

Αρχή Πιστοποίησης Ελληνικού Δημοσίου



Δήλωση Γνωστοποίησης Αρχής Χρονοσφραγίδας

Έκδοση 1.1

Ιστορικό εκδόσεων

Ημερομηνία	Έκδοση	Μεταβολές
15/12/2021	1.0	Αρχικό έγγραφο
14/5/2024	1.1	Διορθώσεις τυπογραφικών λαθών

1. Επισκόπηση

Το παρόν έγγραφο αποσκοπεί στην παροχή προς τον Συνδρομητή και τα Βασιζόμενα Μέρη Εγκεκριμένων Χρονοσφραγίδων σύνοψη των πληροφοριών, οι οποίες είναι διαθέσιμες στη Δήλωση Πρακτικής Πιστοποίησης (ΔΠΠ) της Αρχής Χρονοσφραγίδας της ΑΠΕΔ και στους Γενικούς Όρους και Προϋποθέσεις Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης της ΑΠΕΔ.

Το παρόν έγγραφο δεν υποκαθιστά ή αντικαθιστά ούτε τους Γενικούς Όρους και Προϋποθέσεις της ΑΠΕΔ ούτε την Πολιτική Πιστοποιητικού (ΠΠ) ή ΔΠΠ, παρά μόνο συνοψίζει τα βασικά σημεία προς όφελος των Συνδρομητών και των Βασιζόμενων Μερών.

2. Στοιχεία Επικοινωνίας

Αρχή Πιστοποίησης Ελληνικού Δημοσίου (ΑΠΕΔ)

Εγκεκριμένος Πάροχος Υπηρεσιών Εμπιστοσύνης

Διεύθυνση:

Υπουργείο Ψηφιακής Διακυβέρνησης

Διεύθυνση Ηλεκτρονικής Διακυβέρνησης

Φραγκούδη 11 & Αλ. Πάντου, 101 63 Καλλιθέα

email: aped@mindigital.gr

τηλέφωνο: 210-9098505

3. Κατηγορίες Ηλεκτρονικών Χρονοσφραγίδων και Χρήση

Εφαρμοστέα Πολιτική

Η Πολιτική Πιστοποιητικού και Δήλωση Πρακτικών Πιστοποιητικού της ΑΠΕΔ βασίζεται στην Πολιτική Βέλτιστων Πρακτικών Χρονοσφραγίδας του ETSI BTSP (OID 0.4.0.2023.1.1).

Κατηγορίες Χρονοσφραγίδων, Αναμενόμενος χρόνος ζωής Χρονοσφραγίδας

Οι Χρονοσφραγίδες που εκδίδει η ΑΠΕΔ είναι Εγκεκριμένες βάσει του Κανονισμού eIDAS.

Η δήλωση "esi4-qtstStatement-1" όπως ορίζεται στο ETSI EN 319 422 χρησιμοποιείται ως ένδειξη ότι η χρονοσφραγίδα είναι εγκεκριμένη.

Οι Υπηρεσίες Χρονοσφραγίδας μπορούν να χρησιμοποιηθούν είτε ανεξάρτητα είτε σε συνδυασμό με ένα Πιστοποιητικό για Ηλεκτρονική Υπογραφή ή Σφραγίδα, προς απόδειξη ότι δεδομένα σε ηλεκτρονική μορφή υπήρχαν σε συγκεκριμένο χρόνο.

Η αναμενόμενη περίοδος ισχύος της Μονάδας Χρονοσήμανσης (MX) της ΑΠΕΔ είναι πέντε (5) έτη.

Οι λειτουργίες κρυπτογραφικού κατακερματισμού (hashing) που χρησιμοποιούνται στη διαδικασία χρονοσφράγισης είναι σύμφωνες με τις κανονιστικές απαιτήσεις SHA-256 and SHA-512.

Χρήση Χρονοσφραγίδων

Οι Υπηρεσίες Χρονοσφραγίδας δεν πρέπει να χρησιμοποιούνται εκτός των ορίων και των πλαισίων που ορίζονται στην Πολιτική Πιστοποιητικού και Δήλωση Πρακτικών Πιστοποιητικού της Αρχής Χρονοσφραγίδας της ΑΠΕΔ και για παράνομους σκοπούς ή αντίθετους προς το δημόσιο συμφέρον. Ενδεικτικά, απαγορεύεται η Χρήση Χρονοσφραγίδων για οποιονδήποτε από τους ακόλουθους σκοπούς:

- παράνομη δραστηριότητα (συμπεριλαμβανομένων επιθέσεων στον κυβερνοχώρο)
- έκδοση νέων Χρονοσφραγίδων και πληροφορίες σχετικά με την ισχύ της Χρονοσφραγίδας
- δυνατότητα χρήσης της υπηρεσίας Χρονοσφραγίδας του Συνδρομητή από άλλα μέρη
- χρήση της Χρονοσφραγίδας που έχει εκδοθεί για την χρονοσφράγιση εγγράφων που μπορεί να προκαλέσουν ανεπιθύμητες συνέπειες (συμπεριλαμβανομένης της υπογραφής τέτοιων εγγράφων για δοκιμαστικούς σκοπούς).

Πληροφορίες για την επαλήθευση των χρονοσφραγίδων

- Οι Χρονοσφραγίδες μπορούν να επαληθευθούν όπως περιγράφεται στην Ενότητα 5 και 6 του παρόντος εγγράφου.

4. Όρια Εμπιστοσύνης

Ισχύς Χρονοσφραγίδων

Οι Χρονοσφραγίδες ισχύουν από την ημερομηνία που καθορίζεται σε αυτές. Η ισχύς των Χρονοσφραγίδων λήγει κατά την ημερομηνία λήξης που αναφέρεται στη Χρονοσφραγίδα ή εάν ανακληθεί το Πιστοποιητικό της ΜΧ.

Η Αρχή Χρονοσφραγίδας της ΑΠΕΔ διασφαλίζει ότι τα ιδιωτικά κλειδιά της Μονάδας Χρονοσφραγίδας δεν χρησιμοποιούνται πέραν του τέλους του κύκλου ζωής τους.

Το σύστημα δημιουργίας Διακριτικών Χρονοσφραγίδας θα απορρίψει κάθε προσπάθεια έκδοσης Διακριτικού Χρονοσφραγίδας εάν το ιδιωτικό κλειδί υπογραφής έχει λήξει ή εάν έχει λήξει η περίοδος χρήσης του ιδιωτικού κλειδιού υπογραφής.

Ακρίβεια χρόνου

Η ΑΠΕΔ διασφαλίζει ότι τα Διακριτικά Χρονοσφραγίδας εκδίδονται με ασφάλεια και περιέχουν τη σωστή ώρα. Η Αρχή Χρονοσφραγίδας (ΑΧ) της ΑΠΕΔ διασφαλίζει ότι η ώρα της συγχρονίζεται με UTC εντός της δηλωθείσας ακρίβειας με πολλαπλές ανεξάρτητες πηγές χρόνου. Τα Διακριτικά

Χρονοσφραγίδας εκδίδονται με ακρίβεια ενός (1) δευτερολέπτου. Η ΑΠΕΔ εφαρμόζει ελέγχους ασφαλείας που εμποδίζουν τη μη εξουσιοδοτημένη λειτουργία, με σκοπό τη βαθμονόμηση του χρόνου της ΑΧ εκτός λειτουργίας. Η ΑΠΕΔ παρακολουθεί ότι ο συγχρονισμός διατηρείται όταν προκύψει ένα άλμα δευτερολέπτου.

Διατήρηση αρχείων καταγραφής

Η ΑΠΕΔ διασφαλίζει ότι:

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

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

5. Υποχρεώσεις Συνδρομητή

Ο Συνδρομητής των Υπηρεσιών Χρονοσφραγίδας πρέπει να επαληθεύει τις υπογραφές που δημιούργησε η ΑΧ της ΑΠΕΔ στο Διακριτικό Χρονοσφραγίδας (ΔΧ). Η επαλήθευση αυτή περιλαμβάνει:

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

Ο Συνδρομητής πρέπει να χρησιμοποιεί ασφαλείς κρυπτογραφικές λειτουργίες για αιτήσεις χρονοσφραγίδων. Οι υποχρεώσεις των Συνδρομητών ορίζονται επίσης στους Όρους και Προϋποθέσεις για τη Χρήση Εγκεκριμένων Πιστοποιητικών της ΑΠΕΔ.

6. Υποχρέωση Ελέγχου Κατάστασης Πιστοποιητικού του Δημοσίου Κλειδιού της ΑΧ από τα Βασιζόμενα Μέρη

Το Βασιζόμενο Μέρος πρέπει να επαληθεύει τις υπογραφές που δημιούργησε η ΑΧ της ΑΠΕΔ στο ΔΧ. Η επαλήθευση αυτή περιλαμβάνει:

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

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

- Τα Βασιζόμενα Μέρη αναμένεται να χρησιμοποιήσουν τον Κατάλογο Εμπιστοσύνης για να διαπιστώσουν αν η ΜΧ και η χρονοσφραγίδα είναι εγκεκριμένες.

7. Περιορισμένη Εγγύηση και Δήλωση αποποίησης / Περιορισμός ευθύνης

Για περιορισμούς εγγύησης και ευθύνης, παρακαλούμε να ανατρέξετε στους Όρους και Προϋποθέσεις που είναι δημοσιευμένοι στον ιστότοπο της ΑΠΕΔ στο <https://pki.aped.gov.gr/repository>.

8. Ισχύουσες συμφωνίες, ΔΠ, ΔΠΠ

Σχετικές συμφωνίες, πολιτικές και δηλώσεις πρακτικών για τη χρήση των Πιστοποιητικών είναι:

- Η Πολιτική Πιστοποιητικού και η Δήλωση Πρακτικής Πιστοποίησης για Εγκεκριμένες Υπηρεσίες Χρονοσφραγίδας της ΑΠΕΔ
- Όροι και Προϋποθέσεις Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης της ΑΠΕΔ

Οι τελευταίες εκδόσεις όλων των εφαρμοστέων εγγράφων είναι διαθέσιμες στον Αποθηκευτικό χώρο της ΑΠΕΔ στο <https://pki.aped.gov.gr/repository>

9. Πολιτική Απορρήτου

Η ΑΠΕΔ επεξεργάζεται προσωπικά δεδομένα σύμφωνα με την ισχύουσα νομοθεσία για την προστασία τους. Για περισσότερες λεπτομέρειες, παρακαλούμε να ανατρέξετε στη Δήλωση Απορρήτου της ΑΠΕΔ: <https://pki.aped.gov.gr/repository>

10. Άδειες Αποθηκευτικού Χώρου, Σήματα Αξιοπιστίας και Έλεγχος

Οι Υπηρεσίες Εμπιστοσύνης της ΑΠΕΔ για τις Εγκεκριμένες Ηλεκτρονικές Υπογραφές και Εγκεκριμένες Χρονοσφραγίδες είναι καταχωρημένες στο Μητρώο παρόχων υπηρεσιών εμπιστοσύνης της Εθνικής Επιτροπής Τηλεπικοινωνιών και Ταχυδρομείων (ΕΕΤΤ):

<https://www.eett.gr/katanalotes/ypiresies-empistosynis/plirofories/mitroo-parochon-ypiresion-empistosynis/>

και στη σχετική Ευρωπαϊκή λίστα Εμπιστοσύνης:

<https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home>

Η απαίτηση της εν λόγω καταχώρισης είναι σύμφωνη με ισχύοντες κανονισμούς και πρότυπα.

Ο Οργανισμός αξιολόγησης της συμμόρφωσης έχει διαπιστευθεί σύμφωνα με τον κανονισμό (ΕΚ) αριθ. 765/2008 ως ικανός να αξιολογεί τη συμμόρφωση των Εγκεκριμένων Παρόχων Υπηρεσιών Εμπιστοσύνης και των Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης που παρέχουν. 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 ιστότοπο της ΑΠΕΔ στη διεύθυνση: <https://pki.aped.gov.gr/repository>.

11. Εφαρμοστέο δίκαιο, Καταγγελίες, Επίλυση διαφορών

Τυχόν διαφορές που σχετίζονται με τις υπηρεσίες εμπιστοσύνης που παρέχονται από την ΑΠΕΔ, διέπονται από την Ελληνική νομοθεσία. Ο Συνδρομητής πρέπει να ενημερώσει την ΑΠΕΔ σχετικά με οποιαδήποτε αξίωση ή διαμαρτυρία, το αργότερο εντός τριάντα (30) ημερολογιακών ημερών από τη θεμελίωση της βάσης της αξίωσης, εκτός εάν προβλέπεται διαφορετικά από τον νόμο. Εάν η διαφορά δεν επιλυθεί εντός εξήντα (60) ημερών μετά την αρχική ειδοποίηση, τότε το μέρος μπορεί να προσφύγει σε ένδικη διαδικασία επίλυσης. Τα δικαστήρια της Αθήνας στην Ελλάδα έχουν αποκλειστική δικαιοδοσία και είναι αρμόδια για την επίλυση οποιασδήποτε διαφοράς.