ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ
Γενική Διεύθυνση
ΠΡΟΣΩΠΙΚΟ ΚΑΙ ΔΙΟΙΚΗΣΗ
Διεύθυνση SPS - Υπηρεσία πρωτοκόλλου και ασφάλειας
Ασφάλεια πληροφορικής

Ευρωπαϊκή Επιτροπή

ΔΗΛΩΣΗ ΓΙΑ ΤΗΝ ΠΡΑΚΤΙΚΗ ΠΙΣΤΟΠΟΙΗΣΗΣ

(Έκδοση 1.0 της 25/02/2002)

Bâtiment Jean Monnet, Rue Alcide de Gasperi, L-2920 Luxembourg. Τηλέφωνο: (352)43011.

Rue de la Loi 200, B-1049 Bruxelles / Wetstraat 200, B-1049 Brussel - Belgium. Τηλέφωνο: (32-2)299 11 11.

Πίνακας περιεχομένων

1. ΕΙΣΑΓΩΓΗ

Η γενική δομή του παρόντος εγγράφου βασίζεται στην αίτηση για σχολιασμό 2527 (RFC 2527), στην οποία περιλαμβάνεται περιεκτική ανάλυση του θέματος.

Στο πλαίσιο το οποίο τίθεται από το έγγραφο RFC 2527 γίνεται μια περιεκτική απαρίθμηση των θεμάτων τα οποία πρέπει να περιλαμβάνονται σε μια δήλωση για την πρακτική πιστοποίησης.

Οι ακόλουθες τυπογραφικές συμβάσεις σημαίνουν:

- απλοί χαρακτήρες: έχει υλοποιηθεί και λειτουργεί
- πλάγιοι χαρακτήρες: δεν έχει υλοποιηθεί ακόμη, αφορά μελλοντικές εξελίξεις
- Κείμενο μέσα σε αγκύλες: προς συζήτηση

Η Ευρωπαϊκή Επιτροπή υλοποιεί μια υποδομή δημόσιου κλειδιού (ΥΔΚ) προκειμένου να διασφαλίσει την ασφάλεια των ηλεκτρονικών πληροφοριών της. Η ΥΔΚ αυτή αποτελείται από συστήματα, προϊόντα και υπηρεσίες που χορηγούν και διαχειρίζονται πιστοποιητικά X.509 για κρυπτογραφία δημόσιου κλειδιού.

Σκοπός του παρόντος εγγράφου είναι να περιγραφούν οι πρακτικές πιστοποίησης οι οποίες ακολουθούνται από την αρχή πιστοποίησης (ΑΠ) της Ευρωπαϊκής Επιτροπής, η οποία ονομάζεται CommisSign, ώστε να διασφαλιστεί η αξιοπιστία της ΑΠ όσον αφορά τη χορήγηση πιστοποιητικών δημόσιου κλειδιού σε συνδρομητές. Το παρόν έγγραφο έχει εκπονηθεί σύμφωνα με τις απαιτήσεις της πολιτικής πιστοποιητικών της ευρωπαϊκής υποδομής δημόσιου κλειδιού (ΥΔΚ). Η σχέση μεταξύ της πολιτικής πιστοποιητικών της ΥΔΚ της Ευρωπαϊκής Επιτροπής και του παρόντος εγγράφου είναι η εξής: στην πολιτική πιστοποιητικών δηλώνονται οι πολιτικές της ΑΠ CommisSign, ενώ στο παρόν έγγραφο περιέχονται αναλυτικές οδηγίες για την υλοποίηση της πολιτικής πιστοποιητικών.

Συνιστάται στους χρήστες του παρόντος εγγράφου να ανατρέξουν στην πολιτική πιστοποιητικών της υποδομής δημόσιου κλειδιού (ΥΔΚ) της Ευρωπαϊκής Επιτροπής, ώστε να ενημερωθούν σχετικά με τις πολιτικές στις οποίες βασίζεται η δήλωση για την πρακτική πιστοποίησης (ΔΠΠ) της ΑΠ CommisSign.

1.1. Επισκόπηση

Οι προδιαγραφές της παρούσας δήλωσης για την πρακτική πιστοποίησης ακολουθούν και τηρούν την πολιτική πιστοποιητικών της ΥΔΚ X.509 της Internet Engineering Task Force (IETF PKIX) και το πλαίσιο δήλωσης για την πρακτική πιστοποίησης (τμήμα 4).

Το παρόν έγγραφο προορίζεται για χρήση από την Ευρωπαϊκή Επιτροπή και κάθε άλλο φορέα που χρειάζεται να εκτιμά την αξιοπιστία της ΑΠ CommisSign και την καταλληλότητα των πιστοποιητικών της όσον αφορά την τήρηση των απαιτήσεών του σχετικά με την ασφάλεια των ηλεκτρονικών πληροφοριών.

Οι πρακτικές στο παρόν έγγραφο υποστηρίζουν ασφάλεια μεσαίου επιπέδου, εκτός εάν ορίζεται διαφορετικά. Καθώς η Ευρωπαϊκή Επιτροπή προσθέτει περαιτέρω επίπεδα ασφάλειας, το παρόν έγγραφο θα τροποποιείται ώστε να περιλαμβάνει και την περιγραφή των πρακτικών για τα αντίστοιχα επίπεδα ασφάλειας.

Στη δήλωση για την πρακτική πιστοποίησης (ΔΠΠ) της ΑΠ CommisSign περιγράφεται η δημιουργία, η διαχείριση και η χρήση των πιστοποιητικών δημόσιου κλειδιού X.509 έκδοση 3 σε εφαρμογές που απαιτούν επικοινωνία μεταξύ δικτυωμένων συστημάτων που βασίζονται σε ηλεκτρονικό υπολογιστή και σε εφαρμογές που απαιτούν ακεραιότητα και εμπιστευτικότητα των ηλεκτρονικών πληροφοριών. Στις εφαρμογές αυτές περιλαμβάνονται, ενδεικτικά, το ηλεκτρονικό ταχυδρομείο, η μετάδοση πληροφοριών με διαβάθμιση μέχρι και «περιορισμένης χρήσης ΕΕ», η ψηφιακή υπογραφή ηλεκτρονικών εγγράφων. Επισημαίνεται ότι ο όρος «πιστοποιητικά X.509», όπως χρησιμοποιείται στο πλαίσιο του παρόντος εγγράφου, σημαίνει το πιστοποιητικό X.509 έκδοση 3. Επισημαίνεται επίσης ότι ο όρος «λογισμικό πελάτη ΥΔΚ» ή «λογισμικό ΥΔΚ» αναφέρεται στο λογισμικό που παρέχει τη δυνατότητα εκτέλεσης λειτουργιών ΥΔΚ στο πλαίσιο του τομέα της ΑΠ CommisSign.

Η χορήγηση πιστοποιητικών δημόσιου κλειδιού στο πλαίσιο της παρούσας ΔΠΠ

- δεν πρέπει να χρησιμοποιείται για την προστασία εμπιστευτικών, απόρρητων και άκρως απόρρητων πληροφοριών της ΕΕ

- δεν συνεπάγεται ότι ο συνδρομητής εξουσιοδοτείται να διενεργεί επιχειρηματικές συναλλαγές εξ ονόματος της Ευρωπαϊκής Επιτροπής.

Η παρούσα ΔΠΠ αξιολογείται από την αρχή για την άσκηση πολιτικής (ΑΑΠ) σε θέματα ΥΔΚ της Ευρωπαϊκής Επιτροπής, η οποία εγκρίνει όλες τις ΔΠΠ της ΑΠ στο πλαίσιο της ΥΔΚ της Ευρωπαϊκής Επιτροπής.

Όσον αφορά τη δυνατότητα επιβολής, τη σύνταξη, την ερμηνεία και την ισχύ της παρούσας ΔΠΠ και της σχετικής πολιτικής πιστοποιητικών, η ΑΠ CommisSign διέπεται από τις κανονιστικές ρυθμίσεις της Ευρωπαϊκής Επιτροπής.

Η αρχή για την άσκηση πολιτικής (ΑΑΠ) της Ευρωπαϊκής Επιτροπής είναι υπεύθυνη για τη γενική διαχείριση της ΥΔΚ της Ευρωπαϊκής Επιτροπής. Είναι επίσης υπεύθυνη για τη χάραξη των πολιτικών στο πλαίσιο των οποίων λειτουργεί η ΥΔΚ της Ευρωπαϊκής Επιτροπής. Καθήκον της ΑΑΠ είναι, μεταξύ άλλων, να διασφαλίζει ότι η ΑΠ CommisSign λειτουργεί σύμφωνα με τις πολιτικές και τις πρακτικές που καθορίζονται στα σχετικά έγγραφα πιστοποίησης και πιστοποιητικών και να εγκρίνει και να χορηγεί αμοιβαίες πιστοποιήσεις. Φορείς της ΑΑΠ είναι το σύνολο των μελών της Ευρωπαϊκής Επιτροπής.

Η αρχή πιστοποίησης (ΑΠ) της Ευρωπαϊκής Επιτροπής είναι υπεύθυνη για τη δημιουργία και τη διαχείριση των πιστοποιητικών δημόσιου κλειδιού X.509 έκδοση 3, τα οποία θα χρησιμοποιηθούν από την Ευρωπαϊκή

Επιτροπή σύμφωνα με την πολιτική πιστοποιητικών της Ευρωπαϊκής Επιτροπής και την παρούσα ΔΠΠ.

Η Ευρωπαϊκή Επιτροπή χρησιμοποιεί μία κεντρική αρχή καταχώρισης (ΑΚ) και τοπικές αρχές καταχώρισης (ΤΑΚ) για τη συγκέντρωση πληροφοριών, την επαλήθευση της ταυτότητας και της εξουσιοδότησης και την υποβολή αιτημάτων εξ ονόματος των χρηστών τους για τη λήψη μέτρων διαχείρισης των πιστοποιητικών.

1.2. Ορισμός

Το παρόν έγγραφο είναι η δήλωση για την πρακτική πιστοποίησης (ΔΠΠ) της αρχής πιστοποίησης της Ευρωπαϊκής Επιτροπής. Οι πρακτικές που περιγράφονται στο παρόν έγγραφο συμμορφώνονται με την πολιτική ασφάλειας σχετικά με την υποδομή δημόσιου κλειδιού (ΥΔΚ) της Ευρωπαϊκής Επιτροπής.

1.3. Κοινότητα και δυνατότητα εφαρμογής

Η παρούσα ΔΠΠ καταρτίστηκε με τρόπον ώστε να πληροί τις γενικές απαιτήσεις της Ευρωπαϊκής Επιτροπής όσον αφορά τα πιστοποιητικά δημόσιου κλειδιού.

Η ΑΠ CommisSign είναι η αρχή πιστοποίησης (ΑΠ) στο πλαίσιο της ΥΔΚ της Ευρωπαϊκής Επιτροπής.

1.3.1. Αρχή πιστοποίησης (ΑΠ)

Η ΑΠ CommisSign προορίζεται για χρήση στο πλαίσιο της Ευρωπαϊκής Επιτροπής και ενδεχομένως από οργανισμούς ή ιδιώτες εκτός Ευρωπαϊκής Επιτροπής, οι οποίοι ωστόσο ανταλλάσσουν με αυτήν μηνύματα μέσω ηλεκτρονικού ταχυδρομείου.

Η ΑΠ CommisSign χορηγεί, υπογράφει και διαχειρίζεται πιστοποιητικά δημόσιου κλειδιού, καθώς επίσης χορηγεί πιστοποιητικά χρήστη σε όλα τα μέλη του προσωπικού της Ευρωπαϊκής Επιτροπής ανάλογα με τις εκάστοτε ανάγκες, αποκλείοντας οποιονδήποτε άλλον.

Η ΑΠ CommisSign στελεχώνεται από προσωπικό υπεύθυνο για τη γενική λειτουργία της ΑΠ και από προσωπικό υπεύθυνο για τη λειτουργία και συντήρηση του εξυπηρετητή της ΑΠ και του λογισμικού της. Η αρχή λειτουργίας (ΑΛ) της ΑΠ είναι υπεύθυνη για την κατάρτιση και τη διαχείριση της δήλωσης για την πρακτική της ΑΠ και για τη διαχείριση του κύριου κλειδιού. Η ΑΛ είναι υπεύθυνη για την επανεξέταση των λειτουργιών των αρχών καταχώρισης (ΑΚ) στο πλαίσιο του τομέα της ΑΠ της. Η ΑΛ υποβάλλει εκθέσεις στην ΑΑΠ σχετικά με θέματα λειτουργίας της ΑΠ.

Τα στελέχη της ΑΠ είναι υπεύθυνα για τη λειτουργία και τη διαχείριση του εξυπηρετητή και του λογισμικού της ΑΠ.

Η ΑΠ CommisSign είναι υπεύθυνη για:

- τη δημιουργία και την υπογραφή των πιστοποιητικών X.509 τα οποία συνδέουν τους συνδρομητές που ανήκουν στο προσωπικό της Ευρωπαϊκής Επιτροπής με τα δημόσια κλειδιά τους

- τη διάδοση των πιστοποιητικών X.509 μέσω καταλόγων

- τη δημοσιοποίηση της κατάστασης των πιστοποιητικών μέσω των ΚΑΠ [δεν έχει τεθεί ακόμη σε λειτουργία]

- τη λειτουργία της ΑΠ σύμφωνα με την παρούσα ΔΠΠ

- την έγκριση και το διορισμό στελεχών για την πλήρωση των θέσεων της ΥΔΚ

- την επανεξέταση και τον έλεγχο των λειτουργιών των ΑΚ και ΤΑΚ στο πλαίσιο του τομέα της

- την επίλυση διαφορών μεταξύ τελικών χρηστών και ΑΠ, ΑΚ ή ΤΑΚ

- την υποβολή αιτήματος ανάκλησης πιστοποιητικού στελέχους της ΥΔΚ ή της ΑΚ.

Όπου κρίνεται αναγκαίο, στην παρούσα ΔΠΠ γίνεται διάκριση των διαφόρων χρηστών και ρόλων που έχουν πρόσβαση στις λειτουργίες της ΑΠ. Όταν δεν απαιτείται να γίνει διάκριση, ο όρος ΑΠ αναφέρεται στο σύνολο της οντότητας ΑΠ, συμπεριλαμβανομένου του λογισμικού και των λειτουργιών της.

(* Επισημαίνεται ότι η αμοιβαία πιστοποίηση διεξάγεται σύμφωνα με την παρούσα ΔΠΠ και οποιεσδήποτε περαιτέρω απαιτήσεις ορίζονται από την ΑΑΠ της Ευρωπαϊκής Επιτροπής. Όλες οι αμοιβαίες πιστοποιήσεις μεταξύ χρηστών της Ευρωπαϊκής Επιτροπής και άλλων ΑΠ θα πραγματοποιούνται σύμφωνα με τις οδηγίες της ΑΑΠ της Ευρωπαϊκής Επιτροπής. Οποιαδήποτε αποδοχή πραγματοποιείται με άλλες ΑΠ πρέπει να τεκμηριώνεται και οι αντίστοιχες ρήτρες αποποίησης ευθύνης να τίθενται στη διάθεση των χρηστών που ανήκουν στο προσωπικό της Ευρωπαϊκής Επιτροπής).

1.3.2. Αρχές καταχώρισης (ΑΚ)

Η αρχή καταχώρισης (ΑΚ) είναι μια οντότητα αρμόδια για τη διαχείριση των τελικών οντοτήτων εξ ονόματος της ΑΠ της Ευρωπαϊκής Επιτροπής. Υπάρχουν μία κεντρική αρχή καταχώρισης (ΑΚ) και πολλές τοπικές αρχές καταχώρισης (ΤΑΚ).

Οι όροι ΑΚ/ΤΑΚ αναφέρονται σε έναν υπάλληλο της Ευρωπαϊκής Επιτροπής με προνόμια ΑΚ/ΤΑΚ, ο οποίος εκτελεί τις λειτουργίες ΑΚ/ΤΑΚ.

Η **ΑΚ** είναι υπεύθυνη για:

- την ταυτοποίηση και την επαλήθευση της διοικητικής ταυτότητας των αιτούντων χορήγηση πιστοποιητικού

- τη δημιουργία και την αλλαγή του SubjectName του χρήστη στο πιστοποιητικό
- την εξέταση των μητρώων ελέγχου και την αναφορά των ύποπτων συμβάντων στην ΑΛ της ΑΠ και
- τη σύνταξη σειράς εκθέσεων σχετικά με την κατάσταση των χρηστών.

Η **ΤΑΚ** είναι υπεύθυνη για:

- την ταυτοποίηση και την επαλήθευση της φυσικής ταυτότητας των αιτούντων χορήγηση πιστοποιητικού
- την επαλήθευση της αυθεντικότητας του αιτήματος για τη χορήγηση πιστοποιητικού
- την επαλήθευση του SubjectName του χρήστη
- την παραλαβή και τη διανομή στοιχείων σχετικά με την εξουσιοδότηση του συνδρομητή
- την εκτέλεση λειτουργιών πιστοποίησης και διαχείρισης για τις τελικές οντότητές της (όπως ενεργοποίηση χρηστών, απενεργοποίηση/αναστολή ισχύος πιστοποιητικού χρήστη)
- την ενημέρωση των πιστοποιητικών, [*την ανάκληση πιστοποιητικών* και] τη διαχείριση της ανάκτησης κλειδιών των τελικών οντοτήτων.

1.3.3. Φορείς αποθήκευσης

Η ΑΠ CommisSign χρησιμοποιεί τον κατάλογο της Ευρωπαϊκής Επιτροπής για τη δημοσίευση και διανομή των πιστοποιητικών, των καταστάσεων ανάκλησης πιστοποιητικών (ΚΑΠ) [και των καταστάσεων ανάκλησης εξουσιοδοτήσεων (ΚΑΕ)]. Τον κατάλογο της Ευρωπαϊκής Επιτροπής διαχειρίζεται η Γενική Διεύθυνση Πληροφορικής. Ο κατάλογος είναι διαθέσιμος 24 ώρες το εικοσιτετράωρο με λειτουργική υποστήριξη 12 ώρες ημερησίως, τις εργάσιμες ημέρες.

1.3.4. Συνδρομητές

Οι συνδρομητές χρησιμοποιούν ιδιωτικά κλειδιά τα οποία [εκχωρούνται και/ή] πιστοποιούνται από την ΑΠ CommisSign εφόσον εγκριθεί η αίτησή τους. Οι συνδρομητές ανήκουν στο προσωπικό της Ευρωπαϊκής Επιτροπής.

Πιστοποιητικά είναι δυνατόν να χορηγούνται και σε λειτουργικές ταχυδρομικές θυρίδες. Στην περίπτωση αυτή, η υποβολή αίτησης και η διατήρηση του πιστοποιητικού πρέπει να γίνεται από τον αρμόδιο γι' αυτήν την χωρίς ανθρώπινη υπόσταση τελική οντότητα. Ο αρμόδιος μπορεί να εκχωρήσει τα δικαιώματά του σε άλλο πρόσωπο (που ενεργεί ως αναπληρωτής).

Επιπλέον, οι συνδρομητές μπορούν να χρησιμοποιούν τα πιστοποιητικά που χορηγούνται από την ΑΠ CommisSign για να κρυπτογραφούν πληροφορίες

για άλλους συνδρομητές και να επαληθεύουν τις ψηφιακές υπογραφές τους (στο πλαίσιο του τομέα της ΑΠ CommisSign, καθώς επίσης τομέων που έχουν πιστοποιηθεί αμοιβαία). Υπό αυτή την έννοια, οι συνδρομητές είναι και συμβαλλόμενα μέρη.

Στην παρούσα ΔΠΠ, ο όρος τελική οντότητα αναφέρεται γενικά στους χρήστες είτε ενεργούν ως συνδρομητές είτε ενεργούν ως συμβαλλόμενα μέρη. Στις περιπτώσεις στις οποίες απαιτείται διαχωρισμός των ρόλων αυτών στην παρούσα ΔΠΠ, ο όρος συνδρομητής αναφέρεται στην τελική οντότητα ως υποκείμενο του πιστοποιητικού, ενώ ο όρος συμβαλλόμενο μέρος αναφέρεται στην τελική οντότητα ως φορέα που επαληθεύει τα πιστοποιητικά που έχουν χορηγηθεί από την ΑΠ CommisSign.

1.3.5. Συμβαλλόμενα μέρη

Συμβαλλόμενο μέρος μπορεί να είναι είτε ένα υποκείμενο πιστοποιητικού της ΑΠ CommisSign είτε κάποιος συνδρομητής εξωτερικής ΑΠ που έχει [υπογράψει συμφωνία αμοιβαίας πιστοποίησης με] εμπιστευτεί την ΑΠ CommisSign. Τα δικαιώματα και οι υποχρεώσεις των συμβαλλομένων μερών που είναι υποκείμενα πιστοποιητικών της ΑΠ CommisSign περιλαμβάνονται στην παρούσα ΔΠΠ. [Τα δικαιώματα και οι υποχρεώσεις των συμβαλλομένων μερών που ανήκουν σε εξωτερική ΑΠ περιλαμβάνονται στη συμφωνία αμοιβαίας πιστοποίησης που συνάπτεται μεταξύ των δύο κατόχων των ΑΠ].

1.3.6. Δυνατότητα εφαρμογής

Οι πρακτικές που περιγράφονται στην παρούσα ΔΠΠ ισχύουν για την ΑΠ CommisSign και τους διαχειριστές της, το φορέα αποθήκευσης που χρησιμοποιείται από την ΑΠ CommisSign, τις τελικές οντότητες στις οποίες χορηγούνται πιστοποιητικά από την ΑΠ CommisSign και τα συμβαλλόμενα μέρη.

Οι πρακτικές που περιγράφονται στην παρούσα ΔΠΠ ενδείκνυνται για χρήση των πιστοποιητικών με σκοπό, μεταξύ άλλων, την ηλεκτρονική επαλήθευση της ταυτότητας, της εξουσιοδότησης και της ακεραιότητας των δεδομένων όσον αφορά πληροφορίες της Ευρωπαϊκή Επιτροπής που διαβιβάζονται σε συστήματα μέχρι και κρίσιμων πληροφοριών (βλ. πολιτική ασφάλειας ΤΠΕ).

Οι πρακτικές που περιγράφονται στην παρούσα ΔΠΠ ενδείκνυνται για χρήση των πιστοποιητικών σε περιπτώσεις στις οποίες απαιτείται να διασφαλιστεί η εμπιστευτικότητα πληροφοριών της Ευρωπαϊκής Επιτροπής με διαβάθμιση μέχρι και «πληροφορίες περιορισμένης χρήσης ΕΕ» (βλ. πολιτική ασφάλειας ΤΠΕ).

Απαγορεύεται η χρήση των πιστοποιητικών για τις εφαρμογές οι οποίες καθορίζονται από την ΑΑΠ της Ευρωπαϊκής Επιτροπής. Γενικά εφαρμογές για τις οποίες απαγορεύεται η χρήση των χορηγούμενων πιστοποιητικών είναι:

- εφαρμογές που χρησιμοποιούν ή περιέχουν εμπιστευτικές, απόρρητες και άκρως απόρρητες πληροφορίες της ΕΕ

- εφαρμογές που δεν σχετίζονται με το έργο της Ευρωπαϊκής Επιτροπής.

1.4. Υπεύθυνος επικοινωνίας

Την παρούσα δήλωση για την πρακτική πιστοποίησης διαχειρίζεται η υπηρεσία πρωτοκόλλου και ασφάλειας της Ευρωπαϊκής Επιτροπής.

Υπεύθυνος επικοινωνίας:

Mr Gérard BREMAUD

CommisSign CA Operations Authority

Protocol and Security Service

Jean-Monnet Building B2/072

L-2920 LUXEMBOURG

2. ΓΕΝΙΚΕΣ ΔΙΑΤΑΞΕΙΣ

2.1. Υποχρεώσεις

2.1.1. Υποχρεώσεις της ΑΠ

Η ΑΠ CommisSign συμμορφώνεται με τις απαιτήσεις της πολιτικής ασφάλειας ΤΕΠ, με όλες τις απαιτήσεις της παρούσας ΔΠΠ και με τις σχετικές ευρωπαϊκές και εθνικές κανονιστικές ρυθμίσεις.

Η **ΑΠ CommisSign** υποχρεούται:

- να καταρτίζει, να διατηρεί και να δημοσιεύει δήλωση για την πρακτική πιστοποίησης
- να παρέχει υπηρεσίες ΑΠ σύμφωνα με τις πρακτικές που περιγράφονται στην παρούσα ΔΠΠ
- να παρέχει υπηρεσίες εξυπηρετητή ΑΠ 7 ημέρες την εβδομάδα, 24 ώρες το εικοσιτετράωρο, με τον όρο ότι τούτο δεν αποτελεί εγγύηση για 100% διαθεσιμότητα (η διαθεσιμότητα μπορεί να επηρεαστεί από τις εργασίες συντήρησης ή επιδιόρθωσης του συστήματος ή από παράγοντες εκτός του ελέγχου της ΑΠ)
- να χορηγεί πιστοποιητικά στα μέλη του προσωπικού της Ευρωπαϊκής Επιτροπής [και σε άλλες ΑΠ], σύμφωνα με τις πρακτικές που αναφέρονται στην παρούσα ΔΠΠ και στην πολιτική για το πιστοποιητικό X.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής
- να ανακαλεί πιστοποιητικά εφόσον λάβει σχετικό έγκυρο αίτημα, σύμφωνα με τις πρακτικές της παρούσας ΔΠΠ και την πολιτική για το πιστοποιητικό X.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής

- να παρέχει υπηρεσίες ανάκτησης κλειδιού κρυπτογράφησης, σύμφωνα με τις πρακτικές που αναφέρονται στην παρούσα ΔΠΠ και στην πολιτική για το πιστοποιητικό X.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής

- να εκδίδει και να δημοσιεύει ΚΑΠ [και ΚΑΕ] σε τακτά χρονικά διαστήματα, όπως προβλέπεται στην παρούσα ΔΠΠ και στην πολιτική για το πιστοποιητικό X.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής

- να ενημερώνει τρίτους (π.χ. συμβαλλόμενα μέρη) σχετικά με τη χορήγηση/ανάκληση πιστοποιητικών εξασφαλίζοντας πρόσβαση στα πιστοποιητικά, στις ΚΑΠ [και στις ΚΑΕ] που βρίσκονται στο φορέα αποθήκευσης της ΑΠ CommisSign

- να διασφαλίζει τη γνώση και την τήρηση, εκ μέρους των συνδρομητών της ΑΠ CommisSign και των ΑΚ, της παρούσας ΔΠΠ δημοσιεύοντας τη ΔΠΠ και την πολιτική για το πιστοποιητικό X.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής, καθώς επίσης ασκώντας έλεγχο στις ΑΚ στο πλαίσιο του τομέα της ΑΠ CommisSign

- να διασφαλίζει, από κοινού με την ΑΑΠ της Ευρωπαϊκής Επιτροπής, τη λήψη διορθωτικών μέτρων για την αντιμετώπιση αδυναμιών της ΑΠ ή της ΑΚ που διαπιστώνονται μέσω του ελέγχου

- να υποβάλλει στην ΑΑΠ έκθεση σχετικά με την πρόοδο των διορθωτικών ενεργειών.

Μετά τη δημιουργία του, το πιστοποιητικό του συνδρομητή δημοσιεύεται στον κατάλογο της Ευρωπαϊκής Επιτροπής. Σε περίπτωση ανάκλησης πιστοποιητικού συνδρομητή, η ανάκληση εγγράφεται και δημοσιεύεται στην κατάσταση ανάκλησης πιστοποιητικών (ΚΑΠ) και στον κατάλογο της Ευρωπαϊκής Επιτροπής.

Με τη δημοσίευση ενός πιστοποιητικού στον κατάλογο της Ευρωπαϊκής Επιτροπής, η ΑΠ CommisSign πιστοποιεί ότι έχει χορηγήσει πιστοποιητικό στο όνομα του εν λόγω συνδρομητή, ότι τα στοιχεία που αναφέρονται στο πιστοποιητικό έχουν επαληθευθεί σύμφωνα με την παρούσα ΔΠΠ και ότι ο συνδρομητής έχει δεχτεί το πιστοποιητικό.

Η ΑΠ CommisSign κοινοποιεί τα δικαιώματα και τις υποχρεώσεις των συνδρομητών και των συμβαλλομένων μερών που προβλέπονται στην παρούσα ΔΠΠ μέσω της δημοσίευσης της παρούσας ΔΠΠ και της πολιτικής για το πιστοποιητικό X.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής.

Η ΑΠ CommisSign προστατεύει τα ιδιωτικά κλειδιά της όπως προβλέπεται στο τμήμα 6 της παρούσας ΔΠΠ.

[Η ΑΠ CommisSign προστατεύει τα ιδιωτικά κλειδιά τα οποία κατέχει ή αποθηκεύει σύμφωνα με τα τμήματα 4 και 6 της παρούσας ΔΠΠ].

Το κλειδί υπογραφής της ΑΠ CommisSign χρησιμοποιείται για την υπογραφή των πιστοποιητικών και των ΚΑΠ.

[Η ΑΠ CommisSign μπορεί να χορηγεί αμοιβαίες πιστοποιήσεις προς άλλες ΑΠ και να τις υπογράφει μόνον εφόσον διαθέτει ρητή εξουσιοδότηση από την ΑΑΠ της Ευρωπαϊκής Επιτροπής].

2.1.2. Υποχρεώσεις των ΑΚ και ΤΑΚ

Οι ΑΚ και ΤΑΚ της Ευρωπαϊκής Επιτροπής στο πλαίσιο του τομέα της ΑΠ CommisSign υποχρεούνται να συμμορφώνονται με τις απαιτήσεις της παρούσας ΔΠΠ και της πολιτικής για το πιστοποιητικό Χ.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής.

Η **ΑΚ** υποχρεούται:

- να παρέχει υπηρεσίες ΑΚ στις αντίστοιχες ΤΑΚ της. Οι ώρες λειτουργίας της ΑΚ συμπίπτουν με το σύνηθες ωράριο εργασίας των υπηρεσιών της Ευρωπαϊκής Επιτροπής.

- να διασφαλίζει ότι οι υπηρεσίες ΑΚ συνάδουν με τις απαιτήσεις για τις σχετικές πρακτικές που προβλέπονται στο παρόν έγγραφο και στην πολιτική για το πιστοποιητικό Χ.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής

- να λογοδοτεί για συναλλαγές οι οποίες πραγματοποιούνται εξ ονόματος της ΑΠ

- να εφιστά την προσοχή των συνδρομητών της σε όλες τις σημαντικές πληροφορίες σχετικά με τα δικαιώματα και τις υποχρεώσεις της ΑΠ, της ΑΚ και των συνδρομητών, οι οποίες περιέχονται στην παρούσα ΔΠΠ, στη σύμβαση συνδρομής και σε κάθε άλλο σχετικό έγγραφο στο οποίο περιγράφονται οι όροι και οι προϋποθέσεις χρήσης.

Όταν η ΑΚ συνδέεται με τον εξυπηρετητή της ΑΠ για να επεξεργαστεί ένα αίτημα για πιστοποιητικό, η ΑΚ πιστοποιεί ότι έχει επαληθεύσει την ταυτότητα του συγκεκριμένου συνδρομητή σύμφωνα με τις πρακτικές που περιγράφονται στα τμήματα 3 και 4 της παρούσας ΔΠΠ.

Οι **ΤΑΚ** υποχρεούνται:

- να επαληθεύουν την ακρίβεια και την αυθεντικότητα των στοιχείων που παρέχονται από τους συνδρομητές για τη χορήγηση πιστοποιητικού (η επαλήθευση αυτή παρέχεται από τις ΤΑΚ εξ ονόματος της ΑΠ CommisSign)

- να ζητούν την ανάκληση του πιστοποιητικού συνδρομητή σύμφωνα με τις διατάξεις του παρόντος εγγράφου]

- να διασφαλίζουν ότι οι υπηρεσίες ΤΑΚ συνάδουν με τις απαιτήσεις για τις σχετικές πρακτικές που προβλέπονται στο παρόν έγγραφο και στην πολιτική για το πιστοποιητικό Χ.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής

- να λογοδοτούν για συναλλαγές οι οποίες πραγματοποιούνται εξ ονόματος της ΑΠ

- να έχουν την ευθύνη για την επεξεργασία των αιτήσεων χορήγησης [*και ανάκλησης]* πιστοποιητικού

- να γνωστοποιούν στο συνδρομητή την έγκριση της αίτησής του και τυχόν περαιτέρω ενέργειες που απαιτούνται από αυτόν.

Κάθε ΑΚ και ΤΑΚ πρέπει να διασφαλίζει ότι τα ιδιωτικά κλειδιά της προστατεύονται σύμφωνα με τους ελέγχους που περιγράφονται στο τμήμα 6 της παρούσας ΔΠΠ.

Οι ΑΚ και ΤΑΚ μπορούν να χρησιμοποιούν τα ιδιωτικά κλειδιά τους μόνο για τις εργασίες της Ευρωπαϊκής Επιτροπής και μόνο για σκοπούς εγκεκριμένους από την πολιτική για το πιστοποιητικό Χ.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής και σύμφωνα με την παρούσα ΔΠΠ.

2.1.3. Υποχρεώσεις των συνδρομητών

Στον τομέα της ΑΠ CommisSign, οι τελικές οντότητες είναι τόσο συνδρομητές όσο και συμβαλλόμενα μέρη. Ως συνδρομητές, υποχρεούνται:

- να δηλώνουν πάντοτε επακριβώς, τόσο στην ΑΠ CommisSign όσο και στην ΑΚ, τα στοιχεία που αναφέρονται στα πιστοποιητικά τους, καθώς και άλλα στοιχεία ταυτοποίησης και επαλήθευσης της ταυτότητάς τους

- να χρησιμοποιούν τα πιστοποιητικά αποκλειστικά για νόμιμες και εγκεκριμένες εργασίες της Ευρωπαϊκής Επιτροπής, συνεπείς προς την ισχύουσα πολιτική πιστοποιητικών και την παρούσα ΔΠΠ

- να προστατεύουν τα ιδιωτικά κλειδιά αποθηκεύοντάς τα είτε σε σκληρό δίσκο [σε έξυπνη κάρτα] είτε σε δισκέτα, ανάλογα με την πρακτική που εφαρμόζει η εκάστοτε ΓΔ

- να αφαιρούν το μέσο στο οποίο είναι αποθηκευμένο το ιδιωτικό κλειδί από τον ηλεκτρονικό υπολογιστή όταν δεν χρησιμοποιείται, εφόσον το ιδιωτικό κλειδί είναι αποθηκευμένο σε δισκέτα [ή σε έξυπνη κάρτα]

- να φέρουν επάνω τους το μέσο στο οποίο είναι αποθηκευμένο το ιδιωτικό κλειδί ή να το φυλάσσουν σε ασφαλή και κλειδωμένο χώρο, εφόσον το ιδιωτικό κλειδί είναι αποθηκευμένο σε δισκέτα [ή σε έξυπνη κάρτα]

- να προστατεύουν τον κωδικό πρόσβασης συνδρομητή σύμφωνα με τους κανόνες ασφάλειας ΤΕΠ

- να ενημερώνουν την ΤΑΚ τους εντός 48 ωρών σχετικά με οποιαδήποτε μεταβολή των στοιχείων που περιλαμβάνονται στο πιστοποιητικό τους ή στην αίτηση χορήγησης πιστοποιητικού

- να ενημερώνουν την ΤΑΚ τους εντός 8 ωρών σχετικά με οποιαδήποτε υποψία αλλοίωσης ενός ή και των δύο ιδιωτικών κλειδιών τους

- να λαμβάνουν λογικές προφυλάξεις ώστε να αποφεύγεται η απώλεια, η αποκάλυψη, η τροποποίηση ή η μη εξουσιοδοτημένη χρήση των ιδιωτικών κλειδιών τους.

Τηρώντας τις πρακτικές που περιγράφονται στην παρούσα ΔΠΠ, οι συνδρομητές εκπληρώνουν τις υποχρεώσεις που προβλέπονται στις πολιτικές σύμφωνα με τις οποίες χορηγούνται τα πιστοποιητικά τους.

[Με την υπογραφή ενός αιτήματος σχετικού με το πιστοποιητικό (χορήγηση, ανάκληση, ανάκτηση), ο συνδρομητής πιστοποιεί στην ΑΠ CommisSign και στην ΑΚ ότι κάθε στοιχείο το οποίο υποβάλλει στην ΑΠ ή στην ΑΚ είναι πλήρες και ακριβές.]

Οι συνδρομητές μπορούν να χρησιμοποιούν τα ιδιωτικά κλειδιά τους μόνο για τις εργασίες της Ευρωπαϊκής Επιτροπής και μόνο για σκοπούς εγκεκριμένους από την πολιτική ασφάλειας για την ΥΔΚ της Ευρωπαϊκής Επιτροπής και σύμφωνα με την παρούσα ΔΠΠ.

2.1.4. Υποχρεώσεις των συμβαλλομένων μερών

Στον τομέα της ΑΠ CommisSign, οι τελικές οντότητες είναι τόσο συνδρομητές όσο και συμβαλλόμενα μέρη. Ως συμβαλλόμενα μέρη υποχρεούνται:

- να περιορίζουν την εμπιστοσύνη τους στα πιστοποιητικά που χορηγούνται από την ΑΠ CommisSign στις ενδεδειγμένες για τα πιστοποιητικά αυτά χρήσεις, σύμφωνα με την πολιτική για το πιστοποιητικό X.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής και με την παρούσα ΔΠΠ

- να επαληθεύουν τα πιστοποιητικά, ανατρέχοντας και στις *ΚΑΠ [και ΚΑΕ]*, [λαβαίνοντας υπόψη τυχόν κρίσιμες επεκτάσεις]. [(Η επαλήθευση των πιστοποιητικών είναι σύμφωνη με τη διαδικασία επικύρωσης της διαδρομής πιστοποίησης όπως καθορίζεται στη σύσταση της Διεθνούς Ένωσης Τηλεπικοινωνιών–Τομέας τυποποίησης τηλεπικοινωνιών (ITU-T) για την τεχνολογία πληροφορικής X.509 – Διασύνδεση ανοιχτών συστημάτων – Ο κατάλογος: Πλαίσιο επαλήθευσης αυθεντικότητας ISO/IEC 9594-8 (1997)).]

- να εμπιστεύονται και να χρησιμοποιούν τα πιστοποιητικά μόνον εφόσον διαπιστώνεται η ύπαρξη έγκυρης ακολουθίας πιστοποιητικών μεταξύ του συμβαλλόμενου μέρους και του υποκειμένου του πιστοποιητικού.

Πριν χρησιμοποιήσουν το πιστοποιητικό συνδρομητή, τα συμβαλλόμενα μέρη πρέπει να βεβαιώνονται ότι είναι κατάλληλο για τη χρήση για την οποία προορίζεται, αποκτώντας γνώση της πολιτικής και της ΔΠΠ στο πλαίσιο των οποίων έχει χορηγηθεί το εν λόγω πιστοποιητικό.

Τα συμβαλλόμενα μέρη οφείλουν να ελέγχουν την εγκυρότητα της υπογραφής της ΑΠ CommisSign και την ημερομηνία λήξης του πιστοποιητικού πριν χρησιμοποιήσουν το αντίστοιχο δημόσιο κλειδί. Επιπλέον, τα συμβαλλόμενα μέρη οφείλουν να ελέγχουν την εγκυρότητα της ψηφιακής υπογραφής των συνδρομητών πριν αποδεχτούν ψηφιακά υπογεγραμμένα στοιχεία. Όπου η επαλήθευση πραγματοποιείται αυτόματα μέσω κρυπτογραφικής διαδικασίας και υλισμικού/λογισμικού υποστήριξης εγκατεστημένου στο σταθμό εργασίας των συμβαλλομένων μερών, τα

συμβαλλόμενα μέρη πρέπει να βεβαιώνονται ότι χρησιμοποιούν συμβατό λογισμικό.

Πριν από τη χρήση οποιουδήποτε πιστοποιητικού, τα συμβαλλόμενα μέρη οφείλουν να ελέγχουν την κατάστασή του στην τρέχουσα ΚΑΠ. Οφείλουν, επίσης, να επαληθεύουν την ψηφιακή υπογραφή της ΚΑΠ για να βεβαιώνονται ότι φέρει την υπογραφή της ΑΠ CommisSign.

2.1.5. Υποχρεώσεις του φορέα αποθήκευσης

[Τα συμβαλλόμενα μέρη έχουν πρόσβαση στα πιστοποιητικά ρίζας της CommisSign, στη ΔΠΠ, στις ΚΑΠ [και στα πιστοποιητικά των συνδρομητών] σύμφωνα με τις πρακτικές που περιγράφονται στο τμήμα 4.4. «Συχνότητα δημοσίευσης ΚΑΠ» της παρούσας ΔΠΠ.]

2.2. Νομική ευθύνη [προς επανεξέταση από τη νομική υπηρεσία]

[Δεδομένου ότι οι λειτουργίες της ΑΠ CommisSign και της ΑΚ παρέχονται από την Ευρωπαϊκή Επιτροπή, οι νομικές ευθύνες που απορρέουν από τις δύο αυτές λειτουργίες παρατίθενται συνδυαστικά στην παρούσα ΔΠΠ.

Η ΑΠ CommisSign, η ΑΚ και οι ΤΑΚ και η Ευρωπαϊκή Επιτροπή δεν φέρουν ουδεμία απολύτως ευθύνη όσον αφορά τη χρήση των πιστοποιητικών ΥΔΚ της Ευρωπαϊκής Επιτροπής ή των αντίστοιχων ζευγών δημόσιου/ιδιωτικού κλειδιού για οποιαδήποτε χρήση εκτός από τις χρήσεις που περιγράφονται στην πολιτική για το πιστοποιητικό X.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής και στην παρούσα ΔΠΠ.

2.2.1. Εγγυήσεις και περιορισμοί εγγυήσεων

Η ΑΠ CommisSign και η ΑΚ υπόσχονται και εγγυώνται ότι:

- παρέχουν υπηρεσίες πιστοποίησης που συνάδουν με την πολιτική πιστοποιητικών όπως ορίζεται στην πολιτική για το πιστοποιητικό X.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής και στην παρούσα ΔΠΠ

- εκτελούν τις διαδικασίες ταυτοποίησης και επαλήθευσης ταυτότητας όπως περιγράφονται στο τμήμα 3 της παρούσας ΔΠΠ

- παρέχουν υπηρεσίες διαχείρισης κλειδιού, καθώς και χορήγησης, δημοσίευσης, ανάκλησης πιστοποιητικού, ανάκτησης κλειδιού και ενημέρωσης, σύμφωνα με την πολιτική πιστοποιητικών όπως ορίζεται στην πολιτική για το πιστοποιητικό X.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής και την παρούσα ΔΠΠ.

Η Ευρωπαϊκή Επιτροπή και το προσωπικό της δεν κάνουν δηλώσεις, δεν παρέχουν εγγυήσεις ούτε θέτουν όρους, ρητά ή σιωπηρά, εκτός όσων ορίζονται ρητά στην πολιτική για το πιστοποιητικό X.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής και στην παρούσα ΔΠΠ.

2.2.2. Ρήτρες αποποίησης και περιορισμοί ευθύνης

Η Ευρωπαϊκή Επιτροπή, η ΑΠ CommisSign και οι ΑΚ δεν φέρουν ευθύνη για οποιαδήποτε ζημία:

- η οποία επέρχεται σε υπηρεσία ΑΠ ή ΑΚ λόγω πολέμου, θεομηνίας ή ανωτέρας βίας
- η οποία επέρχεται κατά το χρονικό διάστημα που μεσολαβεί από την ανάκληση ενός πιστοποιητικού έως την επόμενη προγραμματισμένη δημοσίευση ΚΑΠ
- η οποία οφείλεται σε μη εξουσιοδοτημένη χρήση πιστοποιητικών που χορηγήθηκαν από την ΑΠ CommisSign ή σε χρήση πιστοποιητικών πέραν της προκαθορισμένης όπως ορίζεται στην πολιτική για το πιστοποιητικό X.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής και στην παρούσα ΔΠΠ
- η οποία προκαλείται από δόλια ή αμελή χρήση πιστοποιητικών και/ή ΚΑΠ [ή ΚΑΕ] που εκδίδονται από την ΑΠ CommisSign
- η οποία οφείλεται στην αποκάλυψη προσωπικών δεδομένων που περιλαμβάνονται στα πιστοποιητικά και στις ΚΑΠ.

Η ΑΠ CommisSign και οι ΑΚ δεν παρέχουν καμία εγγύηση και αποποιούνται κάθε ευθύνη, συμπεριλαμβανομένων των εγγυήσεων εμπορευσιμότητας, καταλληλότητας για συγκεκριμένο σκοπό και ακρίβειας των παρεχόμενων πληροφοριών (πέραν του ότι προέρχονται από εξουσιοδοτημένη πηγή), καθώς επίσης αποποιούνται κάθε νομική ευθύνη για αμέλεια ή μη επίδειξη της δέουσας επιμέλειας εκ μέρους των συνδρομητών και των συμβαλλομένων μερών.

Η Ευρωπαϊκή Επιτροπή, η ΑΠ CommisSign, η ΑΚ και οι ΤΑΚ δεν φέρουν ουδεμία απολύτως ευθύνη για ζημία, βλάβη ή οποιαδήποτε άλλη αξίωση ή υποχρέωση που προκύπτει από αδικοπραξία, σύμβαση ή άλλη αιτία σε σχέση με υπηρεσία που συνδέεται με τη χορήγηση, τη χρήση και την επίδειξη εμπιστοσύνης σε πιστοποιητικό ΥΔΚ της Ευρωπαϊκής Επιτροπής ή στο αντίστοιχο ζεύγος δημόσιου/ιδιωτικού κλειδιού που χρησιμοποιείται από συνδρομητή ή συμβαλλόμενο μέρος.

Οι αιτούντες και τα συμβαλλόμενα μέρη δεν δικαιούνται να εγείρουν αξίωση αποζημίωσης για ζημίες που οφείλονται σε μη δέουσα ή δόλια χρήση της παρούσας ΥΔΚ.

Επιπλέον, η ΑΠ CommisSign και η ΑΚ δεν λειτουργούν ως ενδιάμεσοι στις συναλλαγές μεταξύ συνδρομητών και συμβαλλομένων μερών. Οι αξιώσεις κατά της ΑΠ CommisSign και/ή της ΑΚ περιορίζονται στο να καταδειχτεί ότι η ΑΠ ή η ΑΚ λειτούργησαν με τρόπο ο οποίος δεν συνάδει με την πολιτική για το πιστοποιητικό X.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής και την παρούσα ΔΠΠ.]

2.2.3. Άλλοι όροι και προϋποθέσεις

Δεν προβλέπονται.]

2.3. Οικονομική ευθύνη

2.3.1. Αποζημίωση από συμβαλλόμενα μέρη

Δεν προβλέπεται.

2.3.2. Σχέσεις διαχείρισης

Η χορήγηση πιστοποιητικών από την ΑΠ CommisSign και η βοήθεια την οποία προσφέρει στη χορήγηση αυτή η ΑΚ της Ευρωπαϊκής Επιτροπής δεν καθιστά την Ευρωπαϊκή Επιτροπή ούτε την ΑΠ και την ΑΚ της αντιπρόσωπο, θεματοφύλακα, καταπιστευματοδόχο ή υπό άλλη έννοια εκπρόσωπο των αιτούντων ή των συμβαλλομένων μερών ή άλλων οι οποίοι κάνουν χρήση της ΥΔΚ της Ευρωπαϊκής Επιτροπής.

2.4. Ερμηνεία και εφαρμογή

2.4.1. Ισχύουσα νομοθεσία

Η δυνατότητα επιβολής, η σύνταξη, η ερμηνεία και η ισχύς της παρούσας ΔΠΠ διέπονται από τις ευρωπαϊκές και εθνικές κανονιστικές ρυθμίσεις.

2.4.2. Διακοπή λειτουργίας, συνέχεια, συγχώνευση, ειδοποίηση

Εξαιτίας μεταβολών στο πεδίο δραστηριότητας, στη διαχείριση και/ή στη λειτουργία της ΑΠ CommisSign ενδέχεται να επέλθει διακοπή της λειτουργίας της ή συγχώνευσή της. Στην περίπτωση αυτή, η πολιτική για το πιστοποιητικό Χ.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής και η παρούσα ΔΠΠ ενδέχεται να πρέπει επίσης να τροποποιηθούν. Οι μεταβολές των λειτουργιών θα συνάδουν με τις διοικητικές απαιτήσεις που ορίζονται στο τμήμα 8 της παρούσας ΔΠΠ.

2.4.3. Διαδικασίες επίλυσης διαφορών

Οποιαδήποτε διαφορά μεταξύ Ευρωπαϊκής Επιτροπής και οργανισμού ή ιδιώτη εκτός Ευρωπαϊκής Επιτροπής σχετικά με τη διαχείριση κλειδιών και πιστοποιητικών επιλύεται μέσω κατάλληλου μηχανισμού επίλυσης διαφορών. Εφόσον είναι εφικτό, οι διαφορές επιλύονται με διαπραγμάτευση. Οι διαφορές οι οποίες δεν επιλύονται με διαπραγμάτευση επιλύονται μέσω διαιτησίας από την ΑΑΠ της Ευρωπαϊκής Επιτροπής.

Στο πλαίσιο του τομέα της ΑΠ CommisSign, οι διαφορές μεταξύ χρηστών μελών του προσωπικού της Ευρωπαϊκής Επιτροπής, ο ένας από τους οποίους ενεργεί ως συνδρομητής και ο άλλος ως συμβαλλόμενο μέρος, ή μεταξύ χρηστών μελών του προσωπικού της Ευρωπαϊκής Επιτροπής και της ΑΠ ή της ΑΚ αρχικά παραπέμπονται προς επίλυση στην ΑΛ της ΑΠ CommisSign.

2.5. Συνδρομές

Δεν προβλέπονται.

2.6. Δημοσίευση και φορέας αποθήκευσης

2.6.1. Δημοσίευση πληροφοριών της ΑΠ

Η ΑΠ CommisSign δημοσιεύει τα ακόλουθα:

- *τα πιστοποιητικά ρίζας της CommiSign σε ιστοχώρο*
- *αντίγραφα [της πολιτικής ασφάλειας ΤΕΠ της Ευρωπαϊκής Επιτροπής και] της παρούσας ΔΠΠ σε ιστοχώρο*
- *όλα τα πιστοποιητικά δημόσιου κλειδιού που χορηγούνται από την ΑΠ CommisSign στον κατάλογο της Ευρωπαϊκής Επιτροπής*
- *τις τρέχουσες ΚΑΠ δημόσιου κλειδιού χρηστών που έχουν ανακληθεί από την ΑΠ CommisSign στον κατάλογο της Ευρωπαϊκής Επιτροπής και σε έναν ιστοχώρο*
- *[τις τρέχουσες ΚΑΕ της εξωτερικής αρχής πιστοποίησης που έχουν ανακληθεί από την ΑΑΠ της Ευρωπαϊκής Επιτροπής στον κατάλογο της Ευρωπαϊκής Επιτροπής].*

2.6.2. Συχνότητα δημοσίευσης

Μετά την ενεργοποίησή τους, τα πιστοποιητικά που χορηγούνται από την ΑΠ CommisSign δημοσιεύονται άπαξ ημερησίως στον κατάλογο της Ευρωπαϊκής Επιτροπής. Σε περίπτωση ανάκλησής τους, εγγράφονται στις ΚΑΠ, οι οποίες δημοσιεύονται σύμφωνα με τις διατάξεις του τμήματος 4.4. «Συχνότητα δημοσίευσης ΚΑΠ» της παρούσας ΔΠΠ. [Σε περίπτωση ανάκλησης αμοιβαίων πιστοποιητικών, αυτά εγγράφονται στις ΚΑΕ, οι οποίες δημοσιεύονται σύμφωνα με τις διατάξεις του τμήματος 4.4. «Συχνότητα δημοσίευσης ΚΑΠ» της παρούσας ΔΠΠ.]

2.6.3. Έλεγχοι πρόσβασης

Η ΔΠΠ της ΑΠ CommisSign και η πολιτική πιστοποιητικών της Ευρωπαϊκής Επιτροπής διατίθενται μέσω του ιστοχώρου και παραχωρείται πρόσβαση μόνο για ανάγνωση. Δικαίωμα πρόσβασης για εγγραφή ή τροποποίηση των εν λόγω εγγράφων διαθέτει μόνο το προσωπικό της ΑΠ.

[Τα πιστοποιητικά και οι ΚΑΠ διατίθενται μέσω του καταλόγου της Ευρωπαϊκής Επιτροπής και παραχωρείται πρόσβαση μόνο για ανάγνωση. Προνόμια ανάγνωσης/εγγραφής και διαγραφής έχει μόνον η ΑΠ CommisSign.]

2.6.4. Φορείς αποθήκευσης

Ο φορέας αποθήκευσης πιστοποιητικών, ΚΑΠ [και ΚΑΕ] που εκδίδονται από την ΑΠ CommisSign παρέχεται από το σύστημα καταλόγου της Ευρωπαϊκής Επιτροπής. [Για απόκτηση πρόσβασης στον κατάλογο χρησιμοποιείται το πρωτόκολλο Lightweight Directory Access Protocol (LDAP) έκδοση 2, όπως ορίζεται στην αίτηση για σχολιασμό (RFC) 1777 Lightweight Directory Access Protocol (1995). Το LDAP έκδοση 2 χρησιμοποιείται επάνω από το πρωτόκολλο TCP, όπως ορίζεται στο τμήμα 3.1 της RFC 1777.]

[Όταν διαβιβάζονται με το LDAP αιτήματα και αποτελέσματα, τα χαρακτηριστικά που καθορίζονται στο πιστοποιητικό X.500 κωδικοποιούνται μέσω στοιχειοσειρών όπως ορίζεται στην RFC 1778 «String Representation of Standard Attribute Syntaxes» (1995). Αυτές οι κωδικοποιήσεις μέσω στοιχειοσειρών έχουν βασιστεί στους ορισμούς χαρακτηριστικών που περιλαμβάνονται στο πιστοποιητικό X.500 (1988). Επομένως, οι στοιχειοσειρές που ακολουθούν αφορούν πιστοποιητικά έκδοσης 1 και ΚΑΠ έκδοσης 1:

- userCertificate (RFC 1778 τμήμα 2.25)
- CACertificate (RFC 1778 τμήμα 2.26)
- authorityRevocationList, (RFC 1778 τμήμα 2.27)
- certificateRevocationList, (RFC 1778 τμήμα 2.28)
- crossCertificatePair, (RFC 1778 τμήμα 2.29)

Δεδομένου ότι η παρούσα ΔΠΠ χρησιμοποιεί πιστοποιητικά έκδοσης 3 και ΚΑΠ έκδοσης 2, όπως ορίζεται στο X.509, η κωδικοποίηση αυτών των χαρακτηριστικών μέσω στοιχειοσειρών σύμφωνα με την RFC 1778 είναι ακατάλληλη. Για το λόγο αυτό, τα εν λόγω χαρακτηριστικά κωδικοποιούνται μέσω σύνταξης παρόμοιας με τη σύνταξη Undefined όπως προβλέπεται στο τμήμα 2.1 της RFC 1778. Οι τιμές των χαρακτηριστικών αυτών, δηλαδή, κωδικοποιούνται σαν να ήταν τιμές του τύπου OCTET STRING, ενώ η τιμή στοιχειοσειράς της κωδικοποίησης είναι η κωδικοποίηση DER της ίδιας της τιμής.]

Ο φορέας αποθήκευσης της παρούσας ΔΠΠ και της πολιτικής πιστοποιητικών της Ευρωπαϊκής Επιτροπής είναι ένας ιστοχώρος με πρόσβαση μέσω[να προσδιοριστεί ο URL]

2.7. Έλεγχος συμμόρφωσης [προς υλοποίηση] [προς επανεξέταση μετά την υλοποίηση]

2.7.1. Συχνότητα διενέργειας ελέγχου συμμόρφωσης

Πλήρης και επίσημος έλεγχος της λειτουργίας της ΑΠ CommisSign διενεργείται ετησίως.

Η ΑΑΠ μπορεί κατά την κρίση της να παραγγείλει τη διενέργεια ελέγχου συμμόρφωσης από ελεγκτή ανά πάσα στιγμή.

Η ΑΠ CommisSign διατηρεί το δικαίωμα να απαιτεί περιοδικές επιθεωρήσεις και ελέγχους οποιασδήποτε μονάδας ΑΚ στο πλαίσιο του τομέα της ΑΠ CommisSign, προκειμένου να επιβεβαιώνει ότι η ΑΚ λειτουργεί σύμφωνα με τις πρακτικές και τις διαδικασίες ασφάλειας που περιγράφονται στην παρούσα ΔΠΠ.

2.7.2. Ταυτότητα/προσόντα ελεγκτών ΑΠ

Οποιοδήποτε φυσικό πρόσωπο ή οντότητα πρόκειται να διενεργήσει έλεγχο συμμόρφωσης πρέπει να έχει την έγκριση της ΑΑΠ. Ο ελεγκτής πρέπει να έχει ως κύρια δραστηριότητα τη διενέργεια ελέγχων ΑΠ ή ελέγχων ασφάλειας συστημάτων πληροφορικής, να διαθέτει σημαντική πείρα σχετικά με την ΥΔΚ και τις κρυπτογραφικές τεχνολογίες, καθώς και με τη λειτουργία των λογισμικών ΥΔΚ, και να είναι εξοικειωμένος με τις πολιτικές και με τις κανονιστικές ρυθμίσεις της Ευρωπαϊκής Επιτροπής.

2.7.3. Σχέση ελεγκτή και ελεγχόμενης ΑΠ

Ο ελεγκτής που εγκρίνεται από την ΑΑΠ και η ΑΠ CommisSign είναι διαφορετικές οντότητες στο πλαίσιο της οργανωτικής δομής της Ευρωπαϊκής Επιτροπής.

2.7.4. Θέματα που καλύπτονται από τον έλεγχο

Αντικείμενο του ελέγχου συμμόρφωσης είναι η εφαρμογή από την ΑΠ CommisSign και από την ΑΚ των τεχνικών και διαδικαστικών πρακτικών, καθώς και των πρακτικών που αφορούν το προσωπικό, οι οποίες περιγράφονται στην παρούσα ΔΠΠ. Ορισμένα από τα πεδία εστίασης του ελέγχου είναι:

- ταυτοποίηση και επαλήθευση ταυτότητας
- επιχειρησιακές λειτουργίες/υπηρεσίες
- υλικοί και διαδικαστικοί έλεγχοι ασφάλειας και έλεγχος ασφάλειας του προσωπικού
- τεχνικοί έλεγχοι ασφάλειας.

2.7.5. Μέτρα που λαμβάνονται ως αποτέλεσμα του ελέγχου

Τρία είδη μέτρων μπορούν να ληφθούν εφόσον διαπιστωθεί αδυναμία:

(1) συνέχιση της λειτουργίας ως συνήθως

(2) συνέχιση της λειτουργίας, αλλά σε χαμηλότερο επίπεδο ασφάλειας

(3) αναστολή της λειτουργίας.

Εφόσον διαπιστωθεί αδυναμία, ο ελεγκτής, σε συνεννόηση με την ΑΑΠ της Ευρωπαϊκής Επιτροπής, αποφασίζει ποιο από τα τρία μέτρα θα ληφθεί

ανάλογα με τη σοβαρότητα των παρατυπιών, τους κινδύνους που δημιουργούνται και τη διατάραξη που προκαλείται στους χρήστες των πιστοποιητικών.

Εάν επιλεγεί το πρώτο ή το δεύτερο μέτρο, η ΑΠ της Ευρωπαϊκής Επιτροπής και η ΑΛ οφείλουν να διασφαλίσουν ότι τα διορθωτικά αυτά μέτρα θα εφαρμοστούν εντός 30 ημερών. Μετά την πάροδο των 30 ημερών, ή νωρίτερα εάν εγκριθεί από την ΑΑΠ και τον ελεγκτή, η ομάδα ελέγχου διενεργεί επαναξιολόγηση. Εάν, κατά την επαναξιολόγηση, δεν έχουν ληφθεί διορθωτικά μέτρα, ο ελεγκτής αποφασίζει κατά πόσον απαιτείται η λήψη αυστηρότερων μέτρων (π.χ. αναστολή της λειτουργίας).

Εάν επιλεγεί το τρίτο μέτρο, όλα τα πιστοποιητικά τα οποία έχουν χορηγηθεί από την ΑΠ CommisSign, συμπεριλαμβανομένων των πιστοποιητικών τελικών οντοτήτων και των αμοιβαίων πιστοποιητικών της ΑΠ, ανακαλούνται πριν την αναστολή της υπηρεσίας.

Η ΑΑΠ της Ευρωπαϊκής Επιτροπής και η ΑΛ της ΑΠ της Ευρωπαϊκής Επιτροπής είναι αρμόδιες για την υποβολή εκθέσεων στον ελεγκτή σχετικά με την πρόοδο των διορθωτικών μέτρων, σε εβδομαδιαία βάση. Η ΑΑΠ και ο ελεγκτής αποφασίζουν από κοινού το χρόνο διενέργειας της επαναξιολόγησης. Εάν κατά την επαναξιολόγηση θεωρηθεί ότι οι αδυναμίες έχουν διορθωθεί, η λειτουργία της ΑΠ CommisSign επαναλαμβάνεται και χορηγούνται νέα πιστοποιητικά στις τελικές οντότητες και στις άλλες εξωτερικές ΑΠ, σύμφωνα με τους όρους που προβλέπονται στις διάφορες συμφωνίες αμοιβαίας πιστοποίησης.]

2.7.6. Κοινοποίηση των αποτελεσμάτων

Τα αποτελέσματα του ετήσιου ελέγχου υποβάλλονται στην ΑΑΠ της Ευρωπαϊκής Επιτροπής, στην ΑΠ CommisSign και στο διαχειριστή ασφάλειας πληροφορικής κάθε ΤΑΚ της Ευρωπαϊκής Επιτροπής. Σε περίπτωση λήψης του δεύτερου μέτρου, η ΑΑΠ της Ευρωπαϊκής Επιτροπής, συνεπικουρούμενη από τον ελεγκτή, αποφασίζει κατά πόσον πρέπει να ενημερωθούν οι συνδρομητές για τη λήψη του μέτρου. Σε περίπτωση λήψης του τρίτου μέτρου, η ΑΑΠ της Ευρωπαϊκής Επιτροπής διασφαλίζει ότι όλοι οι χρήστες έχουν ενημερωθεί σχετικά. Η κοινοποίηση με σκοπό την ενημέρωση των συνδρομητών σχετικά με τις αδυναμίες και τα μέτρα αντιμετώπισής τους πραγματοποιείται μέσω ηλεκτρονικού ταχυδρομείου, εφόσον αυτό είναι εφικτό. Εάν ο συνδρομητής δεν διαθέτει ηλεκτρονικό ταχυδρομείο, παραδίδεται υπόμνημα μέσω της υπηρεσίας ταχυδρομείου της Ευρωπαϊκής Επιτροπής.

Η μέθοδος και οι λεπτομέρειες της γνωστοποίησης των αποτελεσμάτων του ελέγχου στις ΑΠ οι οποίες έχουν πιστοποιηθεί αμοιβαία με την ΑΠ CommisSign ορίζονται στο πλαίσιο της συμφωνίας αμοιβαίας πιστοποίησης μεταξύ των δύο μερών. Εφόσον δεν υπάρχει πρόβλεψη περί του αντιθέτου σε κάποια συγκεκριμένη συμφωνία αμοιβαίας πιστοποίησης, τα αποτελέσματα του ελέγχου δεν κοινοποιούνται εκτός Ευρωπαϊκής Επιτροπής.

2.8. Πολιτική εμπιστευτικότητας

Όλα τα στοιχεία τα οποία δεν θεωρούνται δημόσιας χρήσης από την ΑΠ της Ευρωπαϊκής Επιτροπής παραμένουν εμπιστευτικά.

2.8.1. Κατηγορίες στοιχείων που δεν αποκαλύπτονται

Το ιδιωτικό κλειδί υπογραφής κάθε συνδρομητή διαβαθμίζεται ως περιορισμένης χρήσης από τον εν λόγω συνδρομητή. Η ΑΠ CommisSign και η κεντρική ΑΚ δεν έχουν πρόσβαση στα κλειδιά αυτά.

Το ιδιωτικό κλειδί εμπιστευτικότητας κάθε συνδρομητή διαβαθμίζεται ως περιορισμένης χρήσης από τον εν λόγω συνδρομητή.

Προσωρινά, είναι διαθέσιμο μόνο ένα ζεύγος δημόσιου/ιδιωτικού κλειδιού και συνδέεται με το «ιδιωτικό κλειδί εμπιστευτικότητας». Δεν έχει εφαρμογή οποιαδήποτε πρόβλεψη αφορά το κλειδί υπογραφής. Ωστόσο, αντίγραφα ασφαλείας των ιδιωτικών κλειδιών εμπιστευτικότητας κρατούνται από την ΤΑΚ και προστατεύονται σύμφωνα με τις προβλέψεις του τμήματος 6 της παρούσας ΔΠΠ.

Στοιχεία τα οποία συλλέγονται κατά τις ανιχνεύσεις ελέγχου θεωρούνται περιορισμένης χρήσης από την Ευρωπαϊκή Επιτροπή και δεν επιτρέπεται να κοινοποιηθούν εκτός του θεσμικού οργάνου, παρά μόνον εφόσον αυτό επιβάλλεται από τη νομοθεσία ή από σχετικές κανονιστικές ρυθμίσεις.

Η συλλογή προσωπικών δεδομένων ενδέχεται να υπόκειται στις απαιτήσεις περί συλλογής, διατήρησης, φύλαξης και προστασίας του κανονισμού 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Δεκεμβρίου 2000. Τα προσωπικά δεδομένα τα οποία αποθηκεύονται τοπικά από την ΑΠ CommisSign και την ΑΚ πρέπει να θεωρούνται περιορισμένης χρήσης και να επιτρέπεται η πρόσβαση σε αυτά μόνο σε όσους οφείλουν λόγω θέσης να τα γνωρίζουν για να εκτελέσουν τα καθήκοντά τους.

Προσωπικά και εταιρικά δεδομένα τα οποία συλλέγονται από την ΑΑΠ της Ευρωπαϊκής Επιτροπής, την ΑΠ και την ΑΚ, εκτός των όσων δημοσιεύονται ρητά ως τμήμα του πιστοποιητικού, της ΚΑΠ [ή της ΚΑΕ,] θεωρούνται περιορισμένης χρήσης και δεν δημοσιοποιούνται παρά μόνον εφόσον αυτό επιβάλλεται από τη νομοθεσία ή από σχετικές κανονιστικές ρυθμίσεις.

Γενικά, τα αποτελέσματα των ετήσιων ελέγχων φυλάσσονται ως πληροφορίες περιορισμένης χρήσης, με εξαίρεση τις περιπτώσεις που αναφέρονται στο τμήμα 2.7 «Κοινοποίηση των αποτελεσμάτων» της παρούσας ΔΠΠ.

Γενικά, δεν προβλέπεται πρόσβαση του κοινού στα μητρώα ελέγχου.

Κλειδιά τα οποία βρίσκονται στην κατοχή της ΑΠ CommisSign θεωρούνται περιορισμένης χρήσης και γνωστοποιούνται μόνο σε εξουσιοδοτημένες οργανωτικές αρχές της Ευρωπαϊκής Επιτροπής, σύμφωνα με την παρούσα ΔΠΠ και την πολιτική ασφάλειας για την ΥΔΚ της Ευρωπαϊκής Επιτροπής ή σε όργανα δημόσιας τάξης, σύμφωνα με τις κανονιστικές ρυθμίσεις της

Ευρωπαϊκής Επιτροπής, την ευρωπαϊκή νομοθεσία, τη νομοθεσία των κρατών μελών και την παρούσα ΔΠΠ.

2.8.2. Κατηγορίες στοιχείων που θεωρούνται δημόσιας χρήσης

Τα στοιχεία που περιλαμβάνονται στα δημόσια πιστοποιητικά, στις ΚΑΠ [και στις ΚΑΕ] που εκδίδονται από την ΑΠ CommisSign θεωρούνται δημόσιας χρήσης.

Οι πληροφορίες που περιλαμβάνονται στην πολιτική πιστοποιητικών της ΥΔΚ της Ευρωπαϊκής Επιτροπής και στην παρούσα ΔΠΠ θεωρούνται δημόσιας χρήσης.

2.8.3. Αποκάλυψη στοιχείων σχετικά με την ανάκληση πιστοποιητικού

Σε περίπτωση ανάκλησης πιστοποιητικού από την ΑΠ CommisSign, στην καταχώριση στην ΚΑΠ περιλαμβάνεται και ένας κωδικός για την αιτία λήψης του μέτρου αυτού. Αυτός ο κωδικός θεωρείται δημόσιας χρήσης και μπορεί να κοινοποιηθεί σε όλους τους άλλους συνδρομητές και τα συμβαλλόμενα μέρη. Ωστόσο, δεν αποκαλύπτονται άλλες λεπτομέρειες σχετικά με την ανάκληση.

2.8.4. Γνωστοποίηση σε όργανα δημόσιας τάξης

Η ΑΠ CommisSign και οι ΑΚ δεν αποκαλύπτουν σε τρίτους πληροφορίες που περιλαμβάνονται στα πιστοποιητικά ή που συνδέονται με αυτά, εκτός εάν:

- δίνεται εξουσιοδότηση από την πολιτική ασφάλειας για την ΥΔΚ της Ευρωπαϊκής Επιτροπής και την παρούσα ΔΠΠ
- η αποκάλυψή τους επιβάλλεται από τη νομοθεσία, την Ευρωπαϊκή Επιτροπή, ευρωπαϊκές ή εθνικές κανονιστικές ρυθμίσεις ή με δικαστική εντολή
- δίνεται εξουσιοδότηση από το συνδρομητή γιατί κρίνεται απαραίτητο για την ορθή χρήση του πιστοποιητικού.

Τα αιτήματα για την αποκάλυψη πληροφοριών πρέπει να υπογράφονται και να διαβιβάζονται στην τοπική ΑΚ της Ευρωπαϊκής Επιτροπής ή στην ΑΠ CommisSign.

2.8.5. Άλλες περιπτώσεις κοινοποίησης στοιχείων

Δεν προβλέπονται.

2.9. Δικαιώματα πνευματικής ιδιοκτησίας

Τα πιστοποιητικά, οι *ΚΑΠ* [και οι ΚΑΕ] που εκδίδονται από την ΑΠ CommisSign, η πολιτική πιστοποιητικών της ΥΔΚ της Ευρωπαϊκής Επιτροπής και η παρούσα ΔΠΠ αποτελούν ιδιοκτησία της Ευρωπαϊκής Επιτροπής.

3. ΤΑΥΤΟΠΟΙΗΣΗ ΚΑΙ ΕΠΑΛΗΘΕΥΣΗ ΤΑΥΤΟΤΗΤΑΣ

3.1. Αρχική καταχώριση

3.1.1. Κατηγορίες ονομάτων

Η ΑΚ αντλεί τα παρακάτω στοιχεία από το σύστημα καταλόγου της Ευρωπαϊκής Επιτροπής:

- επώνυμο συνδρομητή (LASTNAME)
- όνομα συνδρομητή (FIRSTNAME)
- CUID συνδρομητή (μοναδικό και εναρμονισμένο εσωτερικό αναγνωριστικό ταυτότητας)
- διεύθυνση ηλεκτρονικού ταχυδρομείου του συνδρομητή στον εξυπηρετητή της Ευρωπαϊκής Επιτροπής (SMTP)

Η ΑΚ θεωρεί ότι:

- το αναγνωριστικό CUID του συνδρομητή και η διεύθυνση SMTP είναι μοναδικά για το συνδρομητή ο οποίος ανήκει στο προσωπικό της Ευρωπαϊκής Επιτροπής
- μεταξύ του CUID και της διεύθυνσης SMTP του συνδρομητή υπάρχει μονοσήμαντη σχέση
- Η ΑΚ δημιουργεί το SubjectName του πιστοποιητικού σύμφωνα με τον ακόλουθο μορφότυπο:/CN=LASTNAME FIRSTNAME (CUID) /E=SMTP.

Η ΑΚ καταχωρεί το SubjectName του συνδρομητή στη βάση δεδομένων της ΑΠ.

3.1.2. Ονόματα με νόημα

Εφόσον ο συνδρομητής είναι ιδιώτης, το όνομα που ορίζεται στο χαρακτηριστικό Common Name είναι το όνομα του συνδρομητή.

Εφόσον ο συνδρομητής είναι οργανισμός, το όνομα που ορίζεται στο χαρακτηριστικό Common Name είναι το όνομα της λειτουργικής ταχυδρομικής θυρίδας.

3.1.3. Κανόνες για την ερμηνεία των διαφόρων μορφών ονομάτων

Δεν προβλέπονται.

3.1.4. Μοναδικότητα ονομάτων

Τα SubjectName των πιστοποιητικών είναι μοναδικά για όλες τις τελικές οντότητες στο πλαίσιο του τομέα της ΑΠ CommisSign. Η διαχείριση χρηστών της Ευρωπαϊκής Επιτροπής έχει την ευθύνη να διασφαλίζει τη μοναδικότητα του CUID και της διεύθυνσης SMTP.

3.1.5. Διαδικασία επίλυσης διαφορών σχετικά με τη διεκδίκηση ονόματος

Οι διαφορές επιλύονται κατά την κρίση της διαχείρισης χρηστών της Ευρωπαϊκής Επιτροπής.

3.1.6. Αναγνώριση, έλεγχος γνησιότητας και ρόλος εμπορικών σημάτων

Δεν προβλέπεται.

3.1.7. Μέθοδος για την απόδειξη κατοχής ιδιωτικού κλειδιού

Η απόδειξη κατοχής ιδιωτικού κλειδιού ελέγχεται αυτόματα μέσα από τις λειτουργίες ενός πρωτοκόλλου ασφαλούς επικοινωνίας.

3.1.8. Επαλήθευση της ταυτότητας οργανισμού

Τα πιστοποιητικά δημόσιου κλειδιού χορηγούνται σε ιδιώτες, εφόσον αυτό είναι δυνατό. Στις περιπτώσεις στις οποίες περισσότεροι του ενός ιδιώτες ενεργούν υπό μία και την αυτή ιδιότητα, χορηγείται ένα μόνο πιστοποιητικό κρυπτογράφησης, το οποίο περιλαμβάνει το όνομα μιας λειτουργικής ταχυδρομικής θυρίδας. Σε λειτουργικές ταχυδρομικές θυρίδες δεν χορηγείται πιστοποιητικό υπογραφής.

Τα άτομα τα οποία ενεργούν εξ ονόματος της λειτουργικής ταχυδρομικής θυρίδας χρησιμοποιούν το δικό τους προσωπικό πιστοποιητικό υπογραφής.

Η λειτουργική ταχυδρομική θυρίδα ενός οργανισμού πρέπει να έχει δημιουργηθεί από άτομο εξουσιοδοτημένο να ενεργεί εξ ονόματος του υποψήφιου συνδρομητή. Το εν λόγω εξουσιοδοτημένο άτομο έχει την ευθύνη εντός του οργανισμού για τη διασφάλιση του ελέγχου των πιστοποιητικών και των αντίστοιχων ιδιωτικών κλειδιών και είναι υπόλογο για κάθε χρήστη ο οποίος έχει τον έλεγχο των κλειδιών σε μια δεδομένη στιγμή.

Η ταυτοποίηση και η επαλήθευση της ταυτότητας του υποψήφιου συνδρομητή γίνεται ως εξής:

- η ΑΚ επαληθεύει την ταυτότητα και την εξουσιοδότηση του ατόμου που ενεργεί εξ ονόματος του υποψήφιου συνδρομητή και την εξουσιοδότησή του να παραλάβει τα κλειδιά εξ ονόματος του εν λόγω οργανισμού.

- Η ΑΚ ή η ΑΠ καταγράφει το είδος αποδεικτικού ταυτότητας και τα στοιχεία που χρησιμοποιήθηκαν και φυλάσσει το όνομα του υπεύθυνου για την ταχυδρομική θυρίδα στην οποία χορηγείται το πιστοποιητικό οργανισμού.

Οι διαδικασίες χορήγησης ενός πιστοποιητικού οργανισμού δεν συγκρούονται με άλλες διατάξεις της παρούσας ΔΠΠ (π.χ. δημιουργία κλειδιού, προστασία ιδιωτικού κλειδιού και υποχρεώσεις των χρηστών).

[Στην περίπτωση χορήγησης αμοιβαίων πιστοποιητικών σε άλλες ΑΠ, η ΑΠ CommisSign χορηγεί τα εν λόγω πιστοποιητικά σε άλλες ΑΠ με την έγκριση της ΑΑΠ της Ευρωπαϊκής Επιτροπής. Η ΑΑΠ της Ευρωπαϊκής Επιτροπής

εξετάζει τις πολιτικές και τις διαδικασίες των άλλων ΑΠ πριν εγκρίνει την αμοιβαία πιστοποίηση και, αντίστροφα, η ΔΠΠ της ΑΠ CommisSign και η πολιτική για το πιστοποιητικό X.509 της ΥΔΚ της Ευρωπαϊκής Επιτροπής είναι στη διάθεση των άλλων ΑΠ για εξέταση.]

3.1.9. Επαλήθευση της ταυτότητας φυσικού προσώπου

Η αίτηση συνδρομής φυσικού προσώπου πρέπει να υποβληθεί από το ίδιο το φυσικό πρόσωπο ή από τον προϊστάμενό του εξ ονόματός του. Στη δεύτερη περίπτωση, ο συνδρομητής πρέπει να ενημερώνεται. Εκτός της ταυτοποίησης και της επαλήθευσης ταυτότητας που περιγράφονται κατωτέρω, ο υποψήφιος συνδρομητής πρέπει να παρουσιαστεί αυτοπροσώπως στην ΤΑΚ του για επαλήθευση ταυτότητας πριν τη χορήγηση του πιστοποιητικού.

Η επιβεβαίωση της εργασιακής σχέσης είναι ευθύνη της ΑΚ. Η επιβεβαίωση της ταυτότητας του συνδρομητή που υποβάλλει αίτηση πιστοποιητικού είναι ευθύνη της ΤΑΚ. Στα τμήματα που ακολουθούν περιγράφονται οι ενέργειες που συνιστούν τη διαδικασία επαλήθευσης.

3.1.10. Επαλήθευση της εργασιακής σχέσης του συνδρομητή:

Πριν τη χορήγηση πιστοποιητικού στο συνδρομητή, πρέπει να παρέχεται στην ΑΚ επιβεβαίωση της εργασιακής σχέσης του συνδρομητή με την Ευρωπαϊκή Επιτροπή. Η εργασιακή σχέση του συνδρομητή αποδεικνύεται μέσω του καταλόγου της Ευρωπαϊκής Επιτροπής. Η παρουσία του συνδρομητή στον κατάλογο της Ευρωπαϊκής Επιτροπής ελέγχεται μέσω διοικητικής διαδικασίας.

3.1.11. Επαλήθευση της ταυτότητας του συνδρομητή:

Η ΤΑΚ προβαίνει σε επαλήθευση της ταυτότητας είτε κατά την υποβολή του αιτήματος σχετικά με το πιστοποιητικό είτε πριν την υποβολή του αιτήματος, χρησιμοποιώντας τα αρχεία και τα έγγραφα της ΑΚ.

Η επιβεβαίωση της ταυτότητας του συνδρομητή πρέπει να επαληθεύεται από την ΤΑΚ μέσω της υπηρεσιακής κάρτας του.

3.1.12. Επαλήθευση των συσκευών ή των εφαρμογών

Δεν προβλέπεται.

3.2. Τακτική ανανέωση κλειδιού

Η ανανέωση του κλειδιού ενός πιστοποιητικού συνεπάγεται ότι δημιουργείται ένα νέο πιστοποιητικό με:

- το ίδιο SubjectName,
- νέο αύξοντα αριθμό,
- νέο δημόσιο κλειδί,
- πιθανώς με διαφορετική διάρκεια ισχύος.

Η διαδικασία της τακτικής ανανέωσης κλειδιού εφαρμόζεται όταν λήγει η ισχύς του πιστοποιητικού ενός χρήστη. Η διαδικασία είναι ίδια με τη διαδικασία της αρχικής καταχώρισης.

3.3. Ανανέωση κλειδιού μετά από ανάκληση

Για τους συνδρομητές των οποίων τα πιστοποιητικά έχουν ανακληθεί ακολουθείται η διαδικασία της τακτικής ανανέωσης κλειδιού.

3.4. Αίτημα για ανάκληση

Η διαδικασία ανάκλησης περιγράφεται στο τμήμα 4.4 «Αναστολή ισχύος και ανάκληση πιστοποιητικού» της παρούσας ΔΠΠ.

4. ΛΕΙΤΟΥΡΓΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

4.1. Αίτημα χορήγησης πιστοποιητικού

Πριν τη χορήγηση του πιστοποιητικού, ο συνδρομητής πρέπει να υποβάλλει αίτημα, στο οποίο να περιλαμβάνονται οι εξής πληροφορίες:

- το πλήρες όνομα του συνδρομητή
- η εργασιακή σχέση του συνδρομητή με την Ευρωπαϊκή Επιτροπή
- στοιχεία τα οποία να αποδεικνύουν την εργασιακή σχέση του συνδρομητή με την Ευρωπαϊκή Επιτροπή
- η διεύθυνση SMTP ηλεκτρονικού ταχυδρομείου του συνδρομητή στον εξυπηρετητή της Ευρωπαϊκής Επιτροπής
- το κοινό αναγνωριστικό χρήστη του συνδρομητή (CUID)
- αποδοχή των όρων που προβλέπονται στην παρούσα ΔΠΠ.

Ανάλογα με τη διαδικασία επαλήθευσης της ταυτότητας που ακολουθεί η ΑΚ, μπορεί να επιλέξει να συμπεριλάβει πρόσθετες πληροφορίες στο αίτημα χορήγησης πιστοποιητικού, προκειμένου να διευκολυνθεί η επαλήθευση της ταυτότητας.

Το αίτημα για το πιστοποιητικό υπογράφεται από το συνδρομητή (εφόσον πρόκειται για αίτημα από ιδιώτη) και από την ΤΑΚ (μέσω υπογεγραμμένου ηλεκτρονικού ταχυδρομείου). Η ΤΑΚ διαβιβάζει το εν λόγω αίτημα στην ΑΚ.

Με βάση τις πληροφορίες τις οποίες παρέχει ο αιτών, η ΑΚ και η ΤΑΚ προβαίνουν σε επαλήθευση της ταυτότητας σύμφωνα με τους όρους που αναφέρονται στο τμήμα 3.1 «Επαλήθευση της ταυτότητας οργανισμού» και «Επαλήθευση της ταυτότητας φυσικού προσώπου». Ανάλογα με το αποτέλεσμα της επαλήθευσης, η ΑΚ εγκρίνει ή απορρίπτει το αίτημα για πιστοποιητικό. Η ΑΚ κοινοποιεί στο συνδρομητή την έγκριση ή την απόρριψη του αιτήματός του. Η ΑΚ σημειώνει τις ενέργειες που πραγματοποιήθηκαν σχετικά με το αίτημα και με την επαλήθευση της

ταυτότητας του αιτούντος και στη συνέχεια υπογράφει και χρονολογεί το αίτημα. Η ΑΚ φυλάσσει το αίτημα πιστοποιητικού.

4.2. Χορήγηση πιστοποιητικού

Η διαδικασία που περιγράφεται παρακάτω είναι η **στερεότυπη διαδικασία**:

(1) Ο συνδρομητής στέλνει αίτημα για πιστοποιητικό στην ΤΑΚ της ΓΔ του (ρητό αίτημα) ή η ΤΑΚ λαμβάνει τον κατάλογο των υποψήφιων συνδρομητών από τους προϊσταμένους τους (σιωπηρό αίτημα).

(2) Η ΤΑΚ διαβιβάζει το αίτημα στην ΑΚ μέσω υπογεγραμμένου ηλεκτρονικού ταχυδρομείου.

(3) Η ΤΑΚ ενημερώνει τους υποψήφιους συνδρομητές και τους ειδοποιεί ότι θα λάβουν έναν κωδικό αναγνώρισης από την ΑΚ και ένα δεύτερο κωδικό αναγνώρισης από την ίδια.

(4) Η ΑΚ διενεργεί διοικητικό έλεγχο σχετικά με το συνδρομητή και εισάγει το SubjectName στη βάση δεδομένων της ΑΠ.

(5) Η ΑΠ στέλνει στην ΑΚ με ασφαλή τρόπο ένα αρχείο εγγραφής στο οποίο περιέχεται το SubjectName του συνδρομητή και ένας κωδικός αναγνώρισης Κ1.

(6) Η ΑΚ στέλνει με ασφαλές ηλεκτρονικό ταχυδρομείο το αρχείο εγγραφής στην ΤΑΚ που υπέβαλε το αίτημα για πιστοποιητικό.

(7) Η ΑΚ στέλνει με εμπιστευτικό ταχυδρομείο στο συνδρομητή έγγραφο (σε χαρτί) στο οποίο αναγράφεται ο κωδικός αναγνώρισής του Κ1.

(8) Η ΤΑΚ, μετά την παραλαβή του αρχείου εγγραφής από την ΑΚ, ελέγχει κατά πόσον ο συνδρομητής είναι υπαρκτό πρόσωπο.

(9) Η ΤΑΚ απευθύνεται στην ΑΠ για να επιβεβαιώσει την ύπαρξη του συνδρομητή.

(10) Η ΑΠ ενημερώνει το αρχείο εγγραφής και στέλνει στην ΤΑΚ ένα δεύτερο κωδικό αναγνώρισης Κ2.

(11) Η ΤΑΚ στέλνει στο συνδρομητή το αρχείο εγγραφής (με δισκέτα ή ηλεκτρονικό ταχυδρομείο) και ένα έγγραφο (σε χαρτί) στο οποίο περιλαμβάνεται ο κωδικός αναγνώρισης Κ2.

(12) Η ΤΑΚ βοηθά τους εγγεγραμμένους συνδρομητές που έχουν πλέον στην κατοχή τους το αρχείο εγγραφής και τους δύο κωδικούς Κ1 και Κ2, να δημιουργήσουν τα κλειδιά τους και να αποκτήσουν πιστοποιητικό από την ΑΠ. Ο εγγεγραμμένος συνδρομητής οφείλει να είναι παρών κατά τη δημιουργία των κλειδιών, ώστε να εισαγάγει τους κωδικούς αναγνώρισης της ΑΚ και της ΤΑΚ και έναν αρχικό κωδικό πρόσβασης για το ιδιωτικό κλειδί.

(13) Ο εγγεγραμμένος συνδρομητής αποθηκεύει το ιδιωτικό κλειδί του στο σκληρό δίσκο, σε δισκέτα [ή σε έξυπνη κάρτα], ανάλογα με την πρακτική που εφαρμόζει η εκάστοτε ΓΔ.

Δημοσίευση πιστοποίησης: ημερησίως

(1) Τα στελέχη της ΑΠ δημιουργούν ένα αρχείο το οποίο περιλαμβάνει όλα τα πιστοποιητικά και το παραδίδουν στο διαχειριστή του καταλόγου της Ευρωπαϊκής Επιτροπής στις 21.15.

(2) Ο διαχειριστής του καταλόγου της Ευρωπαϊκής Επιτροπής ενημερώνει τον κατάλογο της Ευρωπαϊκής Επιτροπής με τα πιστοποιητικά στις 22.00.

Η διαδικασία που περιγράφεται παρακάτω είναι μια **τροποποιημένη και προσωρινή** διαδικασία που προσφέρει τη δυνατότητα «ανάκτησης κλειδιού» σε επίπεδο ΓΔ. Η διαδικασία αυτή θα εγκαταλειφθεί και θα αρχίσει η χρήση της κανονικής διαδικασίας, μόλις δημιουργηθούν δύο ζεύγη κλειδιών, ένα για την υπογραφή και ένα για την κρυπτογράφηση, καθώς και μια κεντρική υπηρεσία ανάκτησης κλειδιού κρυπτογράφησης. Η προσωρινή διαδικασία για αιτήματα σχετικά με τα πιστοποιητικά είναι η ακόλουθη (ο αστερίσκος (*) σημαίνει ότι δεν έχει τροποποιηθεί η συνήθης διαδικασία):

(1) Ο συνδρομητής στέλνει αίτημα για πιστοποιητικό στην ΤΑΚ της ΓΔ του (ρητό αίτημα) ή η ΤΑΚ λαμβάνει τον κατάλογο των υποψήφιων συνδρομητών από τους προϊσταμένους τους (σιωπηρό αίτημα). (*)

(2) Η ΤΑΚ διαβιβάζει το αίτημα στην ΑΚ μέσω υπογεγραμμένου ηλεκτρονικού ταχυδρομείου. (*)

(3) Η ΤΑΚ ενημερώνει τους υποψήφιους συνδρομητές και τους ειδοποιεί ότι θα λάβουν έναν κωδικό αναγνώρισης από την ΑΚ και ένα δεύτερο κωδικό αναγνώρισης από την ίδια. (*)

(4) Η ΑΚ διενεργεί διοικητικό έλεγχο σχετικά με το συνδρομητή και εισάγει το SubjectName του στη βάση δεδομένων της ΑΠ. (*)

(5) Η ΑΠ στέλνει στην ΑΚ ένα αρχείο εγγραφής στο οποίο περιέχεται το SubjectName του συνδρομητή και ένας κωδικός αναγνώρισης Κ1. (*)

(6) Η ΑΚ στέλνει με ασφαλές ηλεκτρονικό ταχυδρομείο στην ΤΑΚ που υπέβαλε το αίτημα για πιστοποιητικό το αρχείο εγγραφής και τον κωδικό αναγνώρισης Κ1.

(7) Η ΤΑΚ στέλνει στο συνδρομητή (με ηλεκτρονικό ταχυδρομείο) μήνυμα στο οποίο αναφέρεται το αίτημα για πιστοποιητικό.

(8) Η ΤΑΚ, αφού λάβει από την ΑΚ το αρχείο εγγραφής, ελέγχει κατά πόσον ο συνδρομητής είναι υπαρκτό πρόσωπο. (*)

(9) Η ΤΑΚ απευθύνεται στην ΑΠ για να επιβεβαιώσει την ύπαρξη του συνδρομητή. (*)

(10) Η ΑΠ ενημερώνει το αρχείο εγγραφής και στέλνει στην ΤΑΚ ένα δεύτερο κωδικό αναγνώρισης Κ2. (*)

(11) Η ΤΑΚ, που έχει πλέον στην κατοχή της το αρχείο εγγραφής και τους δύο κωδικούς αναγνώρισης του συνδρομητή, δημιουργεί ένα ζεύγος κλειδιών.

(12) Η ΤΑΚ απευθύνεται στην ΑΠ και ζητά τη χορήγηση πιστοποιητικού (η ΤΑΚ παρουσιάζει ως αναγνωριστικό της στην ΑΠ τους δύο κωδικούς αναγνώρισης του συνδρομητή που διαθέτει).

(13) Η ΤΑΚ κάνει αντίγραφο του αρχείου κλειδιών, στο οποίο περιλαμβάνεται το πιστοποιητικό του ιδιωτικού και του δημόσιου κλειδιού του συνδρομητή και ο αρχικός κωδικός πρόσβασης.

(14) Η ΤΑΚ φυλάσσει το αρχείο κλειδιών και τον αρχικό κωδικό πρόσβασης σε ασφαλή χώρο που βρίσκεται υπό τον έλεγχο του υπεύθυνου ασφάλειας.

(15) Η ΤΑΚ παραδίδει το αρχείο κλειδιών και τον αρχικό κωδικό πρόσβασης στο συνδρομητή.

(16) Η ΤΑΚ βοηθά τους εγγεγραμμένους συνδρομητές να αποθηκεύσουν το αρχείο κλειδιών στο σκληρό δίσκο ή σε δισκέτα, ανάλογα με την πρακτική που εφαρμόζει η εκάστοτε ΓΔ.

4.3. Αποδοχή πιστοποιητικού

Η αποδοχή από το συνδρομητή των υποχρεώσεών του όσον αφορά τη χρήση του πιστοποιητικού εξασφαλίζεται στο πλαίσιο της διαδικασίας αιτήματος χορήγησης πιστοποιητικού, όπως περιγράφεται στο τμήμα 4.1 της παρούσας ΔΠΠ. *Ο συνδρομητής υπογράφει ότι αποδέχεται τους όρους της παρούσας ΔΠΠ και τους όρους που αναφέρονται στη σύμβαση συνδρομής*.

Η αποδοχή του πιστοποιητικού γίνεται στο πλαίσιο της διαδικασίας χορήγησης του πιστοποιητικού που περιγράφεται στο τμήμα 4.2 της παρούσας ΔΠΠ. Η λειτουργία του πρωτοκόλλου ασφαλούς επικοινωνίας μεταξύ συνδρομητή και ΑΠ CommisSign προϋποθέτει την αμοιβαία επαλήθευση της ταυτότητας των δύο μερών και μια σειρά αιτημάτων και αποκρίσεων που συνιστούν αποδοχή από το συνδρομητή των πιστοποιητικών δημόσιου κλειδιού που προκύπτουν.

4.4. Αναστολή ισχύος και ανάκληση πιστοποιητικού

4.4.1. Περιπτώσεις ανάκλησης

Τα πιστοποιητικά κρυπτογράφησης και/ή επαλήθευσης υπογραφής, στα οποία περιλαμβάνονται πιστοποιητικά για συνδρομητές, ΑΚ και στελέχη της ΑΠ, ανακαλούνται όταν, για οποιοδήποτε λόγο, δεν χαίρουν πλέον εμπιστοσύνης. Λόγοι απώλειας της εμπιστοσύνης σε πιστοποιητικά είναι, μεταξύ άλλων, οι εξής:

- απόλυση ή θέση σε διαθεσιμότητα για συγκεκριμένη αιτία

- αλλοίωση ή υποψία αλλοίωσης των ιδιωτικών κλειδιών και/ή των κωδικών πρόσβασης και του προφίλ του χρήστη

- λήξη της εργασιακής σχέσης

- αδυναμία του αιτούντος να εκπληρώσει τις υποχρεώσεις του όπως προβλέπονται από το παρόν έγγραφο και τις σχετικές πολιτικές πιστοποιητικών.

4.4.2. Ποιος μπορεί να ζητήσει ανάκληση

Ανάκληση πιστοποιητικού μπορεί να ζητήσει μόνο:

- ο συνδρομητής στο όνομα του οποίου έχει χορηγηθεί το πιστοποιητικό

- *το άτομο το οποίο υπέβαλε την αίτηση χορήγησης πιστοποιητικού εξ ονόματος μιας λειτουργικής ταχυδρομικής θυρίδας*

- *ο προϊστάμενος του συνδρομητή, εφόσον ο συνδρομητής ανήκει στο προσωπικό της Ευρωπαϊκής Επιτροπής*

- *τα μέλη του προσωπικού της ΑΠ CommisSign*

- *τα μέλη του προσωπικού της ΑΚ που συνδέονται με την ΑΠ CommisSign*

- *ο διευθυντής της υπηρεσίας πρωτοκόλλου και ασφάλειας*

- *η αρμόδια για τους διορισμούς αρχή (AIPN)*

- *η ΑΑΠ της Ευρωπαϊκής Επιτροπής*

4.4.3. Διαδικασία αιτήματος ανάκλησης [προς υλοποίηση] [προς επανεξέταση μετά την υλοποίηση]

Ο αιτών που επιθυμεί την ανάκληση ενός πιστοποιητικού οφείλει να το κοινοποιήσει στην ΤΑΚ του, να συμπληρώσει και να υπογράψει γραπτή έγκριση της ανάκλησης και να παρουσιαστεί αυτοπροσώπως με την υπηρεσιακή του κάρτα.

Υπεύθυνη για την επεξεργασία των αιτημάτων ανάκλησης και ανανέωσης πιστοποιητικού είναι η ΤΑΚ. Το αίτημα ανάκλησης πιστοποιητικού πρέπει να υποβληθεί εγγράφως στην ΤΑΚ. Όταν η ΑΚ συνδέεται με τον εξυπηρετητή της ΑΠ για να προβεί στην ανάκληση, η ΑΠ CommisSign ενημερώνει αμέσως την ΚΑΠ. Η ΤΑΚ ενημερώνει τον αιτούντα την ανάκληση το συντομότερο δυνατόν.

Τα πιστοποιητικά που ανακαλούνται καταχωρούνται στις ΚΑΠ και δημοσιεύονται στον κατάλογο της Ευρωπαϊκής Επιτροπής, σύμφωνα με το τμήμα 4.4 «Συχνότητα δημοσίευσης ΚΑΠ» της παρούσας ΔΠΠ. Οι ΑΚ μπορούν να δημοσιεύσουν αμέσως μία ΚΑΠ, εφόσον κριθεί απαραίτητο.

Για τη διευκόλυνση του ελέγχου είναι απαραίτητη η γραπτή έγκριση, η οποία πρέπει να περιλαμβάνει τα παρακάτω στοιχεία:

- την ημερομηνία του αιτήματος ανάκλησης
- το ονοματεπώνυμο του κατόχου του πιστοποιητικού (δηλαδή του συνδρομητή)
- λεπτομερή περιγραφή του λόγου για τον οποίο ζητείται ανάκληση
- το ονοματεπώνυμο και τον τίτλο του αιτούντος την ανάκληση
- τα στοιχεία επικοινωνίας του αιτούντος την ανάκληση
- την υπογραφή του αιτούντος την ανάκληση

Οι γραπτές εγκρίσεις αποστέλλονται στην ΑΚ. Σε περιπτώσεις που ζητείται άμεση ανάκληση του πιστοποιητικού συνδρομητή, το αίτημα πρέπει να υποβληθεί μέσω ηλεκτρονικού ταχυδρομείου ή μέσω τηλεφωνικής κλήσης στην ΑΚ και να επιβεβαιωθεί με γραπτή έγκριση.

Μετά την παραλαβή και την επιβεβαίωση της γραπτής έγκρισης, η ΑΚ ανακαλεί το πιστοποιητικό του συνδρομητή αφού συνδεθεί με τον εξυπηρετητή της ΑΠ και προβεί στην ανάκληση του πιστοποιητικού. Η ΑΚ καταγράφει το συμβάν στο ημερολόγιο διαχείρισης της ΑΚ. Η ΑΚ σημειώνει τις ενέργειες που πραγματοποιήθηκαν σχετικά με τη γραπτή έγκριση και στη συνέχεια υπογράφει και χρονολογεί την έγκριση. Η ΑΚ φυλάσσει την γραπτή έγκριση ανάκλησης.

4.4.4. Περίοδος χάριτος αιτήματος ανάκλησης

Δεν προβλέπεται.

4.4.5. Περιπτώσεις αναστολής ισχύος

Δεν προβλέπονται.

4.4.6. Ποιος μπορεί να ζητήσει αναστολή ισχύος

Δεν προβλέπεται.

4.4.7. Διαδικασία αιτήματος αναστολής ισχύος

Δεν προβλέπεται.

4.4.8. Περιορισμοί περιόδου αναστολής ισχύος

Δεν προβλέπονται.

4.4.9. Συχνότητα δημοσίευσης ΚΑΠ

Η ΑΠ CommisSign δημοσιεύει τις ΚΑΠ [και τις ΚΑΕ] στον κατάλογο της Ευρωπαϊκής Επιτροπής κάθε 24 ώρες. Οι ΚΑΠ [και οι ΚΑΕ] δημοσιεύονται 7 ημέρες την εβδομάδα. Κατ' εξαίρεση, ΚΑΠ [και ΚΑΕ] μπορεί να δημοσιευθούν και ενδιαμέσως (π.χ. σε περίπτωση εντοπισμού σοβαρής αλλοίωσης).

4.4.10. Απαιτήσεις για διενέργεια ελέγχου των ΚΑΠ

[Όλα τα πιστοποιητικά που χορηγούνται από την ΑΠ CommisSign πρέπει να περιλαμβάνουν το πλήρες διακεκριμένο όνομα (DN) του σημείου διανομής της ΚΑΠ, το οποίο ελέγχεται κατά την επαλήθευση του πιστοποιητικού.]

Πριν χρησιμοποιήσουν το πιστοποιητικό, τα συμβαλλόμενα μέρη οφείλουν να ελέγχουν την κατάστασή του βάσει του τρέχοντος αντιγράφου της ΚΑΠ. Εάν είναι προσωρινά αδύνατο να λάβουν πληροφορίες σχετικά με ενδεχόμενη ανάκλησή του, τα συμβαλλόμενα μέρη οφείλουν είτε να απορρίψουν τη χρήση του εν λόγω πιστοποιητικού είτε να λάβουν συνειδητά την απόφαση να αποδεχτούν τον κίνδυνο, την ευθύνη και τις συνέπειες της χρήσης ενός πιστοποιητικού του οποίου η αυθεντικότητα δεν μπορεί να εξασφαλιστεί με βάση τα πρότυπα της παρούσας ΔΠΠ.

4.4.11. Διαθεσιμότητα ελέγχου ανάκλησης/κατάστασης πιστοποιητικών σε απευθείας σύνδεση

Η ΥΔΚ της Ευρωπαϊκής Επιτροπής επί του παρόντος δεν υποστηρίζει τη δυνατότητα ελέγχου ανάκλησης/κατάστασης πιστοποιητικών σε απευθείας σύνδεση.

4.4.12. Απαιτήσεις ελέγχου ανάκλησης σε απευθείας σύνδεση

Δεν προβλέπονται.

4.4.13. Άλλες διαθέσιμες μορφές ανακοίνωσης ανακλήσεων

Δεν προβλέπονται.

4.4.14. Απαιτήσεις ελέγχου για άλλες μορφές ανακοίνωσης ανακλήσεων

Δεν προβλέπονται.

4.4.15. Ειδικές απαιτήσεις σε περίπτωση αλλοίωσης κλειδιού

Η αλλοίωση κλειδιού είναι ένα περιστατικό που αφορά την ασφάλεια και πρέπει να αντιμετωπίζεται σύμφωνα με συγκεκριμένη διαδικασία.

Σε περίπτωση αλλοίωσης κλειδιού τελικής οντότητας, υποβάλλεται έκθεση στην ΤΑΚ, στην οποία αναφέρονται οι περιστάσεις στις οποίες συνέβη η αλλοίωση. Εφόσον είναι τυχαία από πλευράς αιτούντος, δεν απαιτείται η λήψη περαιτέρω μέτρων. Διαφορετικά, η ΤΑΚ αναφέρει την αλλοίωση στην υπηρεσία πρωτοκόλλου και ασφάλειας για ενδεχόμενη περαιτέρω έρευνα και πιθανώς λήψη μέτρων σύμφωνα με τις διαδικασίες που περιγράφονται στην πολιτική ασφάλειας ΤΕΠ.

Σε περίπτωση αλλοίωσης, ή υποψίας αλλοίωσης, του κλειδιού υπογραφής της ΑΠ CommisSign, η ΑΠ CommisSign ειδοποιεί αμέσως την ΑΑΠ. Με τη συνεργασία της ΑΑΠ της Ευρωπαϊκής Επιτροπής, η ΑΠ CommisSign ενημερώνει όλες τις ΑΠ στις οποίες έχει χορηγήσει αμοιβαία πιστοποιητικά.

4.5. Διαδικασίες ελέγχου ασφάλειας [προς υλοποίηση] [προς επανεξέταση μετά την υλοποίηση]

4.5.1. Κατηγορίες συμβάντων που καταγράφονται

[Όλα τα σημαντικά συμβάντα που αφορούν την ασφάλεια στο λογισμικό της ΑΠ CommisSign χρονοσημαίνονται αυτόματα και καταγράφονται σε μητρώα ελέγχου. Στα συμβάντα αυτά περιλαμβάνονται:

- επιτυχημένες και αποτυχημένες απόπειρες εγκαινίασης συνδρομητών, κατάργησης, ενεργοποίησης, απενεργοποίησης, ενημέρωσης και ανάκτησης συνδρομητών, των κλειδιών τους και των πιστοποιητικών τους

- επιτυχημένες και αποτυχημένες απόπειρες δημιουργίας, κατάργησης, σύνδεσης ως, ορισμού, επαναφοράς και αλλαγής κωδικών πρόσβασης, ανάκλησης προνομίων, δημιουργίας, ενημέρωσης και ανάκτησης κλειδιών και πιστοποιητικών στελεχών της ΑΠ, των ΑΚ και των συνδρομητών

- αποτυχημένες διαδράσεις με τον κατάλογο, καθώς και επιτυχημένες και αποτυχημένες απόπειρες σύνδεσης, ανάγνωσης και εγγραφής από το σύστημα της ΑΠ

- όλα τα συμβάντα που αφορούν την ανάκληση πιστοποιητικών, την τροποποίηση και την επικύρωση της πολιτικής ασφάλειας, την έναρξη και την παύση λειτουργίας του λογισμικού της ΑΠ, τη δημιουργία αντιγράφου ασφαλείας της βάσης δεδομένων, την αμοιβαία πιστοποίηση, την επικύρωση πιστοποιητικών και ακολουθίας πιστοποιητικών, τη διαχείριση χαρακτηριστικών πιστοποιητικού, την αναβάθμιση χρηστών, την αλλαγή DN, τη βάση δεδομένων και την ανίχνευση ελέγχου

- η γενική διαχείριση, η διαχείριση του κύκλου ζωής των πιστοποιητικών και διάφορα άλλα συμβάντα

- η έναρξη και ο τερματισμός του συστήματος.

Ο διαχειριστής του συστήματος της ΑΠ διατηρεί πληροφορίες σχετικά με:

- τις αλλαγές στις παραμέτρους και τη συντήρηση του συστήματος

- τα προνόμια του διαχειριστή

- τις αναφορές σχετικά με ανακολουθίες και αλλοιώσεις

- τις μη εξουσιοδοτημένες απόπειρες δικτυακής πρόσβασης στο σύστημα της ΑΠ.

Οι εγκαταστάσεις της ΑΠ διαθέτουν ηλεκτρονικό σύστημα παρακολούθησης που παρέχει πληροφορίες σχετικά με την πρόσβαση στις εγκαταστάσεις της ΑΠ CommisSign.]

4.5.2. Συχνότητα επεξεργασίας μητρώων ελέγχου

[Τα στελέχη της ΑΠ της Ευρωπαϊκής Επιτροπής επεξεργάζονται τα μητρώα ελέγχου εβδομαδιαίως, εξετάζοντας οποιαδήποτε προειδοποιητικά μηνύματα ή παρατυπίες στα μητρώα.]

4.5.3. Περίοδος φύλαξης μητρώων ελέγχου

[Οι ανιχνεύσεις ελέγχου φυλάσσονται σε ηλεκτρονική μορφή επ' αόριστον σύμφωνα με τις παραμέτρους της ΑΠ CommisSign. Στο τμήμα 4.5.5 «Διαδικασία δημιουργίας αντιγράφου ασφαλείας του μητρώου ελέγχου» περιγράφονται οι διαδικασίες αρχειοθέτησης αυτών των μητρώων.]

4.5.4. Προστασία μητρώων ελέγχου

[Η ανίχνευση ελέγχου αποθηκεύεται σε κανονικά μη δομημένα αρχεία του λειτουργικού συστήματος. Κάθε αρχείο ανίχνευσης ελέγχου αποτελείται από μια κεφαλίδα ελέγχου που περιέχει πληροφορίες για τους ελέγχους που έχουν διενεργηθεί στο αρχείο και από έναν κατάλογο συμβάντων. Για κάθε συμβάν ελέγχου και για την κεφαλίδα ελέγχου δημιουργείται ένας κώδικας επαλήθευσης μηνυμάτων. Κάθε αρχείο ανίχνευσης ελέγχου έχει διαφορετικό κλειδί ελέγχου που χρησιμοποιείται για τη δημιουργία του κώδικα επαλήθευσης μηνυμάτων. Ο κύριος χρήστης της ΑΠ CommisSign της Ευρωπαϊκής Επιτροπής προστατεύει το κλειδί ελέγχου, το οποίο αποθηκεύεται στην κεφαλίδα ελέγχου.

Η ανίχνευση ελέγχου μπορεί να επεκτείνεται σε περισσότερα από ένα αρχεία. Ένα νέο αρχείο ανίχνευσης ελέγχου δημιουργείται κάθε φορά που το τρέχον αρχείο ανίχνευσης ελέγχου φτάνει το προκαθορισμένο μέγεθος των 100 Kbytes ή κάθε φορά που αναβαθμίζεται το κύριο κλειδί της ΑΠ.]

4.5.5. Διαδικασία δημιουργίας αντιγράφου ασφαλείας του μητρώου ελέγχου

[Κάθε βράδυ δημιουργούνται αντίγραφα ασφαλείας των ανιχνεύσεων ελέγχου στο πλαίσιο της τακτικής δημιουργίας αντιγράφου ασφαλείας του συστήματος της ΑΠ. Ο διαχειριστής του συστήματος της ΑΠ αρχειοθετεί τα αρχεία των ανιχνεύσεων ελέγχου σε εβδομαδιαία βάση. Όλα τα αρχεία, συμπεριλαμβανομένου και του τρέχοντος, μεταφέρονται σε μαγνητικές ταινίες και αποθηκεύονται σε ασφαλή χώρο αρχειοθέτησης.]

4.5.6. Σύστημα συλλογής στοιχείων ελέγχου

[Το σύστημα συλλογής στοιχείων των ανιχνεύσεων ελέγχου αποτελεί τμήμα του συστήματος λογισμικού της ΑΠ CommisSign.]

4.5.7. Ειδοποίηση του υποκειμένου που προκαλεί το συμβάν

[Όταν ένα συμβάν καταγράφεται από το σύστημα συλλογής στοιχείων ελέγχου, δεν αποστέλλεται ειδοποίηση στο άτομο που προκάλεσε το προς έλεγχο συμβάν. Το υποκείμενο ενδέχεται να ειδοποιηθεί ότι η ενέργειά του ήταν επιτυχημένη ή αποτυχημένη, αλλά όχι ότι η ενέργειά του ελέγχθηκε.]

4.5.8. Εκτίμηση ευπάθειας

[Ο διαχειριστής του συστήματος της ΑΠ CommisSign και τα στελέχη της ΑΠ ακολουθούν τις διαδικασίες που ορίζονται στο τμήμα «Διαδικασία ελέγχου ασφάλειας συστήματος» της παρούσας ΔΠΠ, προκειμένου να παρακολουθούν, να εκτιμούν και να αντιμετωπίζουν δεόντως τις αδυναμίες του συστήματος.]

4.6. Αρχειοθέτηση καταγραφών [προς υλοποίηση] [προς επανεξέταση μετά την υλοποίηση]

4.6.1. Κατηγορίες δεδομένων που αρχειοθετούνται

[Κατά την εκτέλεση των καθηκόντων των ΑΚ και ΤΑΚ, παρέχεται στην ΑΚ και στις ΤΑΚ μια σειρά στοιχείων, στα οποία περιλαμβάνονται:

- στοιχεία ταυτότητας
- αιτήματα πιστοποιητικών
- εγκρίσεις ανάκλησης πιστοποιητικών
- εγκρίσεις ανάκτησης κλειδιών

Ορισμένα από τα παρεχόμενα στοιχεία αποτελούν προσωπικά δεδομένα και εμπίπτουν στις διατάξεις του κανονισμού (ΕΚ) αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Δεκεμβρίου 2000. Τα εν λόγω στοιχεία αποθηκεύονται με ασφάλεια σύμφωνα με τις απαιτήσεις του ανωτέρω κανονισμού. Η πρόσβαση σε αυτά περιορίζεται στο προσωπικό της ΑΚ.

Στις κατηγορίες συμβάντων που καταγράφονται στη βάση δεδομένων του συστήματος της ΑΠ περιλαμβάνονται:

- η δημιουργία του ζεύγους κλειδιών υπογραφής της ΑΠ
- η προσθήκη ή η αφαίρεση τελικών χρηστών από το σύστημα
- οι αλλαγές στο ιστορικό του ζεύγους κλειδιών κρυπτογράφησης και στο ιστορικό του δημόσιου κλειδιού επαλήθευσης για όλους τους χρήστες, συμπεριλαμβανομένων των συμβάντων χορήγησης και ανάκλησης πιστοποιητικών
- οι αλλαγές του DN των τελικών χρηστών
- η προσθήκη ή η αφαίρεση προνομίων των στελεχών της ΑΚ και της ΑΠ
- οι αλλαγές στα προνόμια των στελεχών της ΑΚ και της ΑΠ
- οι αλλαγές σε ορισμένες πτυχές της πολιτικής, όπως η διάρκεια ισχύος των πιστοποιητικών
- η δημιουργία και η ανάκληση αμοιβαίων πιστοποιητικών.

Επιπλέον το σύστημα της ΑΠ CommisSign παρέχει δεδομένα μητρώων ελέγχου όπως περιγράφεται στο τμήμα 4.5 της παρούσας ΔΠΠ.]

4.6.2. Περίοδος φύλαξης αρχείων

[Τα στοιχεία των ελέγχων (βλ. τμήμα 4.5 της παρούσας ΔΠΠ), τα κλειδιά των συνδρομητών και τα αιτήματα/οι εγκρίσεις πιστοποιητικών, καθώς και οι πληροφορίες ταυτοποίησης και επαλήθευσης ταυτότητας αρχειοθετούνται για μία πενταετία.]

[Τα πιστοποιητικά ψηφιακών υπογραφών, τα ιδιωτικά κλειδιά εμπιστευτικότητας που αποθηκεύονται από την ΑΠ [, οι ΚΑΕ] και οι ΚΑΠ που δημιουργούνται από την ΑΠ αρχειοθετούνται σύμφωνα με τις κανονιστικές ρυθμίσεις της Ευρωπαϊκής Επιτροπής και των κρατών μελών.]

4.6.3. Προστασία αρχείων

[Η βάση δεδομένων του συστήματος της ΑΠ CommisSign [κρυπτογραφείται και] προστατεύεται από το σύστημα της ΑΠ. Η προστασία της ανίχνευσης ελέγχου περιγράφεται στο τμήμα 4.5 «Προστασία μητρώων ελέγχου» της παρούσας ΔΠΠ.

Για τα μέσα αρχειοθέτησης προβλέπεται υλική ασφάλεια, δηλαδή φυλάσσονται σε χώρο περιορισμένης πρόσβασης στον οποίο έχουν πρόσβαση μόνον οι διαχειριστές του συστήματος της ΑΠ CommisSign και οι κύριοι χρήστες της ΑΠ.]

4.6.4. Διαδικασία δημιουργίας εφεδρικών αρχείων

Κατά τη δημιουργία των αρχείων δημιουργούνται και εφεδρικά αντίγραφα. Τα πρωτότυπα αποθηκεύονται επιτόπου και στεγάζονται όπου και το σύστημα της ΑΠ CommisSign. Τα εφεδρικά αρχεία αποθηκεύονται σε ασφαλές και διαφορετικό σημείο.]

4.6.5. Σύστημα συλλογής αρχείων

[Το σύστημα συλλογής αρχείων (δυνατότητα δημιουργίας αντιγράφων ασφαλείας) για τη βάση δεδομένων του συστήματος της ΑΠ CommisSign αποτελεί τμήμα του συστήματος της ΑΠ CommisSign.

Το σύστημα συλλογής αρχείων (δυνατότητα δημιουργίας αντιγράφων ασφαλείας) για τα αρχεία της ανίχνευσης ελέγχου περιγράφεται στο τμήμα 4.5 «Διαδικασία δημιουργίας αντιγράφου ασφαλείας του μητρώου ελέγχου» και «Σύστημα συλλογής στοιχείων ελέγχου» της παρούσας ΔΠΠ.

Η αρχειοθέτηση και των δύο συνόλων δεδομένων σε ξεχωριστά μέσα και η ασφαλής αποθήκευση των μέσων αυτών δεν αποτελεί τμήμα του συστήματος της ΑΠ CommisSign.]

4.6.6. Διαδικασίες ανάκτησης και επαλήθευσης των αρχειοθετημένων πληροφοριών

[Δύο φορές ετησίως, τα δεδομένα που αποθηκεύονται σε ταινίες αρχείου ανακτώνται και επαληθεύονται από στελέχη της ΑΠ CommisSign, ώστε να διασφαλίζεται ότι δεν έχει υπάρξει αλλοίωση ή απώλεια. Σε περίπτωση

αλλοίωσης ή απώλειας δεδομένων, ανακτάται το εφεδρικό αρχείο, το οποίο καθίσταται το νέο κύριο αρχείο και δημιουργείται νέο αντίγραφο ασφαλείας.

Μία φορά κάθε πενταετία, δημιουργείται νέο αντίγραφο ασφαλείας κάθε αρχείου, έστω και εάν δεν υπάρχουν ενδείξεις αλλοίωσης ή απώλειας δεδομένων στο κύριο ή στο εφεδρικό αρχείο. Για κάθε ταινία, το νέο εφεδρικό αρχείο γίνεται το κύριο αρχείο, ενώ το προηγούμενο κύριο αρχείο γίνεται το εφεδρικό αρχείο και η ταινία του προηγούμενου εφεδρικού αρχείου ανακυκλώνεται με ασφαλή τρόπο.]

4.7. Μεταβολή κλειδιού

Βλ. τμήματα 3.2 και 3.3 της παρούσας ΔΠΠ.

4.8. Αποκατάσταση σε περίπτωση αλλοίωσης ή καταστροφής [προς υλοποίηση] [προς επανεξέταση μετά την υλοποίηση]

4.8.1. Καταστροφή υπολογιστικών πόρων, λογισμικού και/ή δεδομένων

Σε περίπτωση καταστροφής ή σοβαρής αλλοίωσης, η ΑΠ CommisSign και οι ΑΚ οφείλουν να λάβουν τα παρακάτω μέτρα προκειμένου να αποκατασταθεί το ασφαλές περιβάλλον:

(1) αλλάζουν όλοι οι κωδικοί πρόσβασης στο σύστημα της ΑΠ CommisSign των κύριων χρηστών και των στελεχών της ΑΠ και των ΑΚ (σε περίπτωση αλλοίωσης της ΑΠ)

(2) ανάλογα με τη φύση της καταστροφής, ανακαλούνται τα πιστοποιητικά ορισμένων ή όλων των χρηστών

(3) εάν ο κατάλογος παρουσιάζει αστάθεια ή υπάρχουν υποψίες ότι έχει καταστραφεί, πρέπει να ανακτηθούν τα δεδομένα του καταλόγου, τα πιστοποιητικά κρυπτογράφησης και οι ΚΑΠ. Μετά την αποκατάσταση του καταλόγου βάσει του αντιγράφου ασφαλείας από το διαχειριστή καταλόγου, ο κύριος χρήστης της ΑΠ ενημερώνει τις πληροφορίες της ΥΔΚ στον κατάλογο. Στις πληροφορίες της ΥΔΚ περιλαμβάνονται ΚΑΠ και πιστοποιητικά τα οποία έχουν αλλάξει μετά τη δημιουργία του τρέχοντος αντιγράφου ασφαλείας του καταλόγου.

(4) εφόσον χρειάζεται ανάκτηση το προφίλ στελέχους της ΑΠ ή της ΑΚ, η ανάκτηση μπορεί να γίνει από άλλο στέλεχος της ΑΠ ή της ΑΚ.

Βλ. τμήμα 4.4 «Ειδικές απαιτήσεις σε περίπτωση αλλοίωσης κλειδιού» σχετικά με την αλλοίωση ενός κλειδιού ΑΠ.

4.8.2. Ανάκτηση κλειδιού οντότητας

Η στερεότυπη διαδικασία έχει τροποποιηθεί ώστε να προσφέρεται η δυνατότητα ανάκτησης κλειδιού σε επίπεδο ΓΔ. Αντίγραφο του ιδιωτικού κλειδιού και ο αντίστοιχος αρχικός κωδικός πρόσβασης φυλάσσονται από τον υπεύθυνο ασφάλειας της ΓΔ σε ασφαλές σημείο με ελεγχόμενη πρόσβαση. Πρόσβαση σε κλειδιά και κωδικούς πρόσβασης έχει μόνον ο

υπεύθυνος ασφάλειας ή αρμοδίως εξουσιοδοτημένος επίσημος εκπρόσωπός του. Ανάκτηση κλειδιού πραγματοποιείται μόνον από τις ΤΑΚ. Η ανάκτηση κλειδιού πραγματοποιείται παρουσία της ΤΑΚ και του υπεύθυνου ασφάλειας, που παρέχουν και την εξουσιοδότηση. Εφόσον η ΤΑΚ και ο υπεύθυνος ασφάλειας δεν είναι διαθέσιμοι, σε περίπτωση έκτακτης ανάγκης στελέχη της ΑΠ υποκαθιστούν τους διαχειριστές. Ανάκτηση κλειδιού μπορεί να γίνει σε τρεις περιπτώσεις:

- μετά από αίτημα του χρήστη
- μετά από αίτημα του πειθαρχικού συμβουλίου ή ισότιμου εσωτερικού οργάνου
- μετά από αίτημα της Γενικής Διεύθυνσης σε περίπτωση μόνιμης ή σημαντικής μη διαθεσιμότητας του χρήστη που βλάπτει σοβαρά το συμφέρον της υπηρεσίας.

[Το χρονικό διάστημα που απαιτείται για την ολοκλήρωση μιας μη επείγουσας ανάκτησης κλειδιού είναι 48 ώρες. Σε περιπτώσεις επείγουσας ανάγκης, ενημερώνεται η ΤΑΚ.]

4.8.2.1.Ανάκτηση κλειδιού μετά από αίτημα χρήστη

Περιπτώσεις στις οποίες ο συνδρομητής μπορεί να ζητήσει ανάκτηση κλειδιού είναι μεταξύ άλλων:

- ο συνδρομητής έχει ξεχάσει τον κωδικό πρόσβασης
- ο συνδρομητής έχει χάσει ή έχει καταστρέψει το αρχείο ιδιωτικού κλειδιού.

Για την προστασία του συνδρομητή από μη εξουσιοδοτημένα αιτήματα, ο συνδρομητής οφείλει:

- να φροντίζει να παρουσιάζεται αυτοπροσώπως και
- να υποβάλλει γραπτή έγκριση στην ΤΑΚ στην οποία να αναφέρει το λόγο για τον οποίο ζητά την ανάκτηση.

Μετά την παραλαβή της γραπτής έγκρισης, η ΤΑΚ επαληθεύει οπτικά την ταυτότητα του συνδρομητή μέσω της υπηρεσιακής κάρτας του και εκτελεί τη διαδικασία ανάκτησης κλειδιού. Η ΤΑΚ καταγράφει το συμβάν της ανάκτησης για διευκόλυνση του ελέγχου. Η ΤΑΚ σημειώνει τις ενέργειες οι οποίες πραγματοποιήθηκαν βάσει της γραπτής έγκρισης και στη συνέχεια υπογράφει και χρονολογεί την έγκριση, την οποία φυλάσσει.

Στη συνέχεια η ΤΑΚ δίνει στο συνδρομητή οδηγίες για την απόκτηση νέων στοιχείων εξουσιοδότησης.

4.8.2.2.Ανάκτηση κλειδιού μετά από αίτημα τρίτου

Περιπτώσεις στις οποίες γίνεται ανάκτηση κλειδιού χωρίς τη συναίνεση του συνδρομητή είναι μεταξύ άλλων:

- ο συνδρομητής έχει αποχωρήσει από τον οργανισμό και ο προϊστάμενός του ή ο διευθυντής του τμήματος χρειάζεται να αποκρυπτογραφήσει αρχεία για τη συνέχιση των εργασιών

- οι ενέργειες του συνδρομητή αμφισβητούνται από την Ευρωπαϊκή Επιτροπή και απαιτείται να εξεταστούν τα αρχεία του

- οι ενέργειες του συνδρομητή αμφισβητούνται από εξωτερικό όργανο δημόσιας τάξης και απαιτείται να εξεταστούν τα αρχεία του.

Ο αιτών την ανάκτηση κλειδιού οφείλει να απευθυνθεί στον υπεύθυνο ασφάλειας. Πριν την εκτέλεση της ανάκτησης, υποβάλλεται στις ΤΑΚ γραπτή έγκριση τόσο από το γενικό διευθυντή του συνδρομητή όσο και από το φορέα που ζητά την ανάκτηση του κλειδιού. Στο αίτημα πρέπει να περιλαμβάνονται τα εξής:

- η ημερομηνία υποβολής του αιτήματος για ανάκτηση

- το ονοματεπώνυμο του κατόχου των κλειδιών (δηλαδή του συνδρομητή)

- το ονοματεπώνυμο του αιτούντος και η υπηρεσία της Ευρωπαϊκής Επιτροπής

- αναλυτική περιγραφή του λόγου για τον οποίο ζητείται πρόσβαση στα αρχεία του συνδρομητή

- το ονοματεπώνυμο των συγκεκριμένων προσώπων στα οποία θα επιτραπεί να εξετάσουν τα αρχεία του συνδρομητή και τα οποία θα έχουν την ευθύνη για τυχόν μεταγενέστερη πρόσβαση στα αρχεία ατόμων που δεν κατονομάζονται

- περιγραφή (και/ή το όνομα) των αρχείων του συνδρομητή που πρέπει να εξεταστούν ή δήλωση έγκρισης πρόσβασης σε όλα τα αρχεία

- περιγραφή του ρόλου της ΤΑΚ πέρα από την ανάκτηση του κλειδιού, συμπεριλαμβανομένου του είδους των πληροφοριών που θα παρέχει εφόσον ο συνδρομητής ζητήσει να ενημερωθεί σχετικά με το λόγο της αλλαγής της προσβασιμότητάς του στην ΑΠ CommisSign.

Μετά την παραλαβή γραπτής έγκρισης, η ΤΑΚ επικοινωνεί με τους αρμοδίους ώστε να προγραμματιστούν οι ενέργειες της ανάκτησης του κλειδιού.

[Σημείωση: Υπό ορισμένες συνθήκες η ΤΑΚ μπορεί να λάβει δικαστική εντολή με την οποία να ζητείται ανάκτηση κλειδιού. Στην περίπτωση αυτή, η δικαστική εντολή θα είναι ισότιμη με τη γραπτή έγκριση.]

Οι αιτούντες ενδέχεται να προσκομίσουν δισκέτα στην οποία να περιέχονται τα αρχεία του συνδρομητή τα οποία πρέπει να εξεταστούν κατά την προγραμματισμένη διαδικασία ανάκτησης. Οι ΤΑΚ (υπό τον έλεγχο του υπεύθυνου ασφάλειας) μπορούν να φορτώνουν τα προς αποκρυπτογράφηση και εξέταση αρχεία σε τοπικό μηχάνημα. Μετά την ολοκλήρωση της

διαδικασίας τα αποκρυπτογραφημένα αρχεία διαγράφονται, ώστε να αποφεύγεται η μη εξουσιοδοτημένη πρόσβαση σε αυτά.

Οι αιτούντες πρέπει πρώτα να επιβεβαιώνουν ότι οι ΤΑΚ διαθέτουν μηχανήματα με το απαιτούμενο λογισμικό για την ανάγνωση των αρχείων. Διαφορετικά, οι ΤΑΚ μεταβαίνουν στο χώρο του αιτούντα εντός των εγκαταστάσεων της Ευρωπαϊκής Επιτροπής.

Μετά την παραλαβή της γραπτής έγκρισης, η ΤΑΚ επαληθεύει οπτικά την ταυτότητα των εξουσιοδοτημένων ατόμων μέσω των υπηρεσιακών καρτών τους, εκτελεί τη διαδικασία ανάκτησης κλειδιού και καταγράφει το συμβάν της ανάκτησης. Η ΤΑΚ σημειώνει τις ενέργειες που πραγματοποιήθηκαν βάσει της γραπτής έγκρισης και στη συνέχεια υπογράφει και χρονολογεί την έγκριση, την οποία φυλάσσει για διευκόλυνση του ελέγχου.

Εφόσον ο συνδρομητής διατηρεί τα προνόμια προσβασιμότητας στην ΑΠ CommisSign μετά την ολοκλήρωσης της ανάκτησης κλειδιού που ζητήθηκε, η ΑΚ εκτελεί εκ νέου τη διαδικασία ανάκτησης κλειδιού, ώστε ο συνδρομητής να είναι βέβαιος ότι κανείς δεν έχει πλέον πρόσβαση στα δεδομένα του κλειδιού του.

Εφόσον κριθεί αναγκαίο, η ΤΑΚ μπορεί να απενεργοποιήσει τον ανακτημένο λογαριασμό του συνδρομητή στην ΑΠ CommisSign μετά την προγραμματισμένη διαδικασία, εφόσον ζητείται εξέταση των αρχείων εξ αποστάσεως για σύντομο χρονικό διάστημα. Η επανενεργοποίηση του λογαριασμού εξαρτάται από τις οδηγίες που παρέχονται από τον αιτούντα.

Ο όρος «εξωτερικές οντότητες» αναφέρεται σε οποιοδήποτε όργανο δημόσιας τάξης. Η επεξεργασία των αιτημάτων που υποβάλλονται από εξωτερικές οντότητες γίνεται από την υπηρεσία πρωτοκόλλου και ασφάλειας.

Τα μέτρα που λαμβάνονται σε περίπτωση ανάκτησης κλειδιού χωρίς τη συναίνεση του συνδρομητή λαμβάνονται και για αιτήματα που υποβάλλονται από εξωτερικές οντότητες.

4.8.3. Ανάκτηση σε περίπτωση καταστροφής

[Η ΑΠ CommisSign διαθέτει σχέδιο αποκατάστασης σε περίπτωση καταστροφής όπου περιγράφονται οι διαδικασίες ανάκτησης σε περίπτωση καταστροφής ή σοβαρής αλλοίωσης. Σε περίπτωση καταστροφής δημιουργείται εφεδρική ΑΠ σε άλλο κέντρο της Ευρωπαϊκής Επιτροπής.]

4.9. Λήξη της ΑΠ

Σε περίπτωση λήξης της ΑΠ CommisSign, τη διαδικασίας λήξης εποπτεύει η ΑΑΠ της Ευρωπαϊκής Επιτροπής. Η ΑΚ και οι ΤΑΚ συνεργάζονται με την ΑΠ προκειμένου να γνωστοποιήσουν σε όλους τους συνδρομητές την παύση της λειτουργίας της ΑΠ CommisSign.

Ανακαλούνται όλα τα πιστοποιητικά που χορηγήθηκαν από την ΑΠ CommisSign.

Η Ευρωπαϊκή Επιτροπή διατηρεί αρχείο της βάσης δεδομένων της ΑΠ CommisSign σύμφωνα με την πολιτική ασφάλειας συστημάτων πληροφορικής και τις κανονιστικές ρυθμίσεις της Ευρωπαϊκής Επιτροπής, καθώς και με τις σχετικές κανονιστικές ρυθμίσεις των κρατών μελών.

5. ΥΛΙΚΟΙ ΚΑΙ ΔΙΑΔΙΚΑΣΤΙΚΟΙ ΕΛΕΓΧΟΙ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΕΛΕΓΧΟΙ ΑΣΦΑΛΕΙΑΣ ΤΟΥ ΠΡΟΣΩΠΙΚΟΎ

5.1. Υλικοί έλεγχοι ασφάλειας

5.1.1. Θέση και κατασκευή χώρου

Η ΑΠ CommisSign βρίσκεται σε χώρο, η πρόσβαση στον οποίο ελέγχεται μέσω ενός σημείου εισόδου και περιορίζεται στο εξουσιοδοτημένο προσωπικό. Οι εγκαταστάσεις στις οποίες στεγάζεται είναι κλειδωμένες και παρακολουθούνται ηλεκτρονικώς 24 ώρες το εικοσιτετράωρο, επτά ημέρες την εβδομάδα. [Τα ηλεκτρονικά μητρώα προστατεύονται από ενδεχόμενη παρείσφρηση στην υπηρεσία πρωτοκόλλου και ασφάλειας.]

5.1.2. Υλική πρόσβαση

Οι εγκαταστάσεις της ΑΠ CommisSign είναι κλειδωμένες και η πρόσβαση σε αυτές επιτρέπεται μόνο σε εξουσιοδοτημένα μέλη του προσωπικού τα οποία υποβάλλονται σε ενδεδειγμένο έλεγχο. Πρόσβαση στην ΑΠ CommisSign επιτρέπεται μόνο στους κύριους χρήστες της ΑΠ CommisSign, στα στελέχη της ΑΠ και στο διαχειριστή του συστήματος της ΑΠ.

[Τα συστήματα των ΑΚ βρίσκονται σε χώρους περιορισμένης πρόσβασης.] Οι κεντρικές ΑΚ προστατεύονται με έξυπνη κάρτα.

Όσον αφορά την προστασία και τη χρήση των κλειδιών τους, οι συνδρομητές οφείλουν να συμμορφώνονται με τις απαιτήσεις της παρούσας ΔΠΠ και της πολιτικής πιστοποιητικών της Ευρωπαϊκής Επιτροπής. Οι συνδρομητές ενημερώνονται για τις απαιτήσεις αυτές, αλλά δεν ελέγχονται ούτε παρακολουθούνται σε τακτική βάση.

5.1.3. Ηλεκτρικό ρεύμα και κλιματισμός

Οι εγκαταστάσεις της ΑΠ της Ευρωπαϊκής Επιτροπής διαθέτουν παροχή ηλεκτρικού ρεύματος και κλιματισμό ικανά να δημιουργήσουν ένα αξιόπιστο λειτουργικό περιβάλλον. Οι χώροι εργασίας του προσωπικού εντός των εγκαταστάσεων διαθέτουν επαρκή μέσα για την κάλυψη των αναγκών σε επίπεδο λειτουργίας, υγιεινής και ασφάλειας.

5.1.4. Έκθεση σε νερό

Ο σταθμός εργασίας της ΑΠ CommisSign δεν κινδυνεύει από έκθεση σε νερό.

5.1.5. Πυρασφάλεια

[Οι εγκαταστάσεις της ΑΠ CommisSign διαθέτουν σύστημα πυρόσβεσης σύμφωνα με την πολιτική και τον κώδικα της υπηρεσίας κατάρτισης σε θέματα υγιεινής και ασφάλειας της Ευρωπαϊκής Επιτροπής.]

5.1.6. Μέσα αποθήκευσης

[Τα μέσα αποθήκευσης που χρησιμοποιούνται από την ΑΠ CommisSign προστατεύονται από περιβαλλοντικούς κινδύνους, όπως η θερμοκρασία, η υγρασία και ο μαγνητισμός.]

5.1.7. Διάθεση απορριμάτων

Τα μέσα που χρησιμοποιούνται για την αποθήκευση πληροφοριών από τα αρχεία της ΑΠ CommisSign εξυγιαίνονται ή καταστρέφονται πριν απορριφθούν προς διάθεση.

Τα συνήθη απορρίμματα γραφείου απομακρύνονται ή καταστρέφονται σύμφωνα με τους τοπικούς κανόνες της Ευρωπαϊκής Επιτροπής.

5.1.8. Εφεδρική μονάδα εκτός των εγκαταστάσεων της ΑΠ [άνευ αντικειμένου]

[Η εφεδρική μονάδα της ΑΠ διαθέτει ισότιμο επίπεδο ασφάλειας και ελέγχων με την κύρια ΑΠ CommisSign.]

5.2. Διαδικαστικοί έλεγχοι

5.2.1. Θέσεις εμπιστοσύνης

[Τα μέλη του προσωπικού που πληρούν αυτές τις θέσεις έχουν υποβληθεί επιτυχώς στον έλεγχο ιστορικού που προβλέπεται για την ανάληψη κρίσιμων-ευαίσθητων θέσεων. Τα κριτήρια του ελέγχου ιστορικού και άλλων ελέγχων ασφάλειας του προσωπικού αναφέρονται στα ακόλουθα τμήματα.]

5.2.1.1.Θέσεις εμπιστοσύνης ΑΠ:

Την ευθύνη για τη λειτουργία της ΑΠ CommiSign έχει η υπηρεσία πρωτοκόλλου και ασφάλειας, που έχει αναλάβει το ρόλο της αρχής λειτουργίας ΑΠ, των στελεχών ΑΠ και των διαχειριστών συστήματος ΑΠ όπως περιγράφονται κατωτέρω.

Για να διασφαλιστεί ότι τα μέτρα ασφάλειας δεν μπορούν να παρακαμφθούν με τις μεμονωμένες ενέργειες ενός ατόμου, οι αρμοδιότητες της ΑΠ CommisSign έχουν κατανεμηθεί σε πολλές θέσεις και σε πολλά άτομα. Ο κάθε λογαριασμός στο σύστημα της ΑΠ CommisSign έχει περιορισμένες δυνατότητες, ανάλογα με τη θέση του αντίστοιχου ατόμου. Οι θέσεις στο πλαίσιο της ΑΠ CommisSign είναι:

- Κύριοι χρήστες ΑΠ

[Τρία άτομα αναλαμβάνουν καθήκοντα κύριου χρήστη της ΑΠ.] Οι κύριοι χρήστες διορίζονται από την ΑΛ της ΑΠ και είναι υπεύθυνοι για:

– τη δημιουργία και τη διατήρηση του κύριου κλειδιού της ΑΠ CommisSign

– την αλλαγή των κωδικών πρόσβασης στον εξυπηρετητή της ΑΠ

– την ανάκτηση των κωδικών πρόσβασης των στελεχών της ΑΠ σε περίπτωση που οι κάτοχοί τους τούς έχουν ξεχάσει.

- Στελέχη ΑΠ

[Τρία άτομα αναλαμβάνουν καθήκοντα στελέχους της ΑΠ.]. Τα στελέχη της ΑΠ διορίζονται από την ΑΛ της ΑΠ και είναι υπεύθυνα για:

– τον καθορισμό και την τροποποίηση της πολιτικής ασφάλειας της ΑΠ CommisSign, σύμφωνα με την παρούσα ΔΠΠ και την πολιτική πιστοποιητικών της Ευρωπαϊκής Επιτροπής

– τον καθορισμό του αριθμού των απαιτούμενων εξουσιοδοτήσεων για ευαίσθητες λειτουργίες

– την προσθήκη και τη διαγραφή ΑΚ και ΤΑΚ

– [τη χορήγηση, ενημέρωση και ανάκληση αμοιβαίων πιστοποιητικών σύμφωνα με τις οδηγίες της ΑΑΠ της Ευρωπαϊκής Επιτροπής]

– την αλλαγή του αριθμού PIN της έξυπνης κάρτας των ΑΚ και ΤΑΚ

– τον καθορισμό των προκαθορισμένων ιδιοτήτων των πιστοποιητικών (διάρκεια ισχύος κ.λπ.)

– την επεξεργασία των μητρώων ελέγχου και τη εξασφάλιση αντιγράφου ασφαλείας της βάσης δεδομένων του συστήματος της ΥΔΚ.

- Διαχειριστές συστήματος ΑΠ

[Δύο άτομα αναλαμβάνουν καθήκοντα διαχειριστή συστήματος της ΑΠ, το ένα από τα οποία ενεργεί ως αναπληρωτής.] Οι διαχειριστές συστήματος της ΑΠ διορίζονται από την ΑΛ της ΑΠ και είναι υπεύθυνοι για:

– τη διατήρηση της ορθής λειτουργίας και των ορθών παραμέτρων του υλισμικού και του λογισμικού που χρησιμοποιούνται στην ΑΠ CommisSign

– τη δημιουργία αντιγράφων ασφαλείας του συστήματος της ΑΠ CommisSign.

5.2.1.2.Θέσεις εμπιστοσύνης ΑΚ:

Δύο τουλάχιστον άτομα αναλαμβάνουν καθήκοντα ΑΚ και είναι υπεύθυνα για:

- την αποδοχή και την επεξεργασία αιτημάτων σχετικά με τα πιστοποιητικά [ανάκληση/αναστολή ισχύος πιστοποιητικών][και αιτημάτων ανάκτησης κλειδιού],

- την επαλήθευση της ταυτότητας των αιτούντων
- τη διαβίβαση πληροφοριών σχετικά με τους αιτούντες στην ΑΠ
- την παραλαβή και διανομή πληροφοριών σχετικά με την εξουσιοδότηση των συνδρομητών

5.2.1.3.Θέσεις εμπιστοσύνης ΤΑΚ:

Τουλάχιστον δύο άτομα σε κάθε Γενική Διεύθυνση ή αυτόνομη οντότητα (αντιπροσωπείες κ.λπ.) αναλαμβάνουν καθήκοντα ΤΑΚ και είναι υπεύθυνα για:

- την αποδοχή και την επεξεργασία αιτημάτων σχετικά με τα πιστοποιητικά
- τη διαβίβαση πληροφοριών σχετικά με τους αιτούντες στην ΑΠ
- την παραλαβή πληροφοριών από την ΑΚ σχετικά με την εξουσιοδότηση των συνδρομητών
- την επαλήθευση της ταυτότητας και της φυσικής παρουσίας των αιτούντων
- την ενημέρωση των συνδρομητών σχετικά με την εξουσιοδότησή τους
- την παροχή βοήθειας προς τους συνδρομητές κατά τη διαδικασία δημιουργίας κλειδιών και πιστοποιητικών.

5.2.2. Απαιτούμενος αριθμός ατόμων ανά εργασία

Οι παρακάτω εργασίες χαρακτηρίζονται ευαίσθητες και για την εκτέλεσή τους απαιτούνται τουλάχιστον δύο άτομα.

Δύο στελέχη ΑΠ απαιτούνται για:

- την προσθήκη και τη διαγραφή άλλων στελεχών ΑΠ και ΑΚ
- τον καθορισμό των προκαθορισμένων ιδιοτήτων των πιστοποιητικών

Η ΤΑΚ και ο υπεύθυνος ασφάλειας είναι αρμόδιοι για:

- την ανάκτηση κλειδιού

5.2.3. Ταυτοποίηση και επαλήθευση ταυτότητας ανά θέση

Για την ταυτοποίηση και την επαλήθευση της ταυτότητας του προσωπικού των ΑΚ και ΤΑΚ ισχύουν οι απαιτήσεις που ορίζονται στο τμήμα 5.3.

Εφόσον λάβουν εξουσιοδότηση τα συγκεκριμένα μέλη του προσωπικού, τους χορηγείται πιστοποιητικό και έξυπνη κάρτα, με τα οποία αναγνωρίζεται και επαληθεύεται η ταυτότητά τους από το σύστημα της ΑΠ CommisSign. Επιπλέον, καταχωρούνται στη βάση δεδομένων της ΑΠ CommisSign με διευκρινίσεις σχετικά με τη θέση και τις αρμοδιότητές τους. Κατά την

εκτέλεση ευαίσθητων λειτουργιών, η ταυτότητα του προσωπικού των ΑΚ και ΤΑΚ αναγνωρίζεται μέσω έξυπνης κάρτας.

5.3. Έλεγχοι ασφάλειας του προσωπικού

5.3.1. Απαιτήσεις σχετικά με το ιστορικό, τα τυπικά προσόντα, την εμπειρία και την αξιοπιστία

[Τα μέλη του προσωπικού που πληρούν αυτές τις θέσεις έχουν υποβληθεί επιτυχώς στον έλεγχο ιστορικού που προβλέπεται για την ανάληψη κρίσιμων-ευαίσθητων θέσεων. Οι θέσεις των κύριων χρηστών ΑΠ, των στελεχών ΑΠ και της ΑΚ θεωρούνται κρίσιμες και ευαίσθητες με διαβάθμιση υψηλού κινδύνου. Οι ΤΑΚ θεωρούνται κρίσιμες και ευαίσθητες θέσεις με διαβάθμιση μέσου κινδύνου.]

5.3.2. Διαδικασία ελέγχου ιστορικού

Όλοι οι έλεγχοι ιστορικού διενεργούνται σύμφωνα με τις πολιτικές ασφάλειας του προσωπικού της Ευρωπαϊκής Επιτροπής και των ευρωπαϊκών κυβερνήσεων.

5.3.3. Απαιτήσεις κατάρτισης

Στα μέλη του προσωπικού που αναλαμβάνουν καθήκοντα σχετικά με τις λειτουργίες των ΑΠ, ΑΚ και ΤΑΚ παρέχεται:

- κατάρτιση σχετικά με τη λειτουργία του λογισμικού και/ή του υλισμικού που χρησιμοποιείται στο σύστημα της ΑΠ CommisSign
- κατάρτιση σχετικά με τα καθήκοντα τα οποία αναμένεται να εκτελέσουν
- ενημέρωση σχετικά με τις απαιτήσεις της παρούσας ΔΠΠ και της πολιτικής πιστοποιητικών για την ΥΔΚ της Ευρωπαϊκής Επιτροπής

5.3.4. Απαιτήσεις και συχνότητα επιμόρφωσης

Οι απαιτήσεις του προηγούμενου τμήματος ενημερώνονται, ώστε το προσωπικό να είναι σε θέση να ανταποκρίνεται στις αλλαγές του συστήματος της ΑΠ CommisSign. Τα σεμινάρια επιμόρφωσης διεξάγονται σύμφωνα με τις αλλαγές αυτές.

5.3.5. Εναλλαγή θέσεων εργασίας

Δεν προβλέπεται.

5.3.6. Κυρώσεις για μη εξουσιοδοτημένες ενέργειες

Σε περίπτωση εκτέλεσης ή υποψίας εκτέλεσης μη εξουσιοδοτημένης ενέργειας από άτομο το οποίο εκτελεί καθήκοντα σχετικά με τη λειτουργία της ΑΠ CommisSign ή των ΑΚ, λαμβάνονται πειθαρχικά μέτρα (σύμφωνα με τον κανονισμό της Ευρωπαϊκής Επιτροπής).

Η παράβαση των διατάξεων της παρούσας ΔΠΠ ή της πολιτικής πιστοποιητικών της Ευρωπαϊκής Επιτροπής είτε λόγω αμέλειας είτε εκ

προθέσεως συνεπάγεται ανάκληση των προνομίων και/ή διοικητικές κυρώσεις.

5.3.7. Προσωπικό εργολάβων

Οι υπάλληλοι εργολάβων που απασχολούνται σε οποιοδήποτε τμήμα λειτουργίας της ΑΠ CommisSign ή των ΑΚ υπόκεινται στα ίδια κριτήρια με τους μονίμους υπαλλήλους της Ευρωπαϊκής Επιτροπής και η αξιοπιστία τους ελέγχεται ανάλογα με το επίπεδο της θέσης την οποία αναλαμβάνουν, όπως ορίζεται στο τμήμα 5.3.

5.3.8. Τεκμηρίωση που παρέχεται στο προσωπικό

Η παρούσα ΔΠΠ είναι διαθέσιμη στο προσωπικό της ΑΠ CommisSign και της ΑΚ και στους συνδρομητές. Εγχειρίδια χειρισμού βρίσκονται στη διάθεση του προσωπικού των ΑΠ και ΑΚ, προκειμένου να λειτουργούν και να συντηρούν το υλισμικό και το λογισμικό της ΥΔΚ.

Πέραν της παρούσας ΔΠΠ, στους συνδρομητές παρέχονται πληροφορίες σχετικά με τη χρήση και την προστασία του λογισμικού που χρησιμοποιείται στο πλαίσιο του τομέα της Ευρωπαϊκής Επιτροπής και η ΑΠ CommisSign παρέχει βοήθεια σε όλους τους χρήστες του τομέα μέσω γραφείου τεχνικής υποστήριξης.

6. ΤΕΧΝΙΚΟΙ ΕΛΕΓΧΟΙ ΑΣΦΑΛΕΙΑΣ

6.1. Δημιουργία και εγκατάσταση ζεύγους κλειδιών

6.1.1. Δημιουργία ζεύγους κλειδιών

Το ζεύγος κλειδιών υπογραφής της ΑΠ CommisSign δημιουργείται κατά την αρχική έναρξη λειτουργίας της εφαρμογής κύριου ελέγχου της ΑΠ και προστατεύεται από το κύριο κλειδί της ΑΠ.

Για τους χρήστες, το ζεύγος κλειδιών της ψηφιακής υπογραφής δημιουργείται από το λογισμικό πελάτη της ΥΔΚ. Τα κλειδιά που δημιουργούνται από λογισμικό αποθηκεύονται σε αρχείο στο σκληρό δίσκο ή σε δισκέτα.

6.1.2. Παράδοση ιδιωτικού κλειδιού στις οντότητες

Για το ζεύγος κλειδιών ψηφιακής υπογραφής δεν απαιτείται παράδοση του ιδιωτικού κλειδιού, δεδομένου ότι το ζεύγος κλειδιών δημιουργείται από το λογισμικό χρήστη του συνδρομητή.

6.1.3. Παράδοση δημόσιου κλειδιού στους εκδότες πιστοποιητικών

Το δημόσιο κλειδί επαλήθευσης της ψηφιακής υπογραφής παραδίδεται με ασφαλή τρόπο στο σύστημα της ΑΠ CommisSign μέσω πρωτοκόλλου ασφαλούς επικοινωνίας.

6.1.4. Παράδοση δημόσιου κλειδιού της ΑΠ στους χρήστες

Το δημόσιο κλειδί επαλήθευσης της ΑΠ CommisSign παραδίδεται στους συνδρομητές με ένα πιστοποιητικό ΑΠ μέσω πρωτοκόλλου ασφαλούς επικοινωνίας. Η ΑΠ CommisSign εξασφαλίζει την παράδοση του δημόσιου κλειδιού σε εξωτερικά συμβαλλόμενα μέρη με πιστοποιητικό ΑΠ, το οποίο βρίσκεται σε έναν εξυπηρετητή παγκόσμιου ιστού της Ευρωπαϊκής Επιτροπής μέσω πρωτοκόλλου ασφαλούς επικοινωνίας.

6.1.5. Μήκη ασύμμετρων κλειδιών

Τα ζεύγη κλειδιών υπογραφής χρήστη είναι 1024 δυφία RSA.

Το ζεύγος κλειδιών υπογραφής της ΑΠ CommisSign είναι 1024 δυφία RSA. Τα κλειδιά συνόδου του πρωτοκόλλου ασφαλούς επικοινωνίας είναι Triple DES.

6.1.6. Δημιουργία παραμέτρων δημόσιου κλειδιού

Δεν προβλέπεται.

6.1.7. Έλεγχος ποιότητας παραμέτρων

Δεν προβλέπεται.

6.1.8. Δημιουργία κλειδιών υλισμικού/λογισμικού

Το κύριο κλειδί της ΑΠ CommisSign αποθηκεύεται στο υλισμικό. Τα κλειδιά όλων των άλλων οντοτήτων δημιουργούνται από το λογισμικό πελάτη της ΥΔΚ.

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

Το ζεύγος κλειδιών ψηφιακής υπογραφής χρησιμοποιείται για να διασφαλίζεται η αυθεντικότητα, η ακεραιότητα και η υποστήριξη υπηρεσιών χωρίς άρνηση αναγνώρισης.

Το ζεύγος κλειδιών κρυπτογράφησης χρησιμοποιείται για την προστασία ενός συμμετρικού κλειδιού το οποίο χρησιμοποιείται για την κρυπτογράφηση δεδομένων και ως εκ τούτου παρέχει υπηρεσίες εμπιστευτικότητας.

Το κλειδί υπογραφής της ΑΠ CommisSign χρησιμοποιείται για την υπογραφή των πιστοποιητικών, των ΚΑΠ [και ΚΑΕ] που εκδίδονται από την εν λόγω ΑΠ. Τα κλειδιά συνόδου του πρωτοκόλλου ασφαλούς επικοινωνίας χρησιμοποιούνται για την εξασφάλιση ασφαλούς επικοινωνίας κατά τη διαχείριση των κλειδιών.

Προσωρινά, υπάρχει μόνο ένα ζεύγος κλειδιών.

6.2. Προστασία ιδιωτικού κλειδιού

Ακολουθεί περιγραφή των τεχνικών και διαδικαστικών μεθόδων προστασίας του ιδιωτικού κλειδιού. Τα μέτρα προστασίας που αναφέρονται δεν

απαλλάσσουν τους συνδρομητές από τη δική τους ευθύνη να προστατεύουν τα ιδιωτικά κλειδιά τους από ενδεχόμενη αποκάλυψη.

6.2.1. Πρότυπα κρυπτογραφικής ενότητας

Η κρυπτογραφική ενότητα που χρησιμοποιείται από το λογισμικό του τομέα της ΑΠ CommisSign CA συμμορφώνεται με [.....]

6.2.2. Πολυπρόσωπος έλεγχος ιδιωτικού κλειδιού

Για την ανάκτηση ιδιωτικού κλειδιού απαιτείται έλεγχος από περισσότερα του ενός άτομα (βλ. τμήμα «Απαιτούμενος αριθμός ατόμων ανά εργασία»).

6.2.3. Μεσεγγύηση ιδιωτικού κλειδιού

Δεν προβλέπεται μεσεγγύηση ιδιωτικών κλειδιών από εξωτερικό τρίτο.

6.2.4. Εφεδρικό ιδιωτικό κλειδί

Τα ιδιωτικά κλειδιά της ΑΠ CommisSign βρίσκονται στη βάση δεδομένων του συστήματος της ΑΠ CommisSign. Εφεδρικό ιδιωτικό κλειδί υπογραφής συνδρομητή δεν δημιουργείται ποτέ στο σύστημα της ΑΠ CommisSign, ώστε να εξασφαλίζεται υποστήριξη υπηρεσιών χωρίς άρνηση αναγνώρισης. [Η βάση δεδομένων του συστήματος της ΑΠ CommisSign κρυπτογραφείται.] [Αντίγραφο ασφαλείας της βάσης δεδομένων του συστήματος της ΑΠ CommisSign δημιουργείται κάθε βράδυ.]

6.2.5. Αρχειοθέτηση ιδιωτικού κλειδιού

Για πληροφορίες σχετικά με την αρχειοθέτηση κλειδιού, βλ. τμήμα 4.6 της παρούσας ΔΠΠ.

6.2.6. Καταχώριση ιδιωτικού κλειδιού στην κρυπτογραφική ενότητα

Το ιδιωτικό κλειδί υπογραφής της ΑΠ CommisSign και το ιδιωτικό κλειδί υπογραφής του συνδρομητή δημιουργούνται από το λογισμικό, στο πλαίσιο της κρυπτογραφικής ενότητας, και δεν καταχωρούνται στην ενότητα από άλλες οντότητες.

Τα ιδιωτικά κλειδιά αποθηκεύονται κρυπτογραφημένα στην κρυπτογραφική ενότητα και αποκρυπτογραφούνται μόνον όταν χρησιμοποιούνται.

6.2.7. Μέθοδος ενεργοποίησης ιδιωτικού κλειδιού

Τα ιδιωτικά κλειδιά ενεργοποιούνται κατά τη σύνδεση του συνδρομητή με το κρυπτογραφικό λογισμικό πελάτη. Η σύνδεση έχει τη μορφή κωδικού πρόσβασης, ο οποίος προστατεύεται από ενδεχόμενη αποκάλυψη κατά την πληκτρολόγησή του.

6.2.8. Μέθοδος απενεργοποίησης ιδιωτικού κλειδιού

Τα ιδιωτικά κλειδιά παραμένουν ενεργά καθ' όλη τη διάρκεια της σύνδεσης. Η σύνδεση λήγει είτε με τη διακοπή της από το συνδρομητή είτε με την απενεργοποίηση του κλειδιού του συνδρομητή.

6.2.9. Μέθοδος καταστροφής ιδιωτικού κλειδιού

Η οριστική καταστροφή των ιδιωτικών κλειδιών επιτυγχάνεται με ασφαλείς λειτουργίες διαγραφής.

6.3. Άλλες πτυχές της διαχείρισης ζεύγους κλειδιών

6.3.1. Αρχειοθέτηση δημόσιου κλειδιού

Για τη δημιουργία εφεδρικού κλειδιού και την αρχειοθέτηση κλειδιού βλ. τμήμα 6.2.

6.3.2. Διάρκεια χρήσης δημόσιων και ιδιωτικών κλειδιών

Δημόσιο κλειδί και πιστοποιητικό της ΑΠ CommisSign– [10 έτη]

Ιδιωτικό κλειδί υπογραφής της ΑΠ CommisSign–[10 έτη]

Δημόσιο κλειδί επαλήθευσης και πιστοποιητικό συνδρομητή – δύο έτη

6.4. Δεδομένα ενεργοποίησης

6.4.1. Δημιουργία και εγκατάσταση δεδομένων ενεργοποίησης

Κωδικοί πρόσβασης ή έξυπνες κάρτες απαιτούνται από όλες τις οντότητες που συνδέονται στο λογισμικό της ΥΔΚ. Το λογισμικό εφαρμόζει ένα αυστηρό σύνολο κανόνων σε κάθε κωδικό πρόσβασης ώστε να εξασφαλίζεται η ασφάλειά του. Οι κωδικοί πρόσβασης είναι υποχρεωτικοί για την ΑΠ. Οι ΑΚ και ΤΑΚ προστατεύονται με έξυπνη κάρτα.

Σύμφωνα με τους κανόνες που εφαρμόζονται κατά την επιλογή κωδικού πρόσβασης, ο κωδικός πρόσβασης:

- πρέπει να έχει τουλάχιστον δώδεκα χαρακτήρες
- πρέπει να περιέχει τουλάχιστον ένα κεφαλαίο γράμμα, έναν ειδικό χαρακτήρα και ένα ψηφίο
- πρέπει να περιέχει τουλάχιστον ένα πεζό γράμμα
- δεν πρέπει να περιέχει πολλές επαναλήψεις του ίδιου χαρακτήρα
- δεν πρέπει να είναι ίδιος με το όνομα του προφίλ της οντότητας
- δεν πρέπει να περιέχει μακροσκελή υποστοιχειοσειρά του ονόματος του προφίλ της οντότητας.

Τα δεδομένα που απαιτούνται για την εγκαινίαση του συνδρομητή περιγράφονται στο τμήμα 4.2 της παρούσας ΔΠΠ.

6.4.2. Προστασία δεδομένων ενεργοποίησης

Τα ονόματα χρήστη και οι τιμές ελέγχου κωδικού πρόσβασης του διαχειριστή συστήματος εξυπηρετητή της ΑΠ CommisSign, των στελεχών

της ΑΠ και των ΑΚ αποθηκεύονται στη βάση δεδομένων του συστήματος της ΑΠ CommisSign.

6.4.3. Άλλες πτυχές των δεδομένων ενεργοποίησης

Δεν προβλέπονται

6.5. Έλεγχοι ασφάλειας ηλεκτρονικών υπολογιστών

6.5.1. Ειδικές τεχνικές απαιτήσεις για την ασφάλεια των ηλεκτρονικών υπολογιστών

[Το σύστημα της ΑΠ CommisSign παρέχει την ακόλουθη λειτουργικότητα μέσω του λειτουργικού συστήματος και ενός συνδυασμού του λειτουργικού συστήματος, του λογισμικού της ΑΠ CommisSign και υλικών ελέγχων:

- έλεγχος πρόσβασης στις υπηρεσίες της ΑΠ και στις θέσεις της ΥΔΚ
- αναγκαστικός διαχωρισμός καθηκόντων των διαφόρων θέσεων της ΥΔΚ
- ταυτοποίηση και επαλήθευση των θέσεων της ΥΔΚ και των αντίστοιχων ταυτοτήτων
- χρήση κρυπτογραφίας για την ασφάλεια της βάσης δεδομένων και της επικοινωνίας μέσω συνόδων
- αρχειοθέτηση του ιστορικού της ΑΠ και των τελικών οντοτήτων και των δεδομένων των ελέγχων
- έλεγχος συμβάντων που αφορούν την ασφάλεια
- μηχανισμοί ανάκτησης κλειδιών και του συστήματος της ΑΠ.

Πληροφορίες σχετικά με αυτή τη λειτουργικότητα παρέχονται στα αντίστοιχα τμήματα της παρούσας ΔΠΠ.

6.5.2. Χαρακτηρισμός ασφάλειας ηλεκτρονικών υπολογιστών

Δεν προβλέπεται.

6.6. Έλεγχοι ασφάλειας του κύκλου ζωής

6.6.1. Έλεγχοι ανάπτυξης του συστήματος

Δεν προβλέπονται.

6.6.2. Έλεγχοι διαχείρισης ασφάλειας

Στους ελέγχους διαχείρισης ασφάλειας για την ΑΠ CommisSign περιλαμβάνονται:

- ο μηχανισμός και/ή οι πολιτικές που εφαρμόζονται για τον έλεγχο και την παρακολούθηση των παραμέτρων του συστήματος ΑΠ

- ο εξοπλισμός της ΑΠ CommisSign, ο οποίος είναι ειδικά σχεδιασμένος για τη λειτουργία υποδομής διαχείρισης κλειδιού

- στον εξοπλισμό της ΑΠ CommisSign δεν είναι εγκατεστημένες εφαρμογές ή υποπρογράμματα τα οποία δεν αποτελούν μέρος των παραμέτρων της ΑΠ, με εξαίρεση το λογισμικό προστασίας από ιούς και

- η αναβάθμιση του εξοπλισμού της ΑΠ CommisSign διεξάγεται από έμπιστα και καταρτισμένα μέλη του προσωπικού με καθορισμένο τρόπο.

6.7. Έλεγχοι ασφάλειας δικτύου

[Η εξ αποστάσεως πρόσβαση στο σύστημα της ΑΠ CommisSign εξασφαλίζεται μέσω ενός πρωτοκόλλου ασφαλούς επικοινωνίας. Δεν επιτρέπεται καμία άλλη εξ αποστάσεως πρόσβαση, ενώ δυνατότητες όπως το εισερχόμενο FTP είναι απενεργοποιημένες. Είναι κλειστές όλες οι θύρες TCP/IP, εκτός από όσες απαιτούνται για τον έλεγχο ενεργοποιημένων συμβάντων της ΥΔΚ και τον έλεγχο όλων των αποτυχημένων λειτουργιών και των σπανίως επιτυχών λειτουργιών.]

6.8. Έλεγχοι σχεδιασμού της κρυπτογραφικής ενότητας

Η κρυπτογραφική ενότητα του λογισμικού της ΥΔΚ είναι σχεδιασμένη με τρόπον ώστε να συμμορφώνεται με [.....] Το κύριο κλειδί της ΑΠ CommisSign είναι αποθηκευμένο σε διάταξη υλισμικού που συμμορφώνεται με [.....]

Η κρυπτογραφική ενότητα για τη δημιουργία κλειδιών που χρησιμοποιείται από το λογισμικό της ΥΔΚ είναι σχεδιασμένη με τρόπον ώστε να συμμορφώνεται με [.....]

7. ΠΡΟΦΙΛ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΚΑΙ ΚΑΠ

7.1. Προφίλ πιστοποιητικών

7.1.1. Αριθμός έκδοσης

Η ΑΠ CommisSign χορηγεί πιστοποιητικά X.509 έκδοσης 3 σύμφωνα με το προφίλ πιστοποιητικών και ΚΑΠ PKIX. Υποστηρίζονται τα ακόλουθα πεδία X.509:

Πεδία	**Περιγραφή**
έκδοση:	το πεδίο έκδοσης ορίζεται σε v3
αύξων αριθμός:	όταν δημιουργείται ένα νέο πιστοποιητικό χρήστη, από το σύστημα της ΑΠ CommisSign δημιουργείται ένας μοναδικός αύξων αριθμός στο πλαίσιο του τομέα ασφάλειας της ΑΠ CommisSign

Πεδία	Περιγραφή
αλγόριθμος υπογραφής:	το αναγνωριστικό για τον αλγόριθμο που χρησιμοποιείται από την ΑΠ CommisSign για την υπογραφή του πιστοποιητικού
εκδότης:	το διακεκριμένο όνομα (DN) του εκδότη του πιστοποιητικού της ΑΠ CommisSign
ισχύς:	διάρκεια ισχύος πιστοποιητικού – ορίζονται η ημερομηνία έναρξης και η ημερομηνία λήξης της ισχύος (notBefore και notAfter)
υποκείμενο:	διακεκριμένο όνομα (DN) του υποκείμενου του πιστοποιητικού
στοιχεία δημόσιου κλειδιού:	αναγνωριστικό αλγορίθμου Δημόσιο κλειδί
Αποτύπωμα αλγορίθμου:	Αναγνωριστικό αλγορίθμου
Αποτύπωμα	

7.1.2. Επεκτάσεις πιστοποιητικών

Δεν υποστηρίζονται επεκτάσεις.

7.1.3. Αναγνωριστικό αλγορίθμου αντικειμένου

Η ΑΠ CommisSign υποστηρίζει τους ακόλουθους αλγορίθμους:

Αλγόριθμος	Αναγνωριστικό αντικειμένου	Εκδίδουσα αρχή
SHA1WithRSAEncryption	1 2 840 113549 1 1 5	UTIMACO
DES-EDE3-CBC	1 2 840 113549 3 7	UTIMACO

7.1.4. Μορφές ονομάτων

Σε κάθε πιστοποιητικό, τα πεδία DN εκδότη και DN υποκειμένου περιέχουν το πλήρες διακεκριμένο όνομα (DN) X.500 του εκδότη του πιστοποιητικού ή του υποκειμένου του πιστοποιητικού.

7.1.5. Περιορισμοί στα ονόματα

Δεν εφαρμόζονται περιορισμοί στα ονόματα από την ΑΠ CommisSign.

7.1.6. Αναγνωριστικό πολιτικής πιστοποιητικών αντικειμένου

Δεν προβλέπεται.

7.1.7. Χρήση επέκτασης περιορισμών στην πολιτική

Δεν εφαρμόζονται περιορισμοί στην πολιτική από την ΑΠ CommisSign.

7.1.8. Σύνταξη και σημασιολογία χαρακτηρισμών πολιτικής

Δεν προβλέπεται.

7.1.9. Σημασιολογία επεξεργασίας για την πολιτική κρίσιμων πιστοποιητικών

[Η μόνη επέκταση πιστοποιητικού η οποία μπορεί να χαρακτηριστεί κρίσιμη στα πιστοποιητικά που χορηγούνται από την ΑΠ CommisSign είναι η επέκταση cRLDistributionPoints. Η ΚΑΠ και η ΚΑΕ ανακτώνται από την καταχώρηση καταλόγου του σημείου διανομής ΚΑΠ που αναφέρεται στο πιστοποιητικό, εκτός εάν στο λογισμικό πελάτη του συνδρομητή είναι προσωρινά αποθηκευμένο το τρέχον αντίγραφο της ίδιας ΚΑΠ ή ΚΑΕ.]

7.2. Προφίλ της ΚΑΠ [προς επανεξέταση μετά την υλοποίηση]

7.2.1. Αριθμός έκδοσης

Οι ΚΑΠ που εκδίδονται από την ΑΠ CommisSign CA είναι ΚΑΠ X.509 έκδοσης 2 σύμφωνα με το προφίλ πιστοποιητικών και ΚΑΠ PKIX.

Ακολουθεί κατάλογος των πεδίων που χρησιμοποιούνται από την ΑΠ CommisSign στο μορφότυπο ΚΑΠ X.509 έκδοση 2:

Πεδία	**Περιγραφή**
Έκδοση	ορίζεται σε v2
Υπογραφή	αναγνωριστικό του αλγορίθμου που χρησιμοποιείται για την υπογραφή της ΚΑΠ
Εκδότης	το πλήρες διακεκριμένο όνομα (DN) της ΑΠ CommisSign
τρέχουσα ενημέρωση	χρόνος έκδοσης της ΚΑΠ
επόμενη ενημέρωση	χρόνος επόμενης αναμενόμενης ενημέρωσης της ΚΑΠ
ανακλημένα πιστοποιητικά	κατάσταση ανακλημένων πιστοποιητικών

7.2.2. ΚΑΠ και πεδία επέκτασης ΚΑΠ

Στο ακόλουθο τμήμα περιγράφονται οι ΚΑΠ X.509 έκδοση 2 και τα πεδία επέκτασης ΚΑΠ που υποστηρίζονται από την ΑΠ CommisSign, καθώς και οι ΚΑΠ X.509 έκδοση 2 και τα πεδία επέκτασης ΚΑΠ που δεν υποστηρίζονται στις ΚΑΠ που εκδίδονται από την ΑΠ CommisSign.

7.2.2.1.Επεκτάσεις που υποστηρίζονται

Στον παρακάτω πίνακα παρουσιάζονται οι ΚΑΠ και τα πεδία επέκτασης ΚΑΠ που υποστηρίζονται από την ΑΠ CommisSign.

ΕΠΕΚΤΑΣΗ	**ΚΡΙΣΙΜΗ/ ΜΗ ΚΡΙΣΙΜΗ**	**ΠΡΟΑΙΡΕΤΙΚΗ**	**ΠΑΡΑΤΗΡΗΣΕΙΣ**
AuthorityKeyIdentifier	Μη κρίσιμη	Μη προαιρετική	Συμπληρώνεται μόνο το στοιχείο [0] (authorityKeyIdentifier) Περιέχει τεμάχιο 20 byte του subjectPublicKeyInfo στο πιστοποιητικό της ΑΠ
CRLNumber particular	Μη κρίσιμη	Μη προαιρετική	Αυξάνεται με κάθε αλλαγή ΚΑΠ/ΚΑΕ
ReasonCode	Μη κρίσιμη	Μη προαιρετική	πεδίο επέκτασης ΚΑΠ – επί του παρόντος υποστηρίζονται μόνον οι κωδικοί αιτίας (0), (1), (3), (4) και (5)
IssuingDistributionPoint	Κρίσιμη	Μη προαιρετική	Το στοιχείο [0] (distributionPoint) περιέχει το πλήρες DN του σημείου διανομής Το στοιχείο [1] (onlyContainsUserCerts) περιλαμβάνεται για τις ΚΑΠ Το στοιχείο [2] (onlyContainsCACerts) περιλαμβάνεται για τις ΚΑΕ Τα στοιχεία [1] και [2] δεν εμφανίζονται ποτέ ταυτόχρονα στην ίδια κατάσταση ανάκλησης Τα στοιχεία [3] και [4] δεν χρησιμοποιούνται

7.2.2.2.Επεκτάσεις που δεν υποστηρίζονται

Η ΑΠ CommisSign δεν υποστηρίζει τις ακόλουθες επεκτάσεις ΚΑΠ X.509 έκδοση 2:

- εναλλακτικό όνομα εκδότη
- κωδικός εντολής διατήρησης
- ημερομηνία λήξης
- εκδότης πιστοποιητικού
- δείκτης ΚΑΠ δέλτα

8. ΔΙΑΧΕΙΡΙΣΗ ΠΡΟΔΙΑΓΡΑΦΩΝ

8.1. Διαδικασίες αλλαγής προδιαγραφών

Η παρούσα ΔΠΠ επανεξετάζεται εξ ολοκλήρου ετησίως. Σφάλματα, ενημερώσεις ή προτεινόμενες αλλαγές στο παρόν έγγραφο γνωστοποιούνται στον υπεύθυνο επικοινωνίας που αναφέρεται στο τμήμα 1.4.

8.1.1. Στοιχεία που μπορούν να αλλάξουν χωρίς προειδοποίηση

Αλλαγές σε στοιχεία της παρούσας ΔΠΠ τα οποία, κατά την κρίση της ΑΑΠ, έχουν μηδενικό ή ελάχιστο αντίκτυπο στους χρήστες και στους αμοιβαία πιστοποιημένους τομείς ΑΠ που χρησιμοποιούν πιστοποιητικά και ΚΑΠ που εκδίδονται στο πλαίσιο της παρούσας ΔΠΠ, μπορούν να πραγματοποιηθούν χωρίς αλλαγή του αριθμού έκδοσης του εγγράφου και χωρίς προειδοποίηση των χρηστών.

8.1.2. Αλλαγές κατόπιν προειδοποίησης

Αλλαγές στην πολιτική πιστοποιητικών που υποστηρίζεται από την παρούσα ΔΠΠ, καθώς και αλλαγές σε στοιχεία της παρούσας ΔΠΠ τα οποία, κατά την κρίση της ΑΑΠ, έχουν σημαντικό αντίκτυπο στους χρήστες και στους αμοιβαία πιστοποιημένους τομείς ΑΠ που χρησιμοποιούν πιστοποιητικά και ΚΑΠ που εκδίδονται στο πλαίσιο της παρούσας ΔΠΠ, πραγματοποιούνται κατόπιν προειδοποίησης των χρηστών 30 ημέρες νωρίτερα, ενώ αυξάνεται αναλόγως ο αριθμός έκδοσης του παρόντος εγγράφου.

8.1.2.1.Κατάλογος στοιχείων

Τα στοιχεία της παρούσας ΔΠΠ ενδέχεται να εμπίπτουν στις απαιτήσεις προειδοποίησης που ορίζονται στα τμήματα 8.1.1 και 8.1.2 «Στοιχεία που μπορούν να αλλάξουν χωρίς προειδοποίηση» και «Αλλαγές κατόπιν προειδοποίησης».

8.1.2.2.Μηχανισμός προειδοποίησης

Τριάντα ημέρες πριν την πραγματοποίηση σημαντικών αλλαγών στην παρούσα ΔΠΠ, οι επικείμενες αλλαγές δημοσιεύονται στον ιστοχώρο της ΑΠ CommisSign και διαβιβάζονται στους αμοιβαία πιστοποιημένους οργανισμούς ΑΠ μέσω ασφαλούς ηλεκτρονικού ταχυδρομείου. Η ανακοίνωση περιλαμβάνει δήλωση των προτεινόμενων αλλαγών, προθεσμία παραλαβής παρατηρήσεων και προτεινόμενη ημερομηνία θέσης σε ισχύ των αλλαγών. Η ΑΑΠ μπορεί να ζητήσει από τις ΑΠ να προειδοποιήσουν τους συνδρομητές τους σχετικά με τις προτεινόμενες αλλαγές.

8.1.2.3.Περίοδος σχολιασμού

Η διάρκεια της περιόδου σχολιασμού είναι 30 ημέρες, εκτός εάν ορίζεται διαφορετικά. Η περίοδος σχολιασμού ορίζεται στην ανακοίνωση.

8.1.2.4.Μηχανισμός χειρισμού των παρατηρήσεων

Οι παρατηρήσεις σχετικά με τις προτεινόμενες αλλαγές πρέπει να απευθύνονται στην ΑΛ της ΑΠ και να περιλαμβάνουν περιγραφή της αλλαγής, δικαιολόγηση της αλλαγής, στοιχεία επικοινωνίας με τον αιτούντα την αλλαγή και την υπογραφή του.

Η ΑΛ κάνει δεκτές με ή χωρίς τροποποιήσεις ή απορρίπτει τις προτεινόμενες αλλαγές μετά την πάροδο της περιόδου σχολιασμού. Οι απόψεις της ΑΛ σχετικά με τις προτεινόμενες αλλαγές εξετάζονται από κοινού με την ΑΑΠ της Ευρωπαϊκής Επιτροπής. Οι αποφάσεις σχετικά με τις προτεινόμενες αλλαγές λαμβάνονται κατά την κρίση της ΑΛ και της ΑΑΠ.

8.1.2.5.Περίοδος προειδοποίησης για τις τελικές αλλαγές

Η ΑΛ καθορίζει την περίοδο προειδοποίησης για τις τελικές αλλαγές.

8.1.2.6.Στοιχεία των οποίων η αλλαγή απαιτεί νέα πολιτική

Σε περίπτωση κατά την οποία η ΑΑΠ αποφασίζει την αλλαγή κάποιας πολιτικής, προκειμένου να κατοχυρωθεί η έκδοση της νέας πολιτικής η ΑΑΠ εκχωρεί νέο αναγνωριστικό αντικειμένου (OID) στην τροποποιημένη πολιτική.

8.2. Πολιτικές δημοσίευσης και ανακοίνωσης

Η ΑΛ δημοσιεύει την παρούσα ΔΠΠ και την πολιτική πιστοποιητικών της ΥΔΚ της Ευρωπαϊκής Επιτροπής στον ιστοχώρο της ΑΠ CommisSign. Διαβιβάζει επίσης πληροφορίες μέσω ηλεκτρονικού ταχυδρομείου κατόπιν αιτήματος.

8.3. Διαδικασίες έγκρισης ΔΠΠ

Η ΑΑΠ της Ευρωπαϊκής Επιτροπής κρίνει κατά πόσον η ΔΠΠ της ΑΠ της Ευρωπαϊκής Επιτροπής συμμορφώνεται με την πολιτική πιστοποιητικών της ΥΔΚ της Ευρωπαϊκής Επιτροπής.

9. ΠΑΡΑΡΤΗΜΑΤΑ

9.1. Ακρωνύμια

ΑΑΠ	Αρχή για την άσκηση πολιτικής
ΑΚ	Αρχή καταχώρισης
ΑΛ	Αρχή λειτουργίας
ΑΠ	Αρχή πιστοποίησης
ΓΔ	Γενική Διεύθυνση
ΔΠΠ	Δήλωση για την πρακτική πιστοποίησης
ΚΑΕ	Κατάσταση ανάκλησης εξουσιοδοτήσεων
ΚΑΠ	Κατάσταση ανάκλησης πιστοποιητικών
ΤΑΚ	Τοπική αρχή καταχώρισης
TCP/IP	Πρωτόκολλο ελέγχου μετάδοσης/Πρωτόκολλο Internet (Transmission Control Protocol/Internet Protocol)
ΥΔΚ	Υποδομή δημόσιου κλειδιού
URL	Ομοιόμορφος εντοπιστής πόρου (Unified Resource Locator)

9.2. Ορισμοί

Αναγνωριστικό αντικειμένου (OID). Το μοναδικό αλφαριθμητικό/αριθμητικό αναγνωριστικό που καταχωρείται στο πλαίσιο του προτύπου καταχώρισης ISO ως παραπομπή σε συγκεκριμένο αντικείμενο ή κατηγορία αντικειμένων.

Ανάδοχος. Ανάδοχος στο πλαίσιο της ΥΔΚ της Ευρωπαϊκής Επιτροπής είναι το τμήμα ή ο υπάλληλος της Ευρωπαϊκής Επιτροπής που δηλώνει ως υποψήφιο για χορήγηση πιστοποιητικού ένα συγκεκριμένο άτομο ή οργανισμό, π.χ. για έναν υπάλληλο ανάδοχος μπορεί να είναι ο προϊστάμενός του. Ο ανάδοχος οφείλει να ενημερώνει την ΑΠ ή την ΑΚ σχετικά με τη λήξη ή την αλλαγή της εργασιακής σχέσης με το συνδρομητή, ώστε το πιστοποιητικό να ανακαλείται ή να ενημερώνεται.

Αρχή για την άσκηση πολιτικής. Όργανο της Ευρωπαϊκής Επιτροπής αρμόδιο για τη λήψη, υλοποίηση και διαχείριση πολιτικών αποφάσεων σχετικά με την πολιτική πιστοποιητικών και τις δηλώσεις για την πρακτική πιστοποίησης για το σύνολο της ΥΔΚ της Ευρωπαϊκής Επιτροπής.

Αρχή καταχώρισης (ΑΚ). Οντότητα αρμόδια για την ταυτοποίηση και την επαλήθευση της ταυτότητας των συνδρομητών πιστοποιητικών πριν τη

χορήγηση των πιστοποιητικών, η οποία ωστόσο δεν υπογράφει ούτε χορηγεί τα πιστοποιητικά (δηλαδή, στην ΑΚ ανατίθενται ορισμένες εργασίες από την ΑΠ).

Αρχή λειτουργίας ΑΠ. Η αρχή λειτουργίας της ΑΠ είναι αρμόδια για την εκπόνηση και τη διαχείριση της δήλωσης πρακτικής της ΑΠ και για τη διαχείριση του κύριου κλειδιού.

Αρχή πιστοποίησης. Αρχή την οποία εμπιστεύονται ένας ή περισσότεροι χρήστες για την έκδοση και τη διαχείριση πιστοποιητικών δημόσιου κλειδιού X.509 και ΚΑΠ

Δεδομένα ενεργοποίησης. Δεδομένα προσωπικού χαρακτήρα, εκτός των κλειδιών, τα οποία απαιτούνται για την πρόσβαση σε κρυπτογραφικές ενότητες.

Διαχειριστές ΑΠ. Οι διαχειριστές του συστήματος της ΑΠ είναι υπεύθυνοι για τη διατήρηση της ορθής λειτουργίας και των ορθών παραμέτρων του υλισμικού και του λογισμικού της ΑΠ CommisSign και για τη δημιουργία αντιγράφων ασφαλείας του συστήματος της ΑΠ CommisSign.

Εκδίδουσα ΑΠ. Στο πλαίσιο ενός συγκεκριμένου πιστοποιητικού, η εκδίδουσα ΑΠ είναι η ΑΠ η οποία υπογράφει και εκδίδει το εν λόγω πιστοποιητικό.

Επιχειρησιακή αρχή. Προσωπικό αρμόδιο για τη γενική λειτουργία της ΑΠ στο πλαίσιο της ΥΔΚ της Ευρωπαϊκής Επιτροπής. Η αρμοδιότητά της καλύπτει τομείς όπως στελέχωση, οικονομικά και επίλυση διαφορών. Για την εκτέλεση των καθηκόντων της η επιχειρησιακή αρχή δεν απαιτείται να έχει λογαριασμό στο σταθμό εργασίας της ΑΠ.

Ζώνη υψηλής ασφάλειας. Περιοχή, η πρόσβαση στην οποία ελέγχεται μέσω σημείου εισόδου και περιορίζεται σε εξουσιοδοτημένα μέλη του προσωπικού, τα οποία υποβάλλονται σε ενδεδειγμένο έλεγχο, και σε αρμοδίως συνοδευόμενους επισκέπτες. Οι ζώνες υψηλής ασφάλειας πρέπει να χωρίζονται με περίμετρο. Παρακολουθούνται 24 ώρες το εικοσιτετράωρο και 7 ημέρες την εβδομάδα από προσωπικό ασφάλειας, προσωπικό άλλης ειδικότητας ή ηλεκτρονικά μέσα.

Κατάλογος. Σύστημα καταλόγων που συμμορφώνεται με τη σειρά συστάσεων X.500 της ITU-T.

Κατάσταση ανάκλησης εξουσιοδοτήσεων (ΚΑΕ). Κατάσταση ανακλημένων πιστοποιητικών ΑΠ. Η ΚΑΕ είναι μια κατάσταση ανάκλησης πιστοποιητικών (ΚΑΠ) για αμοιβαία πιστοποιητικά ΑΠ.

Κατάσταση ανάκλησης πιστοποιητικών (ΚΑΠ). Κατάσταση ανακλημένων πιστοποιητικών που δημιουργείται και υπογράφεται από την ΑΠ που έχει εκδώσει τα πιστοποιητικά. Όταν ένα πιστοποιητικό ανακαλείται (π.χ. γιατί υπάρχουν υποψίες αλλοίωσης του κλειδιού), προστίθεται στην κατάσταση. Σε ορισμένες περιπτώσεις η ΑΠ μπορεί να επιλέξει να διαιρέσει την ΚΑΠ σε μια σειρά μικρότερων ΚΑΠ.

Κύριοι χρήστες ΑΠ. Οι κύριοι χρήστες της ΑΠ είναι εξουσιοδοτημένοι για τη δημιουργία και συντήρηση του κύριου κλειδιού της ΑΠ CommisSign, την αλλαγή των κωδικών πρόσβασης στον εξυπηρετητή της ΑΠ και την ανάκτηση του κωδικού πρόσβασης των στελεχών της ΑΠ σε περίπτωση που τον έχουν ξεχάσει.

MD5. Ένας από τους αλγορίθμους σύνοψης μηνύματος που έχει αναπτύξει η RSA Data Security Inc.

Οντότητα. Οποιοδήποτε αυτόνομο στοιχείο στο πλαίσιο της ΥΔΚ. Μπορεί να είναι ΑΠ, ΑΚ ή τελική οντότητα.

Οργανισμός. Τμήμα, υπηρεσία, ανώνυμη εταιρεία, προσωπική εταιρία, συνασπισμός επιχειρήσεων, μεικτή εταιρεία ή άλλος συνεταιρισμός.

Πιστοποιητικό. Το δημόσιο κλειδί του χρήστη, μαζί με ορισμένα άλλα στοιχεία, το οποίο καθίσταται απρόσβλητο έναντι παραχαράξεων μέσω της ψηφιακής υπογραφής του με το ιδιωτικό κλειδί της αρχής πιστοποίησης που το εξέδωσε. Ο μορφότυπος του πιστοποιητικού συμμορφώνεται με τη σύσταση X.509 της ITU-T.

Προσωπικό της Ευρωπαϊκής Επιτροπής. Στο προσωπικό της Ευρωπαϊκής Επιτροπής ανήκουν τα άτομα που απασχολούνται από την Ευρωπαϊκή Επιτροπή. Αμείβονται με μισθό και κατέχουν μόνιμες θέσεις που συνεπάγονται την εκτέλεση καθηκόντων και την ανάληψη ευθυνών στο πλαίσιο της Ευρωπαϊκής Επιτροπής.

Στελέχη ΑΠ. Τα στελέχη ΑΠ είναι υπεύθυνα για τη λειτουργία και τη διαχείριση του εξυπηρετητή και του λογισμικού της ΑΠ.

Στελέχη ΥΔΚ. Κάθε άτομο εξουσιοδοτημένο να εκτελεί τα καθήκοντα που προβλέπονται για τη λειτουργία μιας ΥΔΚ.

Συμβαλλόμενο μέρος. Άτομο το οποίο χρησιμοποιεί πιστοποιητικό υπογεγραμμένο από μια ΑΠ στο πλαίσιο της ΥΔΚ της Ευρωπαϊκής Επιτροπής για να επικυρώνει μια ψηφιακή υπογραφή ή να κρυπτογραφεί μηνύματα που απευθύνει στο υποκείμενο του πιστοποιητικού, και είναι συνδρομητής ΑΠ στο πλαίσιο της ΥΔΚ της Ευρωπαϊκής Επιτροπής ή μιας ΥΔΚ αμοιβαία πιστοποιημένης με την ΥΔΚ της Ευρωπαϊκής Επιτροπής.

Συνδρομητής. Άτομο ή οργανισμός του οποίου το δημόσιο κλειδί πιστοποιείται με πιστοποιητικό δημόσιου κλειδιού. Στο πλαίσιο της ΥΔΚ της Ευρωπαϊκής Επιτροπής μπορεί να είναι υπάλληλος της Ευρωπαϊκής Επιτροπής ή εργολάβου της. Οι συνδρομητές μπορεί να έχουν ένα ή περισσότερα πιστοποιητικά από μια συγκεκριμένη ΑΠ με την οποία συνδέονται. Οι περισσότεροι διαθέτουν τουλάχιστον δύο ενεργά πιστοποιητικά, από τα οποία το ένα περιέχει το κλειδί επαλήθευσης της ψηφιακής υπογραφής τους και το άλλο, το κλειδί κρυπτογράφησης εμπιστευτικών πληροφοριών.

Τελική οντότητα. Οντότητα που χρησιμοποιεί τα κλειδιά και τα πιστοