεωρηθούν κατάλληλες».
Το Χ.Α. λειτουργεί σήμερα στα πλαίσια των μεταβατικών μέτρων (άρθρο 51) του κανονισμού eIDAS. Τα δημόσια κλειδιά των μονάδων TSU του Χ.Α. δεν εμφανίζονται αυτήν τη στιγμή σε κανέναν κατάλογο εμπιστοσύνης. Οι εκδότες των μονάδων TSU του Χ.Α. αναγράφονται σε καταλόγους εμπιστοσύνης.

7.4 Ευθύνη

Το Χ.Α. αναλαμβάνει την υποχρέωση να λειτουργεί την αρχή TSA του Χ.Α. σύμφωνα με τις πολιτικές TSP/PS και CP/CPS του Χ.Α. και τους όρους των συμφωνιών με τους συνδρομητές. Το Χ.Α. δεν παρέχει ρητές ή σιωπηρές δηλώσεις ή εγγυήσεις σχετικά με τη διαθεσιμότητα ή την ακρίβεια της υπηρεσίας χρονοσήμανσης εγγράφων. Το Χ.Α. δεν ευθύνεται σε καμία περίπτωση για απώλεια κερδών, απώλεια πωλήσεων ή κύκλου εργασιών, απώλεια ή ζημία στη φήμη, απώλεια συμβάσεων, απώλεια πελατών, απώλεια χρήσης λογισμικού ή δεδομένων, απώλεια ή χρήση οποιουδήποτε υπολογιστή ή άλλου εξοπλισμού εκτός αυτής που μπορεί να προκύψει άμεσα από παραβίαση των πολιτικών TSP/PS ή CP/CPS του Χ.Α., απώλεια χρόνου διοικητικού ή άλλου προσωπικού, απώλειες ή ευθύνες στο πλαίσιο ή σε σχέση με οποιεσδήποτε άλλες συμβάσεις, έμμεση απώλεια ή ζημία, επακόλουθη απώλεια ή ζημία και, για τους σκοπούς της παρούσας παραγράφου, ο όρος «απώλεια» σημαίνει μερική απώλεια ή μείωση της αξίας καθώς και πλήρης ή ολική απώλεια. Το Χ.Α. φέρει ειδική ευθύνη για ζημιά σε συνδρομητές και τρίτα βασιζόμενα μέρη σε σχέση με τα έγκυρα αναγνωρισμένα ψηφιακά πιστοποιητικά στα οποία βασίζονται, σύμφωνα με συγκεκριμένους εθνικούς νόμους και κανονισμούς.

8. Πρακτικές

Η παροχή αδειοδοτικού χρονοσήμανσης ως απάντηση σε αίτημα γίνεται κατά την κρίση του Χ.Α., ανάλογα με τις συμφωνίες που έχουν γίνει με τον συνδρομητή.

8.1 Πρακτικές και δηλώσεις γνωστοποίησης

8.1.1 Κανονισμός αρχής TSA

Η παρούσα πολιτική TSP/PS του Χ.Α. καθορίζει τους γενικούς κανόνες λειτουργίας της αρχής TSA του Χ.Α. Η πολιτική CP/CPS και πρόσθετα εσωτερικά έγγραφα ορίζουν τον τρόπο με τον οποίον το Χ.Α. πληροί τις τεχνικές, οργανωτικές και διαδικαστικές απαιτήσεις που προσδιορίζονται στην πολιτική TSP/PS του Χ.Α.

Η πολιτική TSP/PS του Χ.Α., η δήλωση γνωστοποίησης της αρχής TSA και άλλα δημόσια έγγραφα είναι διαθέσιμα στη διεύθυνση Http://www.athexgroup.gr/digital-certificates-pki-regulations. Τα εσωτερικά έγγραφα επιτρέπεται να παρασχεθούν μόνο υπό αυστηρά ελεγχόμενες συνθήκες.

Το Χ.Α. διεξάγει αξιολογήσεις κινδύνου για την εκτίμηση των απειλών και τον καθορισμό των απαιτούμενων ελέγχων και λειτουργικών διαδικασιών ασφαλείας.
Η πολιτική TSP/PS του Χ.Α. προσδιορίζει τις υποχρεώσεις των εξωτερικών οργανισμών που υποστηρίζουν τις υπηρεσίες της αρχής TSA, συμπεριλαμβανομένων των εφαρμοστέων πολιτικών και πρακτικών.
Η Υπηρεσία Διαχείρισης Πολιτικών του Χ.Α. είναι υπεύθυνη για την τήρηση και έγκριση όλων των πολιτικών και πρακτικών του Χ.Α. σύμφωνα με τους όρους της ενότητας 1.5 («Διαχείριση πολιτικών») της πολιτικής CP/CPS. Η διοίκηση του Χ.Α. έχει την ευθύνη να διασφαλίζει ότι οι πρακτικές εφαρμόζονται σωστά.

