

# Αρχή Πιστοποίησης Ελληνικού Δημοσίου



## ΣΥΜΒΑΣΗ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΕΜΠΙΣΤΟΣΥΝΗΣ ΤΗΣ ΑΠΕΔ ΜΕ ΣΥΝΔΡΟΜΗΤΗ

### Γενικοί Όροι και Προϋποθέσεις Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης

(Εγκεκριμένες Ηλεκτρονικές Υπογραφές και Χρονοσφραγίδες)

Έκδοση 1.0

## Ιστορικό εκδόσεων

Ημερομηνία	Έκδοση	Μεταβολές
15/12/2021	1.0	Αρχικό έγγραφο

## Ακρωνύμια και Ορισμοί

### Ορισμοί

Πίνακας 1: Πίνακας Ορισμών

Όρος	Ορισμός
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.
OCSP (Online Certificate Status Protocol) / Πρωτόκολλο Δικτυακού Ελέγχου Κατάστασης Πιστοποιητικών	Το πρωτόκολλο που χρησιμοποιείται για την παροχή σε Βασιζόμενα Μέρη πληροφοριών σε πραγματικό χρόνο σχετικά με την κατάσταση των Πιστοποιητικών.
PKCS # 10	Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού (Public-Key Cryptography Standard) #10, που έχει αναπτυχθεί από τη RSA Security Inc., το οποίο καθορίζει τη δομή του Αιτήματος Υπογραφής Πιστοποιητικού.
PKCS # 12	Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού (Public-Key Cryptography Standard) #12, που έχει αναπτυχθεί από τη RSA Security Inc., το οποίο καθορίζει το ασφαλές μέσο για τη μεταβίβαση των ιδιωτικών κλειδιών
RSA	Το κρυπτογραφικό σύστημα δημοσίου κλειδιού που επινοήθηκε από τους Rivest, Shamir, και Adelman.
Secure Sockets Layer (SSL) / (Επίπεδα Ασφαλών Συνδέσεων)	Η καθιερωμένη (βιομηχανικά) μέθοδος για την προστασία των επικοινωνιών Δικτύου που αναπτύχθηκε από τη Netscape Communications Corporation. Το πρωτόκολλο ασφαλείας SSL παρέχει κρυπτογράφηση δεδομένων, ταυτοποίηση εξυπηρετητή (server), αρτιότητα μηνύματος, και προαιρετικά ταυτοποίηση χρήστη (client) για μία σύνδεση Transmission Control Protocol / Internet Protocol (Πρωτοκόλλου Ελέγχου Μετάδοσης/ Πρωτοκόλλου Διαδικτύου).
Αίτημα Πιστοποιητικού Signing Request)	Υπογραφής (Certificate) Μήνυμα που μεταφέρει το αίτημα για την έκδοση ενός Πιστοποιητικού.
Αίτηση για πιστοποιητικό	Το αίτημα από τον Αιτών για Πιστοποιητικό προς μια ΑΠ για την έκδοση ενός Πιστοποιητικού.
Αιτών Πιστοποιητικό	Φυσικό πρόσωπο που ζητά την έκδοση πιστοποιητικού από μια ΑΠ.
Ακριβής χρόνος	Η αναφορά στοιχείων με τα οποία προσδιορίζεται το έτος, ο μήνας, η ημερομηνία, η ώρα, τα λεπτά και τα δευτερόλεπτα. Για τους φορείς του Δημόσιου Τομέα, σύμφωνα με τις διατάξεις της παρούσας, ο ακριβής χρόνος προσδιορίζεται με βάση την Εθνική ώρα Ελλάδας.
Αλυσίδα Πιστοποιητικού	Ο κατάλογος κατά σειρά κατάταξης των Πιστοποιητικών που περιλαμβάνει ένα Πιστοποιητικό Συνδρομητή, Πιστοποιητικά της ΑΠ και καταλήγει σε ένα

	Πιστοποιητικό Βάσης (Root).
<b>ΑΠ βάσης</b>	Η αρχή πιστοποίησης η οποία βρίσκεται στο υψηλότερο επίπεδο εντός του τομέα του ΠΥΕ και η οποία χρησιμοποιείται για να υπογράψει ιεραρχικά υφιστάμενες ΑΠ.
<b>Αρχή Εγγραφής (ΑΕ)</b>	Οντότητα που έχει εγκριθεί από μια ΑΠ και υποβοηθά τους ενδιαφερόμενους για Πιστοποιητικά κατά την υποβολή των αιτήσεών τους, εγκρίνει ή απορρίπτει τις εγγραφές / αιτήσεις καθώς επίσης αιτείται στην Αρχή Πιστοποίησης την ανάκληση και επαναδημιουργία κλειδιών Πιστοποιητικών.
<b>Αρχή Πιστοποίησης (ΑΠ)</b>	Η οντότητα που έχει πιστοποιηθεί να εκδίδει, να χειρίζεται και να ανακαλεί Πιστοποιητικά.
<b>Ασφαλής Κρυπτογραφική Μονάδα (ΑΚΜ –HSM)</b>	Το χρησιμοποιούμενο από τους Παρόχους Υπηρεσιών Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών, Προϊόν Ηλεκτρονικής Υπογραφής που προστατεύεται έναντι τροποποίησης και διασφαλίζει τεχνική και κρυπτογραφική ασφάλεια.
<b>Βασιζόμενο Μέρος</b>	Το φυσικό ή νομικό πρόσωπο το οποίο βασίζεται σε ηλεκτρονική ταυτοποίηση ή σε υπηρεσία εμπιστοσύνης.
<b>Γενικοί Όροι και Προϋποθέσεις Χρήσης Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης</b>	Δεσμευτικό έγγραφο που καθορίζει του όρους και τις προϋποθέσεις βάσει των οποίων ένα φυσικό ή νομικό πρόσωπο ενεργεί ως Συνδρομητής ή ως Βασιζόμενο Μέρος και η ΑΠΕΔ παρέχει τις αντίστοιχες Υπηρεσίες Εμπιστοσύνης.
<b>Δήλωση Πρακτικής</b>	Δήλωση των πρακτικών τις οποίες εφαρμόζει μια Αρχή Πιστοποίησης κατά την έκδοση, τη διαχείριση, την ανάκληση, την ανανέωση ή την επαναδημιουργία κλειδιών πιστοποιητικών.
<b>Δημόσιο Κλειδί</b>	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.
<b>Διαδικασία Παραγωγής Κλειδιών</b>	Μια διαδικασία δια της οποίας παράγεται το ζεύγος κλειδιών μιας ΑΠ ή μιας ΑΕ, το ιδιωτικό κλειδί της μεταφέρεται σε μια κρυπτογραφική μονάδα, παράγεται εφεδρικό αντίγραφο του ιδιωτικού της κλειδιού και/ή πιστοποιείται το δημόσιο κλειδί της
<b>Δικαιώματα Ιδιοκτησίας Πνευματικής</b>	Δικαιώματα επί ενός ή περισσότερων από τα ακόλουθα: κάθε είδους δικαιώματος δημιουργού, εμπορικού μυστικού, εμπορικού σήματος, καθώς και κάθε άλλου δικαιώματος πνευματικής ιδιοκτησίας
<b>Εγκεκριμένη Διάταξη Δημιουργίας Ηλεκτρονικής Υπογραφής</b>	Διάταξη δημιουργίας ηλεκτρονικής υπογραφής που πληροί τις απαιτήσεις του παραρτήματος II του Κανονισμού eIDAS.
<b>Εγκεκριμένη υπογραφή ηλεκτρονική</b>	Προηγμένη ηλεκτρονική υπογραφή που δημιουργείται από εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής και βασίζεται σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής. Η εγκεκριμένη ηλεκτρονική υπογραφή έχει νομική ισχύ ισοδύναμη με την ιδιόχειρη υπογραφή. Εγκεκριμένη ηλεκτρονική υπογραφή βασιζόμενη σε εγκεκριμένο πιστοποιητικό που έχει εκδοθεί σε ένα κράτος μέλος αναγνωρίζεται ως τέτοια σε όλα τα άλλα κράτη μέλη. Δεν απορρίπτονται η νομική ισχύς και το παραδεκτό της ηλεκτρονικής υπογραφής ως αποδεικτικού στοιχείου σε νομικές διαδικασίες μόνο λόγω του γεγονότος ότι είναι σε ηλεκτρονική μορφή ή ότι δεν πληροί όλες τις απαιτήσεις για τις εγκεκριμένες ηλεκτρονικές υπογραφές, σύμφωνα με το Άρθρο 25 του

	Κανονισμού eIDAS.
<b>Εγκεκριμένο Πιστοποιητικό</b>	Το Εγκεκριμένο Πιστοποιητικό είναι ένα Πιστοποιητικό που εκδίδεται από μια ΑΠ και το οποίο έχει διαπιστευθεί και εποπτεύεται από αρχές που ορίζονται από κράτος μέλος της ΕΕ και πληροί τις απαιτήσεις του κανονισμού eIDAS.
<b>Εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής</b>	Πιστοποιητικό ηλεκτρονικής υπογραφής που εκδίδεται από εγκεκριμένο πάροχο υπηρεσιών εμπιστοσύνης και πληροί τις οριζόμενες απαιτήσεις στο Παράρτημα Ι του Κανονισμού eIDAS.
<b>Εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης</b>	Ο πάροχος υπηρεσιών εμπιστοσύνης ο οποίος παρέχει μία ή περισσότερες εγκεκριμένες υπηρεσίες εμπιστοσύνης και έχει αναγνωριστεί ως τέτοιος από τον Εποπτικό Φορέα.
<b>Εκδότης Αρχή Πιστοποίησης</b>	Η Αρχή Πιστοποίησης που εκδίδει Πιστοποιητικά σε Συνδρομητές ακολουθώντας τουλάχιστον μία εκ των πολιτικών πιστοποιητικών της ΑΠΕΔ. Στην έννοια των Εκδοτριών Αρχών Πιστοποίησης περιλαμβάνονται και οι ΥΠΑΠ.
<b>Έκθεση σε Κίνδυνο</b>	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, Έκθεση σε Κίνδυνο αποτελεί η απώλεια, κλοπή, αποκάλυψη, τροποποίηση, μη-εξουσιοδοτημένη χρήση, ή κάθε άλλη έκθεση σε κίνδυνο της ασφάλειας του ιδιωτικού αυτού κλειδιού.
<b>Έμπιστα Πρόσωπα</b>	Οι υπάλληλοι που έχουν πρόσβαση ή ελέγχουν τις κρυπτογραφικές διαδικασίες.
<b>Εμπιστευτικές/ Πληροφορίες</b>	<b>Προσωπικές</b> Οι πληροφορίες που είναι απαραίτητο να παραμείνουν εμπιστευτικές και προσωπικές.
<b>Εξ αποστάσεως ΕΔΔΥ</b>	Εγκεκριμένη Διάταξη Δημιουργίας Υπογραφής Εξ αποστάσεως που πληροί τις απαιτήσεις του Παραρτήματος ΙΙ του Κανονισμού eIDAS.
<b>Ηλεκτρονική Εγγραφή ή Αίτηση</b>	Η ηλεκτρονική διαδικασία που περιγράφεται στους Κανονισμούς Πιστοποίησης των ΥΠΑΠ και που αφορά στα βήματα που πρέπει να προβεί ο Συνδρομητής προκειμένου να αποκτήσει ψηφιακό πιστοποιητικό.
<b>Ηλεκτρονικό έγγραφο</b>	Οποιοδήποτε περιεχόμενο έχει αποθηκευτεί σε ηλεκτρονική μορφή και ειδικότερα ως κείμενο ή με ηχητική, οπτική ή οπτικοακουστική εγγραφή.
<b>Ιδιωτικό Κλειδί</b>	Το κλειδί ενός ζεύγους κλειδιών το οποίο διατηρείται κρυφό από τον κάτοχο του ζεύγους κλειδιών και το οποίο χρησιμοποιείται για τη δημιουργία εγκεκριμένων πιστοποιητικών ή για την αποκρυπτογράφηση ηλεκτρονικών αρχείων ή φακέλων που έχουν κρυπτογραφηθεί με το αντίστοιχο δημόσιο κλειδί.
<b>Κατάλογος Πιστοποιητικών (ΚΑΠ)</b>	<b>Ανακληθέντων</b> Ο περιοδικός (ή έκτακτος) κατάλογος που εκδίδεται ηλεκτρονικά και είναι υπογεγραμμένος από μια ΑΠ, των Πιστοποιητικών που έχουν ανακληθεί πριν από την ημερομηνία λήξης τους. Ο ΚΑΠ αναφέρει το όνομα του εκδότη της ΚΑΠ, την ημερομηνία έκδοσης, την ημερομηνία της επόμενης προγραμματισμένης έκδοσης ΚΑΠ, τους αριθμούς σειράς των ανακληθέντων Πιστοποιητικών, καθώς και τους συγκεκριμένους χρόνους και λόγους ανάκλησής τους.
<b>Κέντρο Επεξεργασίας</b>	Μια ασφαλής λογική και φυσική υποδομή στην οποία φυλάσσονται οι Ασφαλείς Κρυπτογραφικές Μονάδες (ΑΚΜ) και μέσω της οποίας διενεργείται το σύνολο των υπηρεσιών διαχείρισης του κύκλου ζωής πιστοποιητικών (έκδοσης, ανάκλησης, αναστολής και ανανέωσης)
<b>Λειτουργική Περίοδος</b>	Το χρονικό διάστημα το οποίο ξεκινά την ημερομηνία και το χρόνο έκδοσης ενός Πιστοποιητικού και λήγει την ημερομηνία και το χρόνο λήξης ή

		πρώρης ανάκλησης του Πιστοποιητικού.
<b>Μεταφόρτωση εγγράφου</b>	<b>ηλεκτρονικού</b>	Η μεταφορά του συνόλου του περιεχομένου ενός ηλεκτρονικού εγγράφου από το διαδικτυακό τόπο στον οποίο αυτό έχει αναρτηθεί σε αποθηκευτικό χώρο της επιλογής του παραλήπτη.
<b>Εγκεκριμένος Πάροχος Υπηρεσιών Εμπιστοσύνης</b>		Ο πάροχος υπηρεσιών εμπιστοσύνης ο οποίος παρέχει μία ή περισσότερες εγκεκριμένες υπηρεσίες εμπιστοσύνης και έχει αναγνωριστεί ως τέτοιος από τον εποπτικό φορέα.
<b>Πάροχος Χρονοσήμανσης</b>	<b>Υπηρεσιών</b>	Ο φορέας που εκδίδει χρονοσημάνσεις κατ' εφαρμογή του θεσμικού πλαισίου διαπίστευσης της ΕΕΤΤ και περιλαμβάνεται στον κατάλογο εμπιστευσης της ΕΕΤΤ (Κατάλογος Εμπιστευσης εποπτευόμενων/ διαπιστευμένων Παροχών Υπηρεσιών Πιστοποίησης - TSL).
<b>Πιστοποιητικό</b>		Ηλεκτρονική βεβαίωση η οποία συνδέει δεδομένα επαλήθευσης υπογραφής με ένα άτομο και επιβεβαιώνει την ταυτότητά του.
<b>Πιστοποιητικό Υπευθύνου</b>		Το Πιστοποιητικό που εκδίδεται προς έναν Υπεύθυνο ΑΕ και το οποίο μπορεί να χρησιμοποιηθεί αποκλειστικά για την τέλεση αρμοδιοτήτων ΑΕ.
<b>Πολιτική Πιστοποιητικού (ΠΠ)</b>		Κατονομαζόμενο σύνολο κανόνων που υποδεικνύει την εφαρμοσιμότητα ενός πιστοποιητικού σε μια συγκεκριμένη κοινότητα και/ή κατηγορία εφαρμογής με κοινές απαιτήσεις για την ασφάλεια.
<b>Προϊόν</b>		Το υλικό ή λογισμικό ή τα συναφή συστατικά στοιχεία υλικού ή λογισμικού τα οποία προορίζονται να χρησιμοποιηθούν για την παροχή υπηρεσιών εμπιστοσύνης.
<b>Πρωτεύουσα Αρχή Πιστοποίησης (ΠΑΠ)</b>		Μια ΑΠ η οποία ενεργεί ως Πρωτεύουσα ΑΠ (Root) και εκδίδει πιστοποιητικά προς υποκείμενες ΑΠ. Στην παρούσα υποδομή η ΑΠΕΔ λειτουργεί ως Πρωτεύουσα Αρχή Πιστοποίησης.
<b>Συνδρομητής</b>		Το πρόσωπο που αποτελεί το Υποκείμενο (Subject), στο όνομα του οποίου έχει εκδοθεί ένα Πιστοποιητικό. Ο Συνδρομητής, ή ο αιτών το πιστοποιητικό, είναι εξουσιοδοτημένος να χρησιμοποιεί το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που αναγράφεται στο Πιστοποιητικό και φέρει την ευθύνη για την ορθή χρήση του πιστοποιητικού σύμφωνα με τους ΟΧΠ.
<b>Συντονισμένη παγκόσμια ώρα (UTC)</b>		Χρονική κλίμακα βασισμένη στο δευτερόλεπτο όπως ορίζεται στη Σύσταση ITU-R TF.460-5
<b>Συντονισμένος Παγκόσμιος Χρόνος (Coordinated Universal Time -UTC)</b>		Χρονική κλίμακα με βάση το δευτερόλεπτο όπως ορίζεται στη σύσταση ITU-R TF.460-5.
<b>Υπεύθυνος ΑΕ</b>		Ένα Έμπιστο Πρόσωπο το οποίο έχει πρόσβαση στο Κέντρο Ελέγχου της ΑΕ και διενεργεί διαδικασίες του κύκλου ζωής ενός Πιστοποιητικού (π.χ. αποδοχής, ανάκλησης, αναστολής, ανάκτησης ενός Πιστοποιητικού) καθώς και άλλες αρμοδιότητες μιας ΑΕ.
<b>Υπηρεσία Εμπιστοσύνης</b>		Ηλεκτρονική υπηρεσία η οποία συνίσταται: <ul style="list-style-type: none"> <li>• στη δημιουργία, εξακρίβωση και επικύρωση ηλεκτρονικών υπογραφών, ηλεκτρονικών σφραγίδων ή ηλεκτρονικών χρονοσφραγίδων, ηλεκτρονικών υπηρεσιών συστημένης παράδοσης και πιστοποιητικών που σχετίζονται με τις υπηρεσίες αυτές, ή</li> <li>• στη δημιουργία, εξακρίβωση και επικύρωση πιστοποιητικών για επαλήθευση της ταυτότητας ιστοτόπων, ή</li> <li>• στη διαφύλαξη ηλεκτρονικών υπογραφών, σφραγίδων ή πιστοποιητικών που σχετίζονται με τις υπηρεσίες αυτές.</li> </ul>
<b>Υπηρεσία χρονοσήμανσης</b>		Η δημιουργία των απαραίτητων τεκμηρίων για ένα σύνολο δεδομένων σε

	ψηφιακή μορφή, έτσι ώστε να μπορεί να αποδειχθεί ότι τα δεδομένα αυτά υπήρχαν σε μία συγκεκριμένη χρονική στιγμή.
<b>Υποδομή Δημόσιου Κλειδιού (ΥΔΚ)/ Public Key Infrastructure (PKI)</b>	Η αρχιτεκτονική, η οργανωτική δομή, οι τεχνικές, οι κανονισμοί, και οι διαδικασίες που στο σύνολό τους υποστηρίζουν την εφαρμογή και λειτουργία κρυπτογραφικού συστήματος δημοσίου κλειδιού που βασίζεται σε Πιστοποιητικό
<b>Υποκείμενο</b>	Ο κάτοχος ενός ιδιωτικού κλειδιού που αντιστοιχεί σε ένα δημόσιο κλειδί. Το ταυτοποιημένο όνομα ενός Υποκειμένου Πιστοποιητικού είναι συνδεδεμένο με το δημόσιο κλειδί που περιλαμβάνεται στο Πιστοποιητικό.
<b>Χρονοσήμανση</b>	Αλληλουχία χαρακτήρων ή στοιχεία που δηλώνουν με ασφάλεια την ημερομηνία και ώρα που έχει λάβει χώρα μία πράξη ή ενέργεια και εκδίδεται από πάροχο υπηρεσιών χρονοσήμανσης.
<b>Χώρος Αποθήκευσης της Αρχής Πιστοποίησης Δημοσίου Ελληνικού</b>	Η δικτυακά προσπελάσιμη βάση δεδομένων της Αρχής Πιστοποίησης Ελληνικού Δημοσίου στην οποία περιέχονται τα στοιχεία των Πιστοποιητικών καθώς και άλλες πληροφορίες σχετικές με την Υποδομή Δημοσίου Κλειδιού της Αρχής Πιστοποίησης του Ελληνικού Δημοσίου (ΑΠΕΔ).

## Ακρωνύμια

Πίνακας 2: Πίνακας Ακρωνυμίων

Ακρωνύμιο		Όρος (στα Ελληνικά και στα Αγγλικά)
(Ελληνικά)	(Αγγλικά)	
	CC	Common Criteria
	EAL	Evaluation Assurance Level. (Επίπεδο αξιολόγησης εγγυήσεων, σύμφωνα με τα CommonCriteria).
	OCSF	Online Certificate Status Protocol (Πρωτόκολλο Δικτυακής Κατάστασης Πιστοποιητικών)
	PIN	Personal identification Number (Προσωπικός αριθμός ταυτότητας)
	PKCS	Public-Key Cryptography Standard (Πρότυπο Κρυπτογραφίας Δημοσίου Κλειδιού)
	PUK	Personal Unblocking Key (Προσωπικό Κλειδί που χρησιμοποιείται για απεμπλοκή της έξυπνης κάρτας μετά από συνεχή εσφαλμένη εισαγωγή PIN)
	RFC	Request For Comment (Αίτημα για σχολιασμό)
	S/MIME	Secure Multipurpose Internet Mail Extensions
	SSL	Secure Sockets Layer (Επίπεδο Ασφαλών Συνδέσεων)
ΑΕ	RA	Αρχή Εγγραφής (Registration Authority)
ΑΠ	CA	Αρχή Πιστοποίησης (Certification Authority)
ΑΠΕΔ		Αρχή Πιστοποίησης του Ελληνικού Δημοσίου
ΑΤΛΑ	LSVA	Αξιολόγηση Τρωτότητας της Λογικής Ασφάλειας (Logical Security Vulnerability Assessment)
ΑΥΠ	CSR	Αίτημα Υπογραφής Πιστοποιητικού (Certificate Signing Request)
ΑΧ	TSA	Αρχή Χρονοσφραγίδας (Time Stamping Authority)
ΔΠ	CPS	Δήλωση Πρακτικής (Certification Practice Statement)
ΔΧ		Διακριτικό Χρονοσφραγίδας
ΕΕΤΤ		Εθνική Επιτροπή Τηλεπικοινωνιών και Ταχυδρομείων
ΕΠΥΕ		Εγκεκριμένος Πάροχος Υπηρεσιών Εμπιστοσύνης

ΕΠΥΧ		Εγκεκριμένος Πάροχος Υπηρεσιών Χρονοσήμανσης
ΚΑΠ	CRL	Κατάλογος Ανακληθέντων Πιστοποιητικών (Certificate Revocation List)
ΚΜΥ		Κρυπτογραφική Μονάδα Υπογραφής
ΚΠ		Κανονισμός Πιστοποίησης
ΜΧ		Μονάδα Χρονοσήμανσης
ΠΑ	OID	Προσδιοριστής Αντικειμένου (Object Identifier)
ΠΑΠ	RCA	Πρωτεύουσα Αρχή Πιστοποίησης (Root Certification Authority)
ΠΔΠΧ		Πολιτική/Δήλωση Πρακτικής Χρονοσήμανσης
ΠΠ	CP	Πολιτική Πιστοποιητικού
ΠΥΧ		Πάροχος Υπηρεσιών Χρονοσφραγίδας
ΥΔΚ	PKI	Υποδομή Δημόσιου Κλειδιού (Public Key Infrastructure)
ΥπΑΠ		Υποκείμενη Αρχή Πιστοποίησης

## 1. Γενικοί Όροι

Οι παρόντες Γενικοί Όροι και Προϋποθέσεις περιγράφουν τις κύριες πολιτικές και πρακτικές που ακολουθεί η ΑΠΕΔ και προβλέπονται στα παρακάτω έγγραφα:

- στην Πολιτική Πιστοποιητικού και Δήλωση Πρακτικής για Εγκεκριμένες Ηλεκτρονικές Υπογραφές της ΑΠΕΔ, όπως ορίζονται στον Κανονισμό Πιστοποίησης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου και
- στην Πολιτική Πιστοποιητικού και Δήλωση Πρακτικής της Αρχής Χρονοσφραγίδας της ΑΠΕΔ, όπως ορίζονται στον Κανονισμό Πιστοποίησης της Αρχής Πιστοποίησης Ελληνικού Δημοσίου

και περιγράφονται με τρόπο συμπληρωματικό και περιληπτικό

- στη Δήλωση Γνωστοποίησης της Υποδομής Δημοσίου Κλειδιού (PKI Disclosure Statement - PDS) της ΑΠΕΔ για Εγκεκριμένες Ηλεκτρονικές Υπογραφές και
- στη Δήλωση Γνωστοποίησης της Αρχής Χρονοσφραγίδας της ΑΠΕΔ

1.1 Οι Όροι και οι Προϋποθέσεις διέπουν τη χρήση των Εγκεκριμένων Ηλεκτρονικών Υπογραφών και Υπηρεσιών Χρονοσφραγίσης από τους Συνδρομητές και αποτελούν νομικά δεσμευτική σύμβαση μεταξύ του Συνδρομητή και της ΑΠΕΔ.

1.2 Ο Συνδρομητής πρέπει να γνωρίζει και να αποδέχεται τους παρόντες Όρους και τις Προϋποθέσεις.

1.3 Η ΑΠΕΔ έχει το δικαίωμα να τροποποιήσει τους Όρους και τις Προϋποθέσεις οποιαδήποτε στιγμή εφόσον υπάρχει αιτιολογημένη ανάγκη για τέτοιες τροποποιήσεις. Η εν ισχύ έκδοση καθώς και όλες οι προηγούμενες δημοσιεύονται στον δικτυακό τόπο <https://pki.aped.gov.gr/repository>.

1.4 Ο Συνδρομητής μπορεί να υποβάλει αίτηση για Εγκεκριμένη Ηλεκτρονική Υπογραφή (σε ΕΔΔΥ) για φυσικό πρόσωπο. Η ταυτοποίηση πραγματοποιείται μέσω της φυσικής παρουσίας του προσώπου (Συνδρομητή) που υποβάλλει σε εξουσιοδοτημένο υπάλληλο της ΑΕ ή του Εντεταλμένου Γραφείου της

ΑΠΕΔ τα έγγραφα ταυτοποίησης που εξειδικεύονται στην Αίτηση για έκδοση Εγκεκριμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής.

1.5 Η ακυρότητα ή μη εφαρμοσιμότητα οποιασδήποτε διάταξης ή διατάξεων της παρούσας (εν όλω ή εν μέρει) δεν θα καθιστά ανεφάρμοστο το σύνολο των λοιπών διατάξεων και η παρούσα θα θεωρείται τροποποιημένη ως προς τη διαγραφή ή μεταβολή που απαιτείται της άκυρης ή μη εφαρμοσίμης διάταξης, ώστε να καταστεί έγκυρη, εφαρμόσιμη, και στο μέτρο που είναι δυνατό, σύμφωνη με τον αρχικό σκοπό των συμβαλλομένων.

## 2. Αποδοχή πιστοποιητικού για εγκεκριμένη ηλεκτρονική υπογραφή

2.1 Με την υποβολή αίτησης για την έκδοση Εγκεκριμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής, ο/η Συνδρομητής(-τρια) βεβαιώνει ότι γνωρίζει και αποδέχεται τους Όρους και τις Προϋποθέσεις.

Οι ακόλουθες ενέργειες αποτελούν αποδοχή του Πιστοποιητικού για Εγκεκριμένη Ηλεκτρονική Υπογραφή:

- Η έκδοση του Πιστοποιητικού συνιστά την αποδοχή του Πιστοποιητικού από τον Συνδρομητή
- Η μη υποβολή αντίρρησης όσον αφορά το Πιστοποιητικό ή το περιεχόμενό του εντός 24 ωρών από την πραγματοποίηση της λήψης του, συνιστά αποδοχή του Πιστοποιητικού.

2.2 Εάν πραγματοποιηθεί επανέκδοση κλειδιού του Πιστοποιητικού ο/η Συνδρομητής(-τρια) βεβαιώνει ότι έχει διαβάσει και συμφωνεί με τους Όρους και Προϋποθέσεις.

2.3 Τύπος Πιστοποιητικού, Χρήση και Εφαρμοστέα Πολιτική

Τύπος πιστοποιητικού	Χρήση	Εφαρμοστέα και Δημοσιευμένη Πολιτική Πιστοποίησης
Εγκεκριμένη Ηλεκτρονική Υπογραφή που συμμορφώνεται με τον κανονισμό eIDAS.	Δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε άλλα ηλεκτρονικά δεδομένα ή συσχετίζονται λογικά με άλλα δεδομένα σε ηλεκτρονική μορφή και τα οποία χρησιμοποιούνται από τον υπογράφο για να υπογράψει.	Δήλωση Πρακτικής Πιστοποίησης της ΑΠΕΔ για Εγκεκριμένα Πιστοποιητικά Ηλεκτρονικών Υπογραφών, δημοσιευμένη στη διεύθυνση <a href="https://pki.aped.gov.gr/repository">https://pki.aped.gov.gr/repository</a>  Πολιτική ETSI EN 319 411-2 QCP-n-qscd

Τα Εγκεκριμένα Πιστοποιητικά Ηλεκτρονικής Υπογραφής είναι Μακράς διάρκειας και ισχύουν για 3 έτη, ενώ η ΑΠΕΔ διατηρεί τη δυνατότητα να μειώσει τον χρόνο ισχύος των Εγκεκριμένων Πιστοποιητικών Ηλεκτρονικής Υπογραφής.



### 3. Διάρκεια /Λήξη/Ανανέωση - Ανάκληση/Αναστολή/Ενεργοποίηση - Καταγγελία Σύμβασης

**3.1.** Η σύμβαση έχει διάρκεια ίση με τη διάρκεια ισχύος των εκδιδόμενων προς το Συνδρομητή Εγκεκριμένων Πιστοποιητικών Ηλεκτρονικής Υπογραφής τύπου “Document Signing – Qualified Certificates for Qualified Electronic Seals with QSCD” η οποία είναι τριών (3) ετών από την έκδοσή τους και λήγει την ημερομηνία «λήξης ισχύος» των παραπάνω πιστοποιητικών, η οποία αναγράφεται σε αυτά. Οι εκατέρωθεν υποχρεώσεις που προβλέπονται από τους όρους της παρούσας σύμβασης, της σχετικής Πολιτικής της ΑΠΕΔ για μετά τη λήξη ή ανάκληση των πιστοποιητικών, εξακολουθούν να βαρύνουν τους υπόχρεους.

**3.2.** Η ανανέωση του Εγκεκριμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής δεν εφαρμόζεται, αλλά συνίσταται σε επαναδημιουργία κλειδιών πιστοποιητικού. Η επαναδημιουργία κλειδιών πιστοποιητικού είναι η αίτηση για την έκδοση ενός νέου Εγκεκριμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής που πιστοποιεί το νέο δημόσιο κλειδί. Πριν από τη λήξη του υφιστάμενου πιστοποιητικού του Συνδρομητή, ο Συνδρομητής πρέπει να επαναδημιουργήσει κλειδιά για το πιστοποιητικό ώστε να εξασφαλίσει τη συνέχιση της χρήσης του πιστοποιητικού. Μπορεί να επαναδημιουργηθούν κλειδιά για το πιστοποιητικό και μετά τη λήξη του.

**3.3.** Σε περίπτωση παραβίασης των όρων της παρούσας σύμβασης ή της σχετικής Πολιτικής της ΑΠΕΔ από το Συνδρομητή, ή και σε οποιαδήποτε άλλη περίπτωση προβλέπεται στη σχετική Πολιτική, η ΑΠΕΔ δύναται να προβεί σε ανάκληση ή αναστολή των Εγκεκριμένων Πιστοποιητικών Ηλεκτρονικής Υπογραφής του Συνδρομητή (η οποία πραγματοποιείται με την προσθήκη των σειριακών αριθμών αναγνώρισης πιστοποιητικών στην δημοσιευόμενη λίστα ανακληθέντων πιστοποιητικών Certificate Revocation List, CRL, και επίσης με την αντίστοιχη απάντηση του εξυπηρετητή OCSP) ενημερώνοντας σχετικά το Συνδρομητή. Επίσης, ανάκληση ή αναστολή των συγκεκριμένων πιστοποιητικών πραγματοποιείται από την ΑΠΕΔ και στην περίπτωση που η τελευταία ενημερωθεί, με οποιονδήποτε πρόσφορο τρόπο, ότι ο Συνδρομητής δεν έχει πια πραγματικό, νόμιμο και αποκλειστικό έλεγχο των ιδιωτικών κλειδιών του.

**3.4.** Την ανάκληση ή την αναστολή των Εγκεκριμένων Πιστοποιητικών Ηλεκτρονικής Υπογραφής μπορεί αλλά και επιβάλλεται να ζητήσει και ο ίδιος ο Συνδρομητής (για την προστασία του) σε περίπτωση έκθεσης των κλειδιών του, ή του PIN σε τρίτους, ή μετά από απώλεια του USB token, οπότε η ΑΠΕΔ οφείλει, αφού επαληθεύσει την προέλευση του αιτήματος, να προβεί σε άμεση επεξεργασία του.

### 4. Απαγορεύσεις Χρήσης

4.1 Τα Εγκεκριμένα Πιστοποιητικά Ηλεκτρονικής Υπογραφής δεν έχουν σχεδιαστεί, δεν αποσκοπούν και δεν είναι εγκεκριμένα να χρησιμοποιηθούν σε περιπτώσεις όπου απαιτείται τήρηση στοιχείων υψηλής διαβάθμισης ή συνθηκών υψηλής ασφάλειας (όπως για παράδειγμα, εθνική άμυνα και ασφάλεια).

4.2 Τα Εγκεκριμένα Πιστοποιητικά Ηλεκτρονικής Υπογραφής του Συνδρομητή απαγορεύεται να χρησιμοποιηθούν εκτός των ορίων και του περιεχομένου που εξειδικεύεται στη ΔΠΠ για Εγκεκριμένες Ηλεκτρονικές Υπογραφές της ΑΠΕΔ ή για παράνομους σκοπούς, ή σε αντίθεση με το δημόσιο

συμφέρον, ή άλλως για σκοπό που ενδέχεται να βλάψει το Ελληνικό Δημόσιο και την ΑΠΕΔ. Ενδεικτικά, η χρήση των Εγκεκριμένων Πιστοποιητικών Ηλεκτρονικής Υπογραφής απαγορεύεται για οποιονδήποτε από τους ακόλουθους σκοπούς:

4.2.1 παράνομη δραστηριότητα (συμπεριλαμβανομένων επιθέσεων στον κυβερνοχώρο και προσπάθειας παραβίασης του Πιστοποιητικού)

4.2.2 έκδοση νέου Πιστοποιητικού και πληροφοριών σχετικά με την ισχύ του Πιστοποιητικού

4.2.3 διευκόλυνση άλλων μερών να χρησιμοποιούν το Ιδιωτικό Κλειδί του Συνδρομητή

4.2.4 διευκόλυνση αυτοματοποιημένης χρήσης του Πιστοποιητικού που έχει εκδοθεί για ηλεκτρονική υπογραφή

4.2.5 χρήση του Πιστοποιητικού που έχει εκδοθεί για ηλεκτρονική υπογραφή για την υπογραφή εγγράφων που μπορεί να προκαλέσει ανεπιθύμητες συνέπειες (συμπεριλαμβανομένης της υπογραφής τέτοιων εγγράφων για δοκιμαστικούς σκοπούς).

## 5. Όρια Εμπιστοσύνης

5.1 Όρια Εμπιστοσύνης για Εγκεκριμένα Πιστοποιητικά Ηλεκτρονικών Υπογραφών

5.1.1 Οι πληροφορίες στα Εγκεκριμένα Πιστοποιητικά Ηλεκτρονικών Υπογραφών είναι ακριβείς. Δεν υπάρχουν λάθη ή ψευδείς δηλώσεις ως προς τα στοιχεία του Πιστοποιητικού γνωστές ή προερχόμενες από τις οντότητες που εγκρίνουν την Αίτηση για Πιστοποιητικό ή που εκδίδουν το Πιστοποιητικό.

5.1.2 Τα Εγκεκριμένα Πιστοποιητικά Ηλεκτρονικών Υπογραφών ισχύουν από την ημερομηνία που προσδιορίζεται στο Πιστοποιητικό. Η ισχύς του Πιστοποιητικού λήγει την ημερομηνία λήξης που αναφέρεται στο Πιστοποιητικό ή εάν το Πιστοποιητικό ανακληθεί.

5.1.3 Τα ημερολόγια ελέγχου διατηρούνται εντός του συστήματος για τουλάχιστον δύο (2) μήνες. Τα φυσικά ή ψηφιακά αρχεία σχετικά με τις αιτήσεις για Πιστοποιητικά, τις πληροφορίες εγγραφής και τα αιτήματα ή τις αιτήσεις για αναστολή, τερματισμό αναστολής και ανάκληση φυλάσσονται για τουλάχιστον επτά (7) έτη μετά τη λήξη ισχύος του σχετικού Πιστοποιητικού.

5.2 Όρια Εμπιστοσύνης για Χρονοσφραγίδες

5.2.1 Οι Χρονοσφραγίδες ισχύουν από την ημερομηνία που προσδιορίζεται σε αυτές. Η ισχύς της Χρονοσφραγίδας λήγει την ημερομηνία λήξης που προσδιορίζεται στη Χρονοσφραγίδα ή εάν το Πιστοποιητικό της Μονάδας Χρονοσφραγίδας (ΜΧ) ανακληθεί. Η Αρχή Χρονοσφραγίδας (ΑΧ) της ΑΠΕΔ διασφαλίζει ότι τα ιδιωτικά κλειδιά υπογραφής της ΜΧ δεν χρησιμοποιούνται πέρα από το τέλος του κύκλου ζωής τους. Ειδικότερα, εφαρμόζονται λειτουργικές και τεχνικές διαδικασίες για να εξασφαλιστεί ότι ένα νέο κλειδί θα τεθεί σε εφαρμογή 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 Διακριτικού Χρονοσφραγίδας (ΔΧ) θα απορρίπτει κάθε απόπειρα έκδοσης ενός ΔΧ, εάν έχει λήξει το ιδιωτικό κλειδί υπογραφής ή εάν έχει λήξει η περίοδος χρήσης του ιδιωτικού κλειδιού υπογραφής.

5.2.2 Η ΑΠΕΔ έχει θέσει τεχνικές διαδικασίες για να εξασφαλίσει ότι τα Διακριτικά Χρονοσφραγίδας εκδίδονται με ασφάλεια και περιέχουν τη σωστή ώρα. Η ΑΧ της ΑΠΕΔ εξασφαλίζει ότι η ώρα της συγχρονίζεται με το UTC εντός της δηλωμένης ακρίβειας με πολλαπλές ανεξάρτητες πηγές ώρας. Τα Διακριτικά Χρονοσφραγίδας εκδίδονται με ακρίβεια  $\pm$  ενός δευτερολέπτου. Η ΑΠΕΔ εφαρμόζει ελέγχους ασφαλείας που εμποδίζουν τη μη εξουσιοδοτημένη λειτουργία, με σκοπό τη βαθμονόμηση της ώρας εκτός λειτουργίας. Η ΑΠΕΔ παρακολουθεί ότι ο συγχρονισμός διατηρείται όταν εμφανιστεί ένα άλμα δευτερολέπτου.

5.2.3 Τα Πιστοποιητικά Χρονοσφραγίδας ισχύουν για δέκα (10) χρόνια, αλλά απαιτούν ανανέωση κάθε χρόνο του πιστοποιητικού της Μονάδας Χρονοσφραγίδας. Ως εκ τούτου, τα αρχεία καταγραφής για τις Χρονοσφραγίδες διατηρούνται για ένα (1) έτος μετά τη λήξη του Πιστοποιητικού της Μονάδας Χρονοσφραγίδας.

## 6. Δικαιώματα και Υποχρεώσεις του Συνδρομητή

6.1 Ο Συνδρομητής έχει το δικαίωμα να υποβάλει αίτηση για έκδοση Εγκεκριμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής ή να ζητήσει μια Χρονοσφραγίδα, με αποδοχή των παρόντων Όρων και Προϋποθέσεων και συμμόρφωση με τις απαιτήσεις της Δήλωσης Πρακτικής Πιστοποίησης για Εγκεκριμένα Πιστοποιητικά για Ηλεκτρονικές Υπογραφές, καθώς και της Πολιτικής Πιστοποιητικού και Δήλωσης Πρακτικής Πιστοποίησης της Αρχής Χρονοσφραγίδας της ΑΠΕΔ αντίστοιχα.

Ο Συνδρομητής οφείλει να προχωρήσει σε έκδοση του Εγκεκριμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής σε διάστημα σαράντα πέντε (45) ημερών από τη φυσική του ταυτοποίηση στο Εντεταλμένο Γραφείο. Μετά την πάροδο αυτού του διαστήματος η αίτησή του ακυρώνεται και πρέπει να υποβάλλει νέα αίτηση.

6.2 Ο Συνδρομητής ή / και Υποκείμενο των Εγκεκριμένων Ηλεκτρονικών Υπογραφών:

6.2.1 είναι αποκλειστικά υπεύθυνος για την τήρηση του Ιδιωτικού Κλειδιού του

6.2.2 είναι αποκλειστικά πλήρως υπεύθυνος για οποιαδήποτε συνέπειες της χρήσης του Πιστοποιητικού του και κατά τη διάρκεια και μετά τη λήξη ισχύος του Πιστοποιητικού

6.2.3 είναι αποκλειστικά υπεύθυνος για οποιαδήποτε ζημία προκληθεί λόγω αδυναμίας ή αθέμιτης εκπλήρωσης των υποχρεώσεών του που καθορίζονται στους Όρους και Προϋποθέσεις ή / και στην Ελληνική νομοθεσία και τη νομοθεσία της Ευρωπαϊκής Ένωσης

6.2.4 πρέπει να γνωρίζει ότι οι Ηλεκτρονικές Υπογραφές που εκδίδονται με βάση πιστοποιητικά που έχουν λήξει ή ανακληθεί είναι άκυρες.

6.3 Ο Συνδρομητής των Εγκεκριμένων Ηλεκτρονικών Υπογραφών πρέπει:

6.3.1 να υποβάλει ακριβείς, αληθείς και πλήρεις πληροφορίες σχετικά με την έκδοση του Εγκεκριμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής

6.3.2 να υποβάλει τα απαραίτητα έγγραφα και δικαιολογητικά για την ταυτοποίησή του στην ΑΠΕΔ όπως εξειδικεύεται στο έντυπο αίτησης για έκδοση Εγκεκριμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής, καθώς και να ακολουθεί τα βήματα που του η υποδεικνύει η ΑΠΕΔ για την ολοκλήρωση της διαδικασίας εγγραφής

6.3.3 να μην προχωρήσει τη διαδικασία έκδοσης του Εγκεκριμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής, εάν ο Συνδρομητής δεν έχει εκ του νόμου το δικαίωμα να το πράξει, ή/και δεν είναι ενήλικος

6.3.4 να διασφαλίσει ότι το Ιδιωτικό Κλειδί του Συνδρομητή χρησιμοποιείται υπό τον έλεγχο του/της και να επιδεικνύει τη δέουσα επιμέλεια ώστε να αποφεύγεται η μη εξουσιοδοτημένη χρήση του

6.3.5 να είναι υπεύθυνος για την μυστικότητα των ιδιωτικών κλειδιών του Υποκειμένου όταν αυτά βρίσκονται σε τοπική ΕΔΔΥ καθώς και των διαπιστευτηρίων πρόσβασης σε ιδιωτικά κλειδιά (username, password, OTP) όταν βρίσκονται σε εξ αποστάσεως ΕΔΔΥ

6.3.6 να είναι υπεύθυνος για την ορθή χρήση της κινητής συσκευής που χρησιμοποίησε κατά την εγκατάσταση της εφαρμογής για την παραγωγή του OTP προκειμένου να παράγει και να χρησιμοποιήσει το Πιστοποιητικό του όταν βρίσκεται σε εξ αποστάσεως ΕΔΔΥ. Εάν η συσκευή του Συνδρομητή χαθεί ή καταστραφεί ή ο Συνδρομητής δεν δύναται να χρησιμοποιήσει το Εγκεκριμένο Πιστοποιητικό Ηλεκτρονικής Υπογραφής του για οποιονδήποτε λόγο εκτός του ελέγχου της ΑΠΕΔ, ο Συνδρομητής θα πρέπει να επικοινωνήσει άμεσα με την ΑΠΕΔ ώστε να αιτηθεί την ανάκληση του Εγκεκριμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής του.

6.3.7 να χρησιμοποιεί το Ιδιωτικό Κλειδί του/της και το Πιστοποιητικό σύμφωνα με τους Όρους και Προϋποθέσεις, συμπεριλαμβανομένων των ισχυουσών συμφωνιών που ορίζονται στην Ενότητα 9, και τη νομοθεσία της Ελλάδας και της Ευρωπαϊκής Ένωσης

6.3.8 να ενημερώνει την ΑΠΕΔ για τα σωστά στοιχεία εντός εύλογου χρονικού διαστήματος, σε περίπτωση αλλαγής των προσωπικών του/της στοιχείων ή για τυχόν ανακρίβειες του περιεχομένου του Εγκεκριμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής

6.3.9 να ενημερώνει άμεσα την ΑΠΕΔ για την ύπαρξη πιθανότητας μη εξουσιοδοτημένης χρήσης του Ιδιωτικού Κλειδιού του/της ή εάν το Ιδιωτικό του/της Κλειδί έχει χαθεί, κλαπεί, ενδεχομένως εκτεθεί σε κίνδυνο ή εάν έχει χαθεί ο έλεγχος του Ιδιωτικού του/της Κλειδιού λόγω έκθεσης σε κίνδυνο των διαπιστευτηρίων αυθεντικοποίησης (πχ. κωδικός PIN, PUK, Κωδικός Χρήστη, Κωδικός Πρόσβασης, Κωδικός Μιας Χρήσης) ή για άλλους λόγους και να ανακαλεί αμέσως το Εγκεκριμένο Πιστοποιητικό Ηλεκτρονικής Υπογραφής

6.3.10 να μην εξακολουθεί να χρησιμοποιεί το ιδιωτικό κλειδί εάν το Εγκεκριμένο Πιστοποιητικό Ηλεκτρονικής Υπογραφής έχει ανακληθεί ή έχει εκτεθεί σε κίνδυνο η ΑΠ.

6.4 Ο Συνδρομητής δηλώνει ότι ενημερώθηκε πλήρως και γνωρίζει κάθε τι σχετικά με τα δικαιώματα και τις υποχρεώσεις του, καθώς και με όλες τις πιθανές συνθήκες και κινδύνους της ηλεκτρονικής επικοινωνίας που υποστηρίζεται από τις παρεχόμενες υπηρεσίες εμπιστοσύνης της ΑΠΕΔ. Ως εκ τούτου, αναγνωρίζει ότι η εκ μέρους του επίκληση της απώλειας ~~του φορέα τούτης σύνδεσης~~, διαρροής του PIN ή εν γένει ανακρίβειας του πιστοποιητικού είναι ανίσχυρη, απαράδεκτη, καταχρηστική και αντίθετη στην καλή πίστη.

6.5 Ο Συνδρομητής αποδέχεται ότι, κατά τη διαδικασία έκδοσης / ανάκλησης του πιστοποιητικού, θα λαμβάνει στο πιστοποιημένο κινητό τηλέφωνό του, που έχει δηλωθεί στην αίτηση-ΥΔ του gov.gr, ενημερωτικά SMS.

6.65 Ο Συνδρομητής ευθύνεται αποκλειστικά και υποχρεούται να αποκαταστήσει τη ζημιά κάθε τρίτου που βασίστηκε στην υπογραφή του.

6.76 Ο Συνδρομητής οφείλει να μην εκχωρεί τα δικαιώματά του ούτε να μεταβιβάζει τις υποχρεώσεις σε τρίτους βάσει της παρούσας Συμβάσης. Κάθε απόπειρα εκχώρησης ή εξουσιοδότησης θεωρείται άκυρη

6.87 Ο Συνδρομητής των Υπηρεσιών Χρονοσφραγίδας πρέπει:

- να επαληθεύει τις υπογραφές που δημιούργησε η ΑΧ της ΑΠΕΔ στο ΤΧ (Επαλήθευση εάν η υπογραφή της ΑΧ στο ΔΧ είναι έγκυρη και επαλήθευση του πιστοποιητικού της ΑΧ)
- να χρησιμοποιεί ασφαλείς κρυπτογραφικές λειτουργίες για αιτήσεις χρονοσφραγίδων
- να γνωρίζει ότι οι χρονοσφραγίδες που έχουν λήξει δεν είναι έγκυρες.

## 7. Υποχρεώσεις ΑΠΕΔ

Με την επιφύλαξη της ενότητας 8, η ΑΠΕΔ υποχρεούται να παρέχει τις υπηρεσίες σύμφωνα με την Πολιτική Πιστοποιητικού & Δήλωση Πρακτικής Πιστοποίησης της ΑΠΕΔ.

7.1 Η ΑΠΕΔ, οφείλει, έναντι του Συνδρομητή:

α) να δημιουργήσει ζεύγος κρυπτογραφικών κλειδιών τηρώντας κάθε προβλεπόμενη από την Πολιτική διαδικασία,

β) να εκδώσει και να διαχειριστεί προσωπικά πιστοποιητικά τύπου «Document Signing – Qualified Certificates for Qualified Electronic Seals with QSCD» για τα παραπάνω ζεύγη κλειδιών του Συνδρομητή (ήτοι ένα εγκεκριμένο προσωπικό πιστοποιητικό) συμμορφούμενη με την Πολιτική,

γ) να ανακαλεί το Εγκεκριμένο Πιστοποιητικό Ηλεκτρονικής Υπογραφής του Συνδρομητή όταν αυτός το ζητήσει και να δημοσιεύει σε τακτά χρονικά διαστήματα το Certificate Revocation List, καθώς επίσης ο εξυπηρετητής OCSP να απαντά για την κατάσταση του Εγκεκριμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής, σύμφωνα με τις διαδικασίες και τους όρους της σχετικής Πολιτικής της ΑΠΕΔ,

δ) να δημοσιεύει τις Πολιτικές που εκδίδει, καθώς και οποιαδήποτε τροποποίησή τους,

στ) να διασφαλίζει ότι οι μονάδες χρονικής σφράγισης (Time-Stamping Units - TSUs) είναι συντονισμένες σύμφωνα με την παγκόσμια ώρα (UTC) και έχουν απόκλιση  $\pm 1$  δευτερόλεπτο,  
ε) να παρέχει συνεχή πρόσβαση στην υπηρεσία ηλεκτρονικής χρονοσήμανσης πλην ειδικών περιπτώσεων όπως: προγραμματισμένες τεχνικές διακοπές, απώλεια χρόνου συγχρονισμού και άλλων αιτιών που περιγράφονται στο σχετικό κεφάλαιο της Πολιτικής

7.2 Η ΑΠΕΔ, έναντι του Συνδρομητή εγγυάται:

α) την ακρίβεια όλων των πληροφοριών που περιέχονται στο Εγκεκριμένο Πιστοποιητικό Ηλεκτρονικής Υπογραφής και την ύπαρξη όλων των στοιχείων που απαιτούνται για την έκδοσή του, σύμφωνα με τη σχετική Πολιτική της ΑΠΕΔ,

β) ότι οι ανακλήσεις του Εγκεκριμένου Πιστοποιητικού Ηλεκτρονικής Υπογραφής του θα δημοσιεύονται μέσα σε 24 ώρες από την υποβολή της αίτησης, σύμφωνα πάντα με τους όρους και την διαδικασία που περιγράφεται στον Κανονισμό Πιστοποίησης της ΑΠΕΔ.

7.3 Η ΑΠΕΔ λειτουργεί την Παροχή Υπηρεσιών Εμπιστοσύνης σύμφωνα με την Πολιτική και τις σχετικές διατάξεις των Κανονισμών eIDAS και ETSI.

7.4 Οι παραπάνω εγγυήσεις παρέχονται από την ΑΠΕΔ μόνο για χρήση των πιστοποιητικών της και για χρήση υπηρεσίας χρονοσήμανσης από το Συνδρομητή, σύμφωνα με τους περιορισμούς και τους όρους που καθορίζονται στη σχετική Πολιτική της ΑΠΕΔ.

7.5 Η ΑΠΕΔ δεν ευθύνεται προς οποιονδήποτε (συνδρομητή ή τρίτο), εάν δεν το βαραίνει κάποιο πταίσμα ή εάν οι πράξεις του ήταν σύμφωνες με τα οριζόμενα στη σχετική Πολιτική της ΑΠΕΔ. Η ΑΠΕΔ δεν ευθύνεται και για τυχόν δυσλειτουργία των υπηρεσιών της σε περιπτώσεις ανωτέρας βίας, όπως ενδεικτικά σεισμοί, πλημμύρες, πυρκαγιές κ.λ.π., συμπεριλαμβανόμενων των περιπτώσεων διακοπής της παροχής ηλεκτρικού ρεύματος (black-out), προβλημάτων στα τηλεπικοινωνιακά δίκτυα και γενικότερα όλων των εξωτερικών εμποδίων που μπορεί να εμποδίσουν την ομαλή παροχή των υπηρεσιών της και δεν οφείλονται σε υπαιτιότητά της.

7.6 Η ΑΠΕΔ δεν ευθύνεται για οποιαδήποτε έμμεση ή αποθετική ζημιά, ποινική ή πειθαρχική δίωξη ή τιμωρία, διαφυγόντα κέρδη ή οποιοσδήποτε άλλες έμμεσες συνέπειες προκληθούν στον συνδρομητή με αφορμή τη χρήση ή τη στήριξή του σε κάποιο πιστοποιητικό του ή την χρήση της υπηρεσίας ηλεκτρονικής χρονοσήμανσης. Για τους σκοπούς της παρούσας παραγράφου, ο όρος "ζημιά" σημαίνει μερική απώλεια ή μείωση της αξίας καθώς και πλήρης ή ολική απώλεια. νομοθεσία.

## **8. Υποχρεώσεις Ελέγχου κατάστασης Πιστοποιητικού Βασιζόμενων Μερών**

8.1 Έκαστο Βασιζόμενο Μέρος μελετά τους κινδύνους και τις ευθύνες που σχετίζονται με την αποδοχή του Πιστοποιητικού. Οι κίνδυνοι και οι ευθύνες έχουν καθοριστεί στην ΔΠΠ και την ΠΠ. Ένα Βασιζόμενο Μέρος αποδέχεται ότι έχει πρόσβαση σε επαρκείς πληροφορίες που διασφαλίζουν τη δυνατότητά του να λάβει τεκμηριωμένη απόφαση σχετικά με την έκταση που θα επιλέξει να βασιστεί στις πληροφορίες ενός Εγκεκριμένου Πιστοποιητικού. ΕΝΑ ΒΑΣΙΖΟΜΕΝΟ ΜΕΡΟΣ ΕΙΝΑΙ ΥΠΕΥΘΥΝΟ ΝΑ ΑΠΟΦΑΣΙΣΕΙ ΕΑΝ ΘΑ ΒΑΣΙΣΤΕΙ ΣΤΙΣ ΠΛΗΡΟΦΟΡΙΕΣ ΕΝΟΣ ΕΓΚΕΚΡΙΜΕΝΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ.

8.2 Έκαστο Βασιζόμενο Μέρος αποδέχεται και συμφωνεί ότι η χρήση του Αποθηκευτικού Χώρου της ΑΠΕΔ και η εμπιστοσύνη του σε οποιοδήποτε Εγκεκριμένο Πιστοποιητικό διέπεται από την εκάστοτε ισχύουσα ΔΠΠ της ΑΠΕΔ. Η ισχύουσα ΔΠΠ δημοσιεύεται στον δικτυακό Αποθηκευτικό Χώρο στη διεύθυνση: <https://pki.aped.gov.gr/repository>. Οι τροποποιήσεις της ΔΠΠ δημοσιεύονται επίσης, στον δικτυακό Αποθηκευτικό Χώρο της ΑΠΕΔ στην ίδια διεύθυνση.

8.3 Εάν δεν περιέχονται επαρκείς πληροφορίες στο Πιστοποιητικό ή στην Ηλεκτρονική Υπογραφή όσον αφορά την ισχύ του Πιστοποιητικού, το Βασιζόμενο Μέρος επαληθεύει την εγκυρότητα ή την ανάκληση του Εγκεκριμένου Πιστοποιητικού χρησιμοποιώντας τις πληροφορίες της τρέχουσας κατάστασης του Πιστοποιητικού βάσει των υπηρεσιών επικύρωσης πιστοποιητικών που παρέχονται από την ΑΠΕΔ κατά τη στιγμή της χρήσης του Εγκεκριμένου Πιστοποιητικού ή της δημιουργίας Εγκεκριμένης Ηλεκτρονικής Υπογραφής. Μία μέθοδος με την οποία μπορείτε να ελέγξετε την κατάσταση του Πιστοποιητικού είναι να ανατρέξετε στον πιο πρόσφατο Κατάλογο Ανάκλησης Πιστοποιητικών από την Αρχή Πιστοποίησης, η οποία εξέδωσε το ψηφιακό πιστοποιητικό στο οποίο επιθυμείτε να βασιστείτε.

8.4 Το Βασιζόμενο Μέρος ακολουθεί τους περιορισμούς που αναφέρονται στο Πιστοποιητικό και βεβαιώνεται ότι η συναλλαγή που πρόκειται να γίνει αποδεκτή ανταποκρίνεται στην ΔΠΠ και την ΠΠ.

8.4.1 Τα Εγκεκριμένα Πιστοποιητικά χρησιμοποιούνται μόνο στον βαθμό που η χρήση τους είναι σύμφωνη με την εφαρμοστέα νομοθεσία. Τα Εγκεκριμένα Πιστοποιητικά της ΑΠΕΔ δεν έχουν σχεδιαστεί, δεν αποσκοπούν, ή δεν είναι εγκεκριμένα για χρήση ή μεταπώληση ως εξοπλισμός ελέγχου σε επικίνδυνες συνθήκες ή για χρήσεις που απαιτούν την ασφαλή λειτουργία έναντι σφάλματος, όπως στη λειτουργία πυρηνικών εγκαταστάσεων, την πλοήγηση ή τα συστήματα επικοινωνίας αεροσκαφών, τα συστήματα ελέγχου εναέριας κυκλοφορίας ή τα συστήματα οπλικού ελέγχου, όπου κάποιο σφάλμα θα μπορούσε να οδηγήσει απευθείας στον θάνατο, σε προσωπικό τραυματισμό ή σε σημαντική περιβαλλοντική ζημία.

8.4.2 Οι Χρονοσφραγίδες θα χρησιμοποιούνται μόνο στον βαθμό που η χρήση τους είναι σύμφωνη με την εφαρμοστέα νομοθεσία. Οποιοσδήποτε περιορισμός στη χρήση των χρονοσφραγίδων που υποδεικνύεται στην Πολιτική Πιστοποιητικού & Δήλωση Πρακτικής Πιστοποίησης της Αρχής Χρονοσφραγίδας της ΑΠΕΔ θα πρέπει να ληφθεί υπόψη. Οι Συνδρομητές και τα Βασιζόμενα Μέρη των Υπηρεσιών Χρονοσφραγίδας πρέπει να επαληθεύουν τις υπογραφές που δημιούργησε η ΑΧ της ΑΠΕΔ στο ΔΧ. Εάν η επαλήθευση πραγματοποιείται μετά τη λήξη ισχύος του Πιστοποιητικού, θα πρέπει να ακολουθήσουν τις οδηγίες του Παραρτήματος D του ETSI EN 319 421.

8.5 Η ΑΠΕΔ διασφαλίζει ότι οι Υπηρεσίες Εμπιστοσύνης είναι διαθέσιμες επί 24ώρου βάσεως, 7 ημέρες την εβδομάδα, με ελάχιστη συνολική διαθεσιμότητα 99% ανά έτος με τις προγραμματισμένες διακοπές λειτουργίας να μην υπερβαίνουν το ποσοστό του 0,4% ετησίως.

8.6 Το Βασιζόμενο Μέρος επαληθεύει την ισχύ οποιουδήποτε Πιστοποιητικού που έχει εκδοθεί από την ΑΠΕΔ ελέγχοντας τις αναφορές ΟCSP και ΚΑΠ που βρίσκονται στο Πιστοποιητικό.

8.7 Το Βασιζόμενο Μέρος αναμένεται να χρησιμοποιήσει ένα Κατάλογο Εμπιστοσύνης για να διαπιστώσει εάν μια Ηλεκτρονική Υπογραφή ή Χρονοσφραγίδα είναι εγκεκριμένη.

## 9. Περιορισμένη Εγγύηση και Δήλωση αποποίησης /περιορισμού ευθύνης

9.1 Η ΑΠΕΔ είναι υπεύθυνη για την εκτέλεση των Υπηρεσιών Εμπιστοσύνης όπως ορίζεται στη Δήλωση Πρακτικής Πιστοποίησης για Εγκεκριμένες Ηλεκτρονικές Υπογραφές της ΑΠΕΔ και στην Πολιτική Πιστοποιητικού και Δήλωση Πρακτικής Πιστοποίησης της Αρχής Χρονοσφραγίδας της ΑΠΕΔ.

9.2 Η ΑΠΕΔ ενημερώνει όλους τους Συνδρομητές και τα Υποκείμενα πριν παύσει την υπηρεσία Πιστοποιητικών και διατηρεί την τεκμηρίωση σχετικά με την διακοπή της υπηρεσίας Πιστοποιητικών καθώς και τις πληροφορίες που απαιτούνται σύμφωνα με τη διαδικασία που ορίζεται στην ΔΠΠ.

9.3 Η ΑΠΕΔ δεν ευθύνεται για

- το απόρρητο των Ιδιωτικών Κλειδιών του Συνδρομητή και του Υποκειμένου όταν βρίσκονται σε τοπική ΕΔΔΥ, για πιθανή απώλεια ή καταστροφή της τοπικής ΕΔΔΥ
- το απόρρητο των διαπιστευτηρίων αυθεντικοποίησης των Ιδιωτικών Κλειδιών (πχ. Κωδικός Χρήστη, Κωδικός Πρόσβασης, Κωδικός Μιας Χρήσης) όταν βρίσκονται σε εξ αποστάσεως ΕΔΔΥ, για πιθανή απώλεια ή καταστροφή της κινητής συσκευής που χρησιμοποιείται για την παραγωγή του Κωδικού Μιας Χρήσης
- τυχόν κακή χρήση των Πιστοποιητικών ή ανεπαρκείς ελέγχους των Πιστοποιητικών ή για τις λανθασμένες αποφάσεις ενός Βασιζόμενου Μέρους ή τυχόν συνέπειες λόγω σφάλματος ή παράλειψης του ελέγχου ισχύος Πιστοποιητικού
- για τη μη εκπλήρωση των υποχρεώσεων της εάν η εν λόγω μη εκπλήρωση οφείλεται σε σφάλματα ή προβλήματα ασφαλείας του εποπτικού φορέα, του Καταλόγου εμπιστοσύνης ή άλλης δημόσιας αρχής
- για τη μη εκτέλεση εάν αυτή οφείλεται σε ανωτέρα βία.

9.4 Η ΑΠΕΔ παρέχει περιορισμένες εγγυήσεις και αποποιείται κάθε άλλης εγγύησης, συμπεριλαμβανομένων εγγυήσεων εμπορευσιμότητας ή καταλληλότητας για συγκεκριμένο σκοπό, περιορίζει την ευθύνη και αποκλείει κάθε ευθύνη, εξαιρουμένου δόλου ή βαριάς αμέλειας, για τυχόν απώλεια κερδών, απώλεια δεδομένων, ή άλλη έμμεση, παρεπόμενη ή ποινική ζημία που προκύπτει από ή σε σχέση με τη χρήση, παράδοση, άδεια, εκπλήρωση, μη εκπλήρωση ή μη διαθεσιμότητα πιστοποιητικών, ηλεκτρονικών υπογράφων, χρονοσφραγίδων ή οποιωνδήποτε άλλων συναλλαγών ή υπηρεσιών που παρέχονται ή αναφέρονται στο παρόν, ακόμα και αν η ΑΠΕΔ έχει ενημερωθεί για την πιθανότητα τέτοιων ζημιών.

Το Ελληνικό Δημόσιο ευθύνεται για ζημία που προκλήθηκε από πράξεις ή παραλείψεις των οργάνων της ΑΠΕΔ ή των εκδότεων ΑΠ σε οποιοδήποτε φυσικό ή νομικό πρόσωπο, λόγω μη συμμόρφωσης



προς τις υποχρεώσεις που προβλέπονται στην ΠΠ και ΔΠΠ, σύμφωνα με το άρθρο 105 του Εισαγωγικού Νόμου του Αστικού Κώδικα (ΕισΝΑΚ). Οι περιορισμοί ευθύνης περιλαμβάνουν αποκλεισμό έμμεσων, ειδικών, παρεπόμενων και επακόλουθων ζημιών. Ειδικότερα, για την ευθύνη του Ελληνικού Δημοσίου λόγω πράξεων ή παραλείψεων των οργάνων της ΑΠΕΔ, ως προς την τήρηση των διατάξεων της παρούσας ισχύουν τα ακόλουθα:

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

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

9.5 Οι Συνδρομητές, τα Υποκείμενα και τα Βασιζόμενα Μέρη ενημερώνονται με το παρόν σχετικά με την πιθανότητα κλοπής ή άλλης μορφής έκθεσης σε κίνδυνο ενός ιδιωτικού κλειδιού που αντιστοιχεί σε δημόσιο κλειδί το οποίο περιλαμβάνεται σε ένα εγκεκριμένο πιστοποιητικό, η οποία μπορεί να είναι δυνατόν να ανιχνευθεί ή όχι, καθώς και για την πιθανότητα χρήσης ενός κλαπέντος ή εκτεθειμένου σε κίνδυνο κλειδιού για την πλαστογράφηση μιας εγκεκριμένης ηλεκτρονικής υπογραφής ή εγκεκριμένης ηλεκτρονικής σφραγίδας σε ένα έγγραφο.

9.6 Η ΑΠΕΔ δύναται να τερματίσει τη διαδικασία ταυτοποίησης, εάν οι οποιαδήποτε πληροφορία που παρέχεται από τον Συνδρομητή κατά τη διαδικασία ταυτοποίησης είναι ανακριβής ή αναληθής ή υπάρχει υποψία ότι ο Συνδρομητής έχει παράσχει ανακριβείς ή αναληθείς πληροφορίες ή η επαλήθευση της ταυτότητας του Συνδρομητή δεν είναι επιτυχής. Με την επιφύλαξη της παρ. 8.4, η ΑΠΕΔ δεν ευθύνεται για την πλαστότητα ή γνησιότητα των εγγράφων ταυτοποίησης ούτε για οποιαδήποτε ζημία τυχόν προκληθεί στον Συνδρομητή ή σε άλλα πρόσωπα λόγω αυτών.

## **10. Ισχύουσες Συμφωνίες, Πολιτικές, ΠΠ, ΔΠΠ**

Σχετικές συμφωνίες, πολιτικές και δηλώσεις πρακτικών που σχετίζονται με τους Όρους και Προϋποθέσεις για τη χρήση Εγκεκριμένων Υπηρεσιών Εμπιστοσύνης είναι οι εξής:

10.1 Πολιτική Πιστοποίησης της ΑΠΕΔ

10.2 Δήλωση Πρακτικής Πιστοποίησης της ΑΠΕΔ για Εγκεκριμένα Πιστοποιητικά Ηλεκτρονικών Υπογραφών

10.3 Προφίλ Πιστοποιητικών και OCSP για Εγκεκριμένα Πιστοποιητικά Ηλεκτρονικών Υπογραφών και ειδικότερα:

- Πολιτική για Πιστοποιητικό Πρωτεύουσας Αρχής Πιστοποίησης (1.2.300.0.110001.2)
- Πολιτική για Εγκεκριμένο πιστοποιητικό που εκδίδεται σε φυσικό πρόσωπο, όπου το ιδιωτικό κλειδί και το σχετικό πιστοποιητικό εγκαθίστανται σε ΕΔΔΥ (1.2.300.0.110001.2.1.1)
- Normalized Certificate Policy (OID 0.4.0.2042.1.1)
- Normalized Certificate Policy requiring a secure cryptographic device (OID 0.4.0.2042.1.2)

10.4 Πολιτική Πιστοποιητικού και Δήλωση Πρακτικής Πιστοποίησης της Αρχής Χρονosφραγίδας της ΑΠΕΔ

10.5 Πολιτική Απορρήτου της ΑΠΕΔ

10.6 Οι τρέχουσες εκδόσεις όλων των παραπάνω εφαρμοστέων εγγράφων δημοσιεύονται στη διεύθυνση: <https://pki.aped.gov.gr/repository>

## 11. Πολιτική Απορρήτου και Εμπιστευτικότητας

11.1 Η ΑΠΕΔ τηρεί την Πολιτική Απορρήτου, η οποία περιλαμβάνεται στον Αποθηκευτικό Χώρο της ΑΠΕΔ στη διεύθυνση <https://pki.aped.gov.gr/repository> και τη νομοθεσία της Ευρωπαϊκής Ένωσης, κατά την επεξεργασία προσωπικών πληροφοριών και πληροφοριών καταγραφής κινήσεων.

11.2 Όλες οι πληροφορίες που έχουν καταστεί γνωστές κατά την παροχή υπηρεσιών και δεν προορίζονται για κοινοποίηση (πχ. πληροφορίες που ήταν γνωστές στην ΑΠΕΔ λόγω λειτουργίας και παροχής Υπηρεσιών Εμπιστοσύνης) είναι εμπιστευτικές. Ο Συνδρομητής και το Υποκείμενο έχουν το δικαίωμα να λαμβάνουν πληροφορίες από την ΑΠΕΔ σχετικά με τους ίδιους, σύμφωνα με το νόμο. Οι κατηγορίες πληροφοριών που θεωρούνται Εμπιστευτικές αναφέρονται αναλυτικά στην ΠΠ της ΑΠΕΔ και στην Πολιτική Απορρήτου.

11.3 Η ΑΠΕΔ προστατεύει τις εμπιστευτικές πληροφορίες καθώς και πληροφορίες που προορίζονται για εσωτερική χρήση ώστε να μην εκτίθενται σε κίνδυνο και δεν προβαίνει στην αποκάλυψή τους σε τρίτα μέρη.

11.4 Η ΑΠΕΔ έχει το δικαίωμα να κοινοποιεί πληροφορίες σχετικά με τον Συνδρομητή ή το Υποκείμενο σε τρίτους, οι οποίοι σύμφωνα με τη σχετική νομοθεσία δικαιούνται να λαμβάνουν τις εν λόγω πληροφορίες.

11.5 Επιπλέον, τα μη εξατομικευμένα στατιστικά στοιχεία για τις υπηρεσίες της ΑΠΕΔ θεωρούνται επίσης δημόσιες πληροφορίες. Η ΑΠΕΔ μπορεί να δημοσιεύει μη εξατομικευμένα στατιστικά στοιχεία σχετικά με τις υπηρεσίες της.

## 12. Πολιτική Επιστροφής Χρημάτων

Η ΑΠΕΔ παρέχει τις υπηρεσίες εμπιστοσύνης που ορίζονται στην ΠΠ χωρίς κόστος.

## 13. Εφαρμοστέο δίκαιο, καταγγελίες και επίλυση διαφορών

13.1 Διαφορές ανάμεσα στην ΑΠΕΔ, τις εκδότριες ΑΠ, τους Συνδρομητές και Βασιζόμενα Μέρη θα επιλύονται σύμφωνα με την ισχύουσα νομοθεσία που διέπει τη σχέση μεταξύ των μερών.

13.2 Στον βαθμό που επιτρέπεται από τον νόμο, πριν από την προσφυγή σε οποιοδήποτε μηχανισμό επίλυσης διαφορών σε σχέση με διαφορά που αφορά σε οποιαδήποτε πτυχή των υπηρεσιών εμπιστοσύνης της ΑΠΕΔ, ο Συνδρομητής ή οποιοδήποτε άλλο μέρος πρέπει να ενημερώσει την ΑΠΕΔ, και οποιοδήποτε άλλο μέρος εμπλεκόμενο στη διαφορά 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. Όλα τα μέρη συμφωνούν ότι τα δικαστήρια της Αθήνας, στην Ελλάδα, έχουν αποκλειστική δικαιοδοσία και είναι αρμόδια για την επίλυση οποιασδήποτε διαφοράς σχετικά με την ερμηνεία και την εκτέλεση των παρόντων όρων και την παροχή υπηρεσιών της ΑΠΕΔ.

13.3 Όλα τα αιτήματα σχετικά με διαφορές θα πρέπει να αποστέλλονται στα στοιχεία επικοινωνίας που περιλαμβάνονται στους παρόντες Όρους και Προϋποθέσεις.

## 14. Άδειες Αποθηκευτικού χώρου, Σήματα Αξιοπιστίας και Έλεγχοι

14.1 Η ΑΠΕΔ είναι ένας Εγκεκριμένος Πάροχος Υπηρεσιών Εμπιστοσύνης στην οποία χορηγείται το καθεστώς εγκεκριμένου παρόχου από τον εποπτικό φορέα και περιλαμβάνεται στον Κατάλογο Εμπιστοσύνης Εγκεκριμένων Φορέων Παροχής Υπηρεσιών Πιστοποίησης της ΕΕ, μετά την υποβολή έκθεσης αξιολόγησης συμμόρφωσης από διαπιστευμένο Όργανο Αξιολόγησης της Συμμόρφωσης.

14.2 Οι Υπηρεσίες Εμπιστοσύνης της ΑΠΕΔ για τις Εγκεκριμένες Ηλεκτρονικές Υπογραφές είναι καταχωρημένες στην Ευρωπαϊκή λίστα Εμπιστοσύνης Εγκεκριμένων Παρόχων Υπηρεσιών Πιστοποίησης (List Of Trusted Lists - LOTL). Η Ευρωπαϊκή λίστα Εμπιστοσύνης Εγκεκριμένων Παρόχων Υπηρεσιών Πιστοποίησης είναι διαθέσιμη στον παρακάτω σύνδεσμο: [https://ec.europa.eu/information\\_society/policy/esignature/trusted-list/tl-mp.xml](https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml) <https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home>. Η απαίτηση της εν λόγω καταχώρισης είναι σύμφωνη με τον κανονισμό (ΕΥ) Νο 910/2014.

14.3 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.

14.4 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 δικτυακό τόπο της ΑΠΕΔ στη διεύθυνση: <https://pki.aped.gov.gr/repository>.

## 15. Στοιχεία Επικοινωνίας

Τα στοιχεία επικοινωνίας για την Αρχή Πιστοποίησης του Ελληνικού Δημοσίου δημοσιεύονται στην ιστοσελίδα: [www.aped.gov.gr](http://www.aped.gov.gr)

## 16. Ισχύς όρων και προϋποθέσεις

16.1 Η ισχύς του παρόντος κειμένου Όρων και Προϋποθέσεων άρχεται με την δημοσίευση του Κανονισμού Πιστοποίησης της ΑΠΕΔ στο Φύλλο της Εφημερίδας της Κυβέρνησης. Κατόπιν, το παρόν κείμενο δημοσιεύεται άμεσα στον δικτυακό αποθηκευτικό χώρο της ΑΠΕΔ.

16.2 Το παρόν κείμενο Όρων και Προϋποθέσεων θα παραμείνει εν ισχύ έως την αντικατάστασή του από τυχόν νέα, τροποποιημένη έκδοση. Οι τροποποιημένες ή νέες εκδόσεις παρατίθενται στο τμήμα του χώρου αποθήκευσης της ΑΠΕΔ.

16.3 Με την κατάργηση της ΠΠ της ΑΠΕΔ, οι ΥπΑΠ, οι Συνδρομητές και τα Βασιζόμενα Μέρη Υποδομής Δημοσίου Κλειδιού της ΑΠΕΔ, εξακολουθούν να δεσμεύονται από τους όρους της, ως προς όλα τα πιστοποιητικά που έχουν εκδοθεί κατά τη διάρκεια ισχύος της παρούσας, και για το υπόλοιπο της περιόδου ισχύος τους.

16.4 Εάν οποιαδήποτε διάταξη των παρόντων Όρων και Προϋποθέσεων, ή η εφαρμογή της, καταστεί για οποιονδήποτε λόγο και σε οποιονδήποτε βαθμό άκυρη ή ανεφάρμοστη, τότε η διαπίστωση της ακυρότητας ή του ανεφάρμοστου δεν θα επηρεάζει το λοιπό μέρος τους (και την εφαρμογή της άκυρης ή ανεφάρμοστης διάταξης σε άλλα πρόσωπα ή περιστάσεις), και θα ερμηνεύεται κατά τρόπο που ευλόγως θα εκπληρώνει τον σκοπό των μερών.

## 17. Επεξεργασία Δεδομένων Προσωπικού Χαρακτήρα

17.1 Ο συνδρομητής παρέχει στην ΑΠΕΔ την ρητή και ανεπιφύλακτη συγκατάθεσή του να συλλέγει, να ελέγχει, να επεξεργάζεται και να αρχειοθετεί τα προσωπικά του δεδομένα, τα οποία είναι απαραίτητα για την παροχή των υπηρεσιών εμπιστοσύνης. Η επεξεργασία αυτή των προσωπικών δεδομένων γίνεται στο πλαίσιο συμμόρφωσης με τις διατάξεις του σχετικού θεσμικού πλαισίου (νέος Γενικός Κανονισμός (ΕΕ) 2016/679 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 27ης Απριλίου 2016 «για την προστασία των φυσικών προσώπων έναντι της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα και για την ελεύθερη κυκλοφορία των δεδομένων αυτών» (ΓΚΠΔ ή GDPR), ν. 3471/2006, ν. 2472/1997 κ.λπ.) και τα δεδομένα αυτά δεν πρόκειται να χρησιμοποιηθούν για άλλους σκοπούς, χωρίς την ρητή συγκατάθεση του συνδρομητή

17.2 Τα προσωπικά αυτά δεδομένα συγκεντρώνονται αποκλειστικά από τους ίδιους τους συνδρομητές κατά την διαδικασία εγγραφής της συνδρομής τους και διατηρούνται για διάστημα τουλάχιστον 7 ετών από την λήξη των πιστοποιητικών, ώστε να χρησιμοποιηθούν ιδίως για την παροχή αποδεικτικών στοιχείων σε διαδικασίες επίλυσης διαφορών συναφείς με την πιστοποίηση των ηλεκτρονικών υπογραφών του συνδρομητή. Ο συνδρομητής δηλώνει ρητά ότι γνωρίζει, αποδέχεται και συναινεί με την παραπάνω επεξεργασία των προσωπικών του δεδομένων, καθώς και ότι εξουσιοδοτεί την ΑΠΕΔ (ή τον τυχόν διάδοχό της στην παροχή των σχετικών υπηρεσιών) να γνωστοποιεί σε τρίτους τα προσωπικά του δεδομένα σε κάθε διαδικασία επίλυσης διαφορών που σχετίζεται με τη χρήση των πιστοποιητικών του.

17.3 Σε κάθε περίπτωση ο συνδρομητής έχει δικαίωμα να απευθυνθεί στην ΑΠΕΔ (η οποία αποτελεί για την περίπτωση τον «Υπεύθυνο Επεξεργασίας των δεδομένων του» σύμφωνα με τον νόμο), για να κάνει χρήση των δικαιωμάτων «Ενημέρωσης» (άρθρα 12, 13 και 14 του GDPR), «Πρόσβασης» (άρθρο 15 του GDPR) και «Φορητότητας» (άρθρο 20 του GDPR).