8.1.2 Δήλωση γνωστοποίησης της αρχής TSA

Το εν λόγω έγγραφο γνωστοποιεί σε όλους τους συνδρομητές και τα δυνητικά τρίτα βασιζόμενα μέρη τους όρους και τις προϋποθέσεις που αφορούν τη χρήση των υπηρεσιών χρονοσήμανσης εγγράφων του Χ.Α. Τα στοιχεία της δήλωσης γνωστοποίησης της αρχής TSA του Χ.Α. είναι τα εξής:

- Κάθε αδειοδοτικό χρονοσήμανσης που εκδίδεται από την αρχή TSA του Χ.Α. περιέχει το χαρακτηριστικό αναγνώρισης της πολιτικής που περιέχεται στην ενότητα 6.2 («Ταυτοποίηση») του παρόντος εγγράφου.

• Οι αλγόριθμοι κρυπτογράφησης και τα μήκη των κλειδιών που χρησιμοποιεί η αρχή TSA του Χ.Α. συμμορφώνονται με το πρότυπο ETSI EN 319 422 και είναι σήμερα:
- Συνόψεις για αποδεκτά αιτήματα χρονοσήμανσης: SHA-256, SHA-384, SHA-512
- Υπογραφή: sha256WithRSAEncryption (κλειδί 2048 bit)

• Οι μονάδες TSU του Χ.Α. έχουν περίοδο ισχύος μέχρι δέκα έτη.
•. Το Χ.Α. θα αναρτήσει δημόσια ανακοίνωση στον ιστότοπό του εάν διαπιστώσει ότι οι κρυπτογραφικοί αλγόριθμοι και τα μήκη κλειδιών που χρησιμοποιούνται στο σύστημα PKI του Χ.Α. δεν θεωρούνται πλέον ασφαλή.
• Η αρχή TSA του Χ.Α. εξασφαλίζει ακρίβεια ± 1 δευτερολέπτου από αξιόπιστη χρονική πηγή UTC. Εάν δεν μπορεί να εξασφαλιστεί αξιόπιστη χρονική πηγή UTC, η χρονοσήμανση δεν θα εκδίδεται.

• Η χρήση της αρχής TSA του Χ.Α. μπορεί να περιορίζεται σε κατόχους έγκυρου ψηφιακού πιστοποιητικού Χ.Α.
• Οι υποχρεώσεις των συνδρομητών περιγράφονται στην ενότητα 7.2 («Υποχρεώσεις συνδρομητών») του παρόντος εγγράφου.
• Οι υποχρεώσεις των τρίτων βασιζόμενων μερών περιγράφονται στην ενότητα 7.3 («Υποχρεώσεις τρίτων βασιζόμενων μερών») του παρόντος εγγράφου.
• Το Χ.Α. διατηρεί ασφαλή αρχεία σχετικά με τη λειτουργία της αρχής TSA του Χ.Α.
• Το Χ.Α. δεν παρέχει ρητές ή σιωπηρές δηλώσεις ή εγγυήσεις σχετικά με τη διαθεσιμότητα ή την ακρίβεια της αρχής TSA του Χ.Α. Το Χ.Α. φέρει ειδική ευθύνη για ζημιά σε συνδρομητές και τρίτα βασιζόμενα μέρη σε σχέση με τα έγκυρα ψηφιακά πιστοποιητικά στα οποία βασίζονται, σύμφωνα με συγκεκριμένους εθνικούς νόμους και κανονισμούς.
• Το Χ.Α. μπορεί να χρεώνει τέλη για τις υπηρεσίες που παρέχονται από την αρχή TSA του Χ.Α.
• Το εφαρμοστέο νομικό σύστημα και οι διαδικασίες επίλυσης διαφορών σχετικά με την αρχή TSA του Χ.Α. εξετάζονται στην υποκείμενη Συμφωνία Συνδρομητή.
• Τα αρχεία καταγραφής συμβάντων της αρχή TSA τηρούνται για 11 έτη, σε συμμόρφωση με την περίοδο τήρησης των αρχείων καταγραφής ελέγχου που προβλέπεται στην πολιτική CP/CPS.

8.2 Κύκλος ζωής διαχείρισης κλειδιών

8.2.1 Δημιουργία κλειδιών από την αρχή TSA

Το Χ.Α. παράγει τα κρυπτογραφικά κλειδιά που χρησιμοποιούνται στις υπηρεσίες που παρέχει η αρχή TSA υπό τον έλεγχο συγκεκριμένου αριθμού μελών του εξουσιοδοτημένου προσωπικού σε ασφαλές φυσικό περιβάλλον. Το προσωπικό που είναι εξουσιοδοτημένο να ασκεί τη λειτουργία αυτή περιορίζεται σε εκείνους που απαιτείται να το πράξουν σύμφωνα με τις πρακτικές του Χ.Α. Τα κλειδιά δημιουργούνται μέσα σε δομοστοιχεία ασφάλειας του υλισμικού της μονάδας TSU που είναι πιστοποιημένα στο επίπεδο 3 του προτύπου FIPS 140-2. Οι αλγόριθμοι και το μέγεθος του κλειδιού περιγράφονται στην ενότητα 8.1.2 («Γνωστοποίηση αρχής TSA») του παρόντος εγγράφου.

8.2.2 Προστασία ιδιωτικού κλειδιού TSU

Το Χ.Α. λαμβάνει συγκεκριμένα μέτρα ώστε να διασφαλίζει ότι τα ιδιωτικά κλειδιά TSU παραμένουν εμπιστευτικά και διατηρούν την ακεραιότητά τους. Αυτά τα μέτρα περιλαμβάνουν τη χρήση ιεραρχικών συστημάτων αποθήκευσης (HSM) που έχουν πιστοποιηθεί στο επίπεδο 3 ή άνω του προτύπου FIPS 140-2 για τήρηση κλειδιών και υπογραφή μέσω αυτών. Όταν δημιουργούνται αντίγραφα ασφαλείας των ιδιωτικών κλειδιών TSU, αυτά αντιγράφονται, αποθηκεύονται και ανακτώνται μόνο από προσωπικό με ρόλους εμπιστοσύνης, χρησιμοποιώντας τουλάχιστον διπλό έλεγχο σε φυσικά ασφαλές περιβάλλον. Το προσωπικό που είναι εξουσιοδοτημένο να ασκεί τη λειτουργία αυτή περιορίζεται σε εκείνους που απαιτείται να το πράξουν σύμφωνα με τις πρακτικές του Χ.Α.

8.2.3 Διανομή δημόσιων κλειδιών TSU

Τα δημόσια κλειδιά TSU του Χ.Α. είναι διαθέσιμα για ψηφιακά πιστοποιητικά. Ανατρέξτε στην ενότητα «Αρχή χρονοσήμανσης του Χ.Α.» του ακόλουθου ιστοτόπου του Χ.Α., για τη λίστα με τις μονάδες TSU του Χ.Α.
http://www.athexgroup.gr/digital-certificates-repository

8.2.4 Αλλαγή κλειδιού TSU

Τα ιδιωτικά κλειδιά για υπογραφή που εκδίδονται από τη μονάδα TSU αντικαθίστανται πριν από το τέλος της περιόδου ισχύος τους (δηλαδή, όταν ο αλγόριθμος ή το μέγεθος κλειδιού προσδιορίζεται ως ευάλωτο).

8.2.5 Τέλος του κύκλου ζωής του κλειδιού TSU

Τα ιδιωτικά κλειδιά για υπογραφή που εκδίδονται από τη μονάδα TSU αντικαθίστανται κατά τη λήξη τους. Η μονάδα TSU απορρίπτει κάθε απόπειρα έκδοσης χρονοσημάνσεων μετά τη λήξη ενός ιδιωτικού κλειδιού.

8.2.6 Διαχείριση κύκλου ζωής του κρυπτογραφικού δομοστοιχείου που χρησιμοποιείται για τις χρονοσημάνσεις υπογραφής

Το Χ.Α. έχει θεσπίσει διαδικασίες για να διασφαλίζει ότι τα δομοστοιχεία ασφαλείας του υλισμικού που προορίζονται για υπηρεσίες χωρίς τη δυνατότητα αποκήρυξης δεν παραβιάζονται κατά την αποστολή ή την αποθήκευσή τους. Κατά τη παραλαβή, εκτελείται έλεγχος προκειμένου να επαληθευθεί ότι το κρυπτογραφικό υλισμικό λειτουργεί σωστά. Η εγκατάσταση και η ενεργοποίηση εκτελούνται μόνο από συγκεκριμένο αριθμό έμπιστων μελών του εξουσιοδοτημένου προσωπικού και οι συσκευές λειτουργούν σε φυσικά ασφαλές περιβάλλον. Τα ιδιωτικά κλειδιά διαγράφονται από τα δομοστοιχεία όταν αφαιρούνται από την υπηρεσία σύμφωνα με τις οδηγίες του κατασκευαστή.

8.3 Χρονοσήμανση

8.3.1 Αδειοδοτικά χρονοσήμανσης

Το Χ.Α. έχει θεσπίσει τεχνικές προδιαγραφές προκειμένου να διασφαλίζει ότι τα αδειοδοτικά TST εκδίδονται με ασφάλεια και περιλαμβάνουν τη σωστή ώρα. Σύμφωνα με τα πρωτόκολλα που αναφέρονται στην ενότητα 3 του παρόντος εγγράφου, κάθε αδειοδοτικό TST περιλαμβάνει:

- μια αναπαράσταση (π.χ., τιμή σύνοψης) του δεδομένου που φέρει χρονοσήμανση όπως παρέχεται από τον αιτούντα,
- έναν μοναδικό αύξοντα αριθμό που μπορεί να χρησιμοποιηθεί τόσο για την παραγγελία αδειοδοτικών TST όσο και για την ταυτοποίηση συγκεκριμένων αδειοδοτικών TST,
- ένα χαρακτηριστικό αναγνώρισης για την πολιτική χρονοσήμανσης,

- τον χρόνο βαθμονομημένο εντός 1 δευτερολέπτου από την UTC, διακριβωμένο από συγκεκριμένη χρονική πηγή UTC(k).
- μια ηλεκτρονική υπογραφή που παράγεται με τη χρήση κλειδιού που χρησιμοποιείται αποκλειστικά για χρονοσήμανση και
- ένα χαρακτηριστικό αναγνώρισης για την αρχή TSA και τη μονάδα TSU.

Οι μονάδες TSU του Χ.Α. τηρούν αρχεία καταγραφής ελέγχου για όλες τις βαθμονομήσεις έναντι των σημείων αναφοράς UTC(k).

8.3.2 Συγχρονισμός ρολογιού με την ώρα UTC

Η αρχή TSA του Χ.Α. παρέχει χρόνο ακρίβειας εντός ± 1 δευτερολέπτου έναντι της UTC μέσω βαθμονόμησης με πολλαπλές ανεξάρτητες χρονικές πηγές, συμπεριλαμβανομένου του συστήματος GPS και των Εθνικών Ινστιτούτων Μετρήσεων που παρέχουν ώρα UTC(k).
Οι μονάδες TSU του Χ.Α. διαθέτουν τεχνικά μέτρα για να διασφαλίζουν ότι ο χρόνος τους συγχρονίζεται με την ώρα UTC στο πλαίσιο της δηλωμένης ακρίβειας. Τα αρχεία ελέγχου και βαθμονόμησης τηρούνται από το Χ.Α. Η αρχή TSA του Χ.Α. διασφαλίζει ότι ο συγχρονισμός των ρολογιών θα διατηρείται σε περίπτωση πηδήματος δευτερολέπτου όπως γνωστοποιείται από τον αρμόδιο φορέα.
Τα ρολόγια των μονάδων TSU προστατεύονται και βαθμονομούνται τουλάχιστον δύο φορές την ημέρα έναντι του σημείου αναφοράς χρόνου UTC. Τα ρολόγια των μονάδων TSU είναι επίσης σε θέση να παρακολουθήσουν τη χρονική μετατόπιση εκτός των προκαθορισμένων ορίων και να ζητήσουν επιπλέον αναβαθμονομήσεις ανάλογα με τις ανάγκες. Εάν το ρολόι TSU μετακινηθεί εκτός της δηλωμένης ακρίβειας και η αναβαθμονόμηση αποτύχει, η αρχή TSA δεν θα εκδίδει χρονοσημάνσεις αν δεν αποκατασταθεί η σωστή ώρα. Η χειροκίνητη διαχείριση του ρολογιού της μονάδας TSU απαιτεί συγκεκριμένο αριθμό μελών εξουσιοδοτημένου προσωπικού.

8.4 Διαχείριση και λειτουργία αρχής TSA

8.4.1 Διαχείριση ασφαλείας

Το Χ.Α. διαθέτει ενεργό πρόγραμμα διαχείρισης της ασφάλειας που έχει σχεδιαστεί για να τεκμηριώνει, να υλοποιεί και να διατηρεί επαρκείς διατάξεις ασφαλείας για το σύστημα PKI σύμφωνα με τις βέλτιστες πρακτικές και τις απαιτήσεις των σχετικών προτύπων. Η Υπηρεσία Διαχείρισης Πολιτικών του Χ.Α. είναι ο αρμόδιος φορέας για τον καθορισμό πολιτικών και πρακτικών για το σύνολο του συστήματος PKI και, ως εκ τούτου, είναι υπεύθυνη για τον ορισμό της Πολιτικής Ασφάλειας Πληροφοριών του Χ.Α.

8.4.2 Ταξινόμηση και διαχείριση περιουσιακών στοιχείων

Προκειμένου να διασφαλιστεί ότι οι πληροφορίες και άλλα περιουσιακά στοιχεία λαμβάνουν την κατάλληλη μεταχείριση ασφάλειας, το Χ.Α. διατηρεί απογραφή όλων των περιουσιακών στοιχείων και ιεραρχεί τις απαιτήσεις προστασίας για τα εν λόγω περιουσιακά στοιχεία ανάλογα με την ανάλυση κινδύνου.

8.4.3 Ασφάλεια προσωπικού

Προκειμένου να ενισχύσει την αξιοπιστία των λειτουργιών του συστήματος PKI, το Χ.Α. διατηρεί κατάλληλες πρακτικές προσωπικού που πληρούν τις βέλτιστες πρακτικές ασφαλείας και τις απαιτήσεις των σχετικών προτύπων.

Ειδικότερα:

α) Το Χ.Α. απασχολεί προσωπικό το οποίο διαθέτει τις γνώσεις, την εμπειρία και τα προσόντα που απαιτούνται για τις προσφερόμενες υπηρεσίες και αρμόζουν στις λειτουργίες του.
β) Οι ρόλοι και οι ευθύνες ασφαλείας συνοψίζονται στις περιγραφές των θέσεων εργασίας. Οι ρόλοι εμπιστοσύνης, από τους οποίους εξαρτάται η ασφάλεια της λειτουργίας του Χ.Α., προσδιορίζονται σαφώς στην πολιτική CP/CPS.
γ) Οι περιγραφές των θέσεων εργασίας του προσωπικού του Χ.Α. βασίζονται στη αρχή του διαχωρισμού των καθηκόντων και στην αρχή των ελάχιστων προνομίων, καθορίζοντας την ευαισθησία της θέσης με βάση τα επίπεδα καθηκόντων και πρόσβασης, τον έλεγχο του ιστορικού και την κατάρτιση και επίγνωση των εργαζομένων.
δ) Το προσωπικό ασκεί διοικητικές και διαχειριστικές διαδικασίες που συνάδουν με την Πολιτική Ασφάλειας Πληροφοριών του Χ.Α.

Για τη διαχείριση της χρονοσήμανσης εφαρμόζονται οι ακόλουθοι συμπληρωματικοί έλεγχοι:

ε) Θα απασχολείται διοικητικό προσωπικό με:

- γνώση της τεχνολογίας χρονοσήμανσης,
- γνώση της τεχνολογίας ψηφιακών υπογραφών,
- γνώση των μηχανισμών βαθμονόμησης ή συγχρονισμού των ρολογιών των μονάδων TSU με την ώρα UTC.
- εξοικείωση με τις διαδικασίες ασφαλείας για προσωπικό με αρμοδιότητες στον τομέα της ασφάλειας και
- εμπειρία όσον αφορά την ασφάλεια των πληροφοριών και την αξιολόγηση των κινδύνων.

στ) Για κανένα μέλος του προσωπικού του Χ.Α. σε ρόλους εμπιστοσύνης δεν πρέπει να υπάρχει σύγκρουση συμφερόντων που θα μπορούσε να επηρεάσει την αμεροληψία των λειτουργιών της αρχής TSA.
ζ) Οι ρόλοι εμπιστοσύνης περιλαμβάνουν εκείνους με τις ακόλουθες ευθύνες:
- Στελέχη ασφαλείας: Γενική ευθύνη για τη διαχείριση της υλοποίησης των πρακτικών ασφαλείας.
- Διαχειριστές συστήματος: Εξουσιοδοτημένοι να εγκαθιστούν, να διαμορφώνουν και να διατηρούν τα αξιόπιστα συστήματα της αρχής TSA για τη διαχείριση της χρονοσήμανσης εγγράφων.

- Χειριστές συστήματος: Υπεύθυνοι για τη λειτουργία των αξιόπιστων συστημάτων της αρχής TSA σε καθημερινή βάση. Εξουσιοδοτημένοι να δημιουργούν εφεδρικά αντίγραφα και να εκτελούν αποκατάσταση του συστήματος.
- Ελεγκτές συστημάτων: Εξουσιοδοτημένοι να βλέπουν αρχεία και αρχεία καταγραφής ελέγχου των αξιόπιστων συστημάτων της αρχής TSA.

η) Το προσωπικό της αρχής TSA διορίζεται επισήμως σε ρόλους εμπιστοσύνης από ανώτερα διευθυντικά στελέχη αρμόδια για την ασφάλεια.
θ) Η αρχή TSA δεν διορίζει σε ρόλους εμπιστοσύνης ή στη διοίκηση πρόσωπα που είναι γνωστό ότι έχουν καταδικαστεί για σοβαρό έγκλημα ή άλλο αδίκημα που επηρεάζει την καταλληλότητά τους για τη θέση. Το προσωπικό δεν θα έχει πρόσβαση στις λειτουργίες εμπιστοσύνης μέχρι την ολοκλήρωση των αναγκαίων ελέγχων του ιστορικού του.

8.4.4 Φυσική και περιβαλλοντική ασφάλεια

Η αρχή TSA του Χ.Α. λειτουργεί από μια ευέλικτη και ασφαλή εγκατάσταση φιλοξενίας σε συμμόρφωση με τις σχετικές διατάξεις του προτύπου ETSI EN 319 421.

Ειδικότερα:

α) Τόσο για την παροχή όσο και για τη διαχείριση της χρονοσήμανσης:

- η φυσική πρόσβαση σε εγκαταστάσεις που αφορούν υπηρεσίες χρονοσήμανσης εγγράφων περιορίζεται σε άτομα με κατάλληλη εξουσιοδότηση,
- εφαρμόζονται έλεγχοι προκειμένου να αποφευχθεί η απώλεια, η ζημία ή η διαρροή περιουσιακών στοιχείων και η διακοπή των επιχειρηματικών δραστηριοτήτων και
- εφαρμόζονται έλεγχοι προκειμένου να αποφευχθεί η διαρροή ή η κλοπή πληροφοριών και εγκαταστάσεων επεξεργασίας πληροφοριών.

β) Έλεγχοι πρόσβασης εφαρμόζονται στα κρυπτογραφικά δομοστοιχεία ώστε να πληρούνται οι απαιτήσεις ασφαλείας των κρυπτογραφικών δομοστοιχείων όπως προσδιορίζονται στις διατάξεις 8.2.1 και 8.2.2.
γ) Για τη διαχείριση της χρονοσήμανσης έχουν εφαρμοστεί οι ακόλουθοι συμπληρωματικοί έλεγχοι:

- Οι εγκαταστάσεις διαχείρισης της χρονοσήμανσης εγγράφων λειτουργούν σε ένα περιβάλλον το οποίο προστατεύει φυσικά τις υπηρεσίες από διαρροές λόγω μη εξουσιοδοτημένης πρόσβασης σε συστήματα ή δεδομένα.

- Η φυσική προστασία επιτυγχάνεται μέσω της δημιουργίας σαφώς καθορισμένων περιμέτρων ασφαλείας (δηλαδή φυσικών φραγμών) γύρω από τις εγκαταστάσεις διαχείρισης της χρονοσήμανσης. Τυχόν τμήματα της εγκατάστασης που είναι κοινά με άλλους οργανισμούς βρίσκονται εκτός αυτής της περιμέτρου.
- Υλοποιούνται έλεγχοι φυσικής και περιβαλλοντικής ασφάλειας για την προστασία της εγκατάστασης που φιλοξενεί τους πόρους του συστήματος, των ίδιων των πόρων του συστήματος και των εγκαταστάσεων που χρησιμοποιούνται για τη στήριξη της λειτουργίας τους. Η

Πολιτική Ασφαλείας Πληροφοριών του Χ.Α. εξετάζει τον έλεγχο της φυσικής πρόσβασης, τους παράγοντες πυρασφάλειας, τις βλάβες υπηρεσιών κοινής ωφέλειας (π.χ. ηλεκτροδότηση, τηλεπικοινωνίες), την προστασία από κλοπή, διάρρηξη και είσοδο και την αποκατάσταση καταστροφών.

- Εφαρμόζονται έλεγχοι για την αποτροπή της μη εξουσιοδοτημένης απομάκρυνσης εξοπλισμού, πληροφοριών, μέσων και λογισμικού που σχετίζονται με τις υπηρεσίες χρονοσήμανσης εκτός των εγκαταστάσεων.

8.4.5 Διαχείριση λειτουργιών

Το σύστημα PKI του Χ.Α. προβλέπει εκτεταμένους λειτουργικούς ελέγχους σύμφωνα με το πρότυπο ETSI EN 319 421. Αυτή η τεκμηρίωση δεν είναι διαθέσιμη στο κοινό. Το Χ.Α. πραγματοποιεί εσωτερικές και εξωτερικές αναθεωρήσεις της συμμόρφωσης και της αποτελεσματικότητας αυτών των ελέγχων. Οι έλεγχοι διαχείρισης λειτουργιών για την αρχή TSA του Χ.Α. ενσωματώνονται στους γενικούς ελέγχους διαχείρισης λειτουργιών του Χ.Α.

8.4.6 Διαχείριση πρόσβασης στο σύστημα

Το Χ.Α. διατηρεί τους κατάλληλους ελέγχους φυσικής και λογικής πρόσβασης για τις επηρεαζόμενες εγκαταστάσεις, υλισμικό, συστήματα και πληροφορίες. Οι έλεγχοι διαχείρισης πρόσβασης στο σύστημα για την αρχή TSA του Χ.Α. ενσωματώνονται στους γενικούς ελέγχους διαχείρισης πρόσβασης στο σύστημα του Χ.Α.

8.4.7 Ανάπτυξη και συντήρηση αξιόπιστων συστημάτων

Η αρχή TSA του Χ.Α. χρησιμοποιεί αξιόπιστα συστήματα που προστατεύονται από τροποποίηση. Οι έλεγχοι ανάπτυξης και συντήρησης των συστημάτων της αρχής TSA του Χ.Α. ενσωματώνονται στους γενικούς ελέγχους ανάπτυξης και συντήρησης συστημάτων του συστήματος PKI του Χ.Α.

8.4.8 Διαρροή υπηρεσιών της αρχής TSA

Σε περίπτωση διαρροής κάποιου ιδιωτικού κλειδιού μιας μονάδας TSU, το Χ.Α. θα ανακαλέσει το σχετικό πιστοποιητικό και θα το προσθέσει στη λίστα CRL του Χ.Α. Η μονάδα TSU δεν θα εκδίδει χρονοσημάνσεις εάν το ιδιωτικό κλειδί της δεν είναι έγκυρο.

Η μονάδα TSU δεν θα εκδίδει χρονοσημάνσεις εάν το ρολόι της μετακινηθεί εκτός της δηλωμένης ακρίβειας σε σχέση με την ώρα αναφοράς UTC, έως ότου ληφθούν μέτρα για την αποκατάσταση της βαθμονόμησης του χρόνου. Όπως περιγράφεται στην ενότητα 8.4.11 («Καταγραφή πληροφοριών σχετικά με τη λειτουργία των υπηρεσιών χρονοσήμανσης εγγράφων») του παρόντος εγγράφου, η αρχή TSA του Χ.Α. τηρεί διαγράμματα ελέγχου για τη διάκριση μεταξύ αυθεντικών και προχρονολογημένων αδειοδοτικών.

8.4.9 Τερματισμός λειτουργίας της αρχής TSA

Σε περίπτωση τερματισμού της λειτουργίας της αρχής TSA του Χ.Α., το Χ.Α. θα ενημερώσει τουλάχιστον τους συνδρομητές, θα ανακαλέσει τα πιστοποιητικά TSU και θα μεταφέρει τις υποχρεώσεις σε αξιόπιστο συμβαλλόμενο μέρος για τη διατήρηση των αρχείων καταγραφής συμβάντων και ελέγχου καθώς και για πρόσβαση σε ιδιωτικά κλειδιά.

8.4.10 Συμμόρφωση με τις νομικές απαιτήσεις

Η αρχή TSA του Χ.Α. συμμορφώνεται με τις ισχύουσες νομικές απαιτήσεις, καθώς και με τις απαιτήσεις της Ευρωπαϊκής Οδηγίας για την προστασία των δεδομένων [οδηγία 95/46/ΕΚ]. Λαμβάνονται κατάλληλα τεχνικά και οργανωτικά μέτρα κατά της μη εξουσιοδοτημένης ή παράνομης επεξεργασίας δεδομένων προσωπικού χαρακτήρα και κατά της τυχαίας απώλειας ή καταστροφής προσωπικών δεδομένων ή ζημίας σε αυτά. Οι πληροφορίες που δίνουν οι χρήστες στην αρχή TSA πρέπει να προστατεύονται πλήρως από γνωστοποίηση, με εξαίρεση τις περιπτώσεις όπου υπάρχει συναίνεση, δικαστική απόφαση ή άλλη νομική απαίτηση.

8.4.11 Καταγραφή πληροφοριών σχετικά με τη λειτουργία υπηρεσιών χρονοσήμανσης εγγράφων

Το Χ.Α. διατηρεί αρχεία όλων των σχετικών πληροφοριών που αφορούν τη λειτουργία της αρχής TSA του Χ.Α. για περίοδο 11 ετών, σύμφωνα με τις επιχειρηματικές πρακτικές του Χ.Α. Τα αρχεία φέρουν χρονοσήμανση για την προστασία της ακεραιότητας των δεδομένων και μετακινούνται σε προστατευμένο διακομιστή για αποθήκευση και επακόλουθη αρχειοθέτηση. Δεν μεταδίδονται προσωπικά δεδομένα σχετικά με συνδρομητές μεταξύ δικαιοδοσιών.
Τα αρχεία που αφορούν τη λειτουργία των υπηρεσιών χρονοσήμανσης εγγράφων είναι διαθέσιμα κατόπιν αιτήματος των συνδρομητών ή εάν απαιτηθεί από δικαστική απόφαση ή άλλη νομική απαίτηση. Η αρχή TSA του Χ.Α. διατηρεί αρχεία, συμπεριλαμβανομένου του ακριβούς χρόνου, για:

- Αιτήσεις χρονοσήμανσης και χρονοσημάνσεις που δημιουργήθηκαν
- Γεγονότα που σχετίζονται με τη διοίκηση της αρχής TSA (συμπεριλαμβανομένης της διαχείρισης πιστοποιητικών, της διαχείρισης κλειδιών και του συγχρονισμού ρολογιών).

- Γεγονότα σχετικά με τον κύκλο ζωής των κλειδιών και πιστοποιητικών TSU.

8.5 Οργανωτικά θέματα

Η οργανωτική δομή, οι πολιτικές, οι διαδικασίες και οι έλεγχοι του Χ.Α. ισχύουν για την αρχή TSA του Χ.Α. Οι διαδικασίες οργάνωσης του Χ.Α. πληρούν τα πρότυπα της ενότητας 2 («Παραπομπές») του παρόντος εγγράφου και, ειδικότερα, το πρότυπο ETSI EN 319 421. Σημαντικά έγγραφα πολιτικής και πρακτικής για το σύστημα PKI του Χ.Α. διατίθενται στη διεύθυνση http://www.athexgroup.gr/digital-certificates-pki-regulations.

8.6 Συμμόρφωση με τον εφαρμοστέο νόμο

Οι συνδρομητές και τα τρίτα βασιζόμενα μέρη αναγνωρίζουν και συμφωνούν να χρησιμοποιούν τα πιστοποιητικά σύμφωνα με όλους τους ισχύοντες νόμους και κανονισμούς. Η ΕΛΛΗΝΙΚΑ ΧΡΗΜΑΤΙΣΤΗΡΙΑ – ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ Α.Ε. ΣΥΜΜΕΤΟΧΩΝ μπορεί να αρνηθεί να εκδώσει ή ενδέχεται να ανακαλέσει Πιστοποιητικά εάν, κατά την εύλογη γνώμη της ΕΛΛΗΝΙΚΑ ΧΡΗΜΑΤΙΣΤΗΡΙΑ –

ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ Α.Ε. ΣΥΜΜΕΤΟΧΩΝ, η έκδοση ή συνέχιση της χρήσης των εν λόγω πιστοποιητικών θα παραβίαζε τους ισχύοντες νόμους και κανονισμούς.

8.7 Διάφορες διατάξεις

8.7.1 Πλήρης συμφωνία

Δεν ισχύει

8.7.2 Εκχώρηση

8.7.3 Διαχωρισμός

Εάν κάποια διάταξη του παρόντος κανονισμού CPS κριθεί άκυρη, παράνομη ή μη εκτελεστή, η εγκυρότητα, η νομιμότητα ή η εκτελεστότητα του υπολοίπου κανονισμού CPS δεν θα επηρεαστεί ούτε θα θιγεί με κανένα τρόπο από αυτό.

8.7.4 Εκτέλεση (αμοιβές δικηγόρου και παραίτηση από δικαιώματα)

Δεν ισχύει

8.7.5 Ανωτέρα βία

Η ΕΛΛΗΝΙΚΑ ΧΡΗΜΑΤΙΣΤΗΡΙΑ – ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ Α.Ε. ΣΥΜΜΕΤΟΧΩΝ δεν θα είναι υπεύθυνη για τυχόν αθέτηση ή καθυστέρηση στην εκπλήρωση των υποχρεώσεων που υπέχει δυνάμει του παρόντος, στο μέτρο που η αθέτηση ή η καθυστέρηση προκαλείται, άμεσα ή έμμεσα, από πυρκαγιές, πλημμύρες, σεισμούς, φυσικά φαινόμενα ή θεομηνίες, πράξεις πολέμου, τρομοκρατία, ταραχές, διαδηλώσεις, εξεγέρσεις, ανταπεργίες ή εργασιακές δυσκολίες ή οποιαδήποτε άλλη παρόμοια αιτία πέρα από τον εύλογο έλεγχο της ΕΛΛΗΝΙΚΑ ΧΡΗΜΑΤΙΣΤΗΡΙΑ – ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ Α.Ε. ΣΥΜΜΕΤΟΧΩΝ.

8.8 Λοιπές προβλέψεις

Δεν ισχύει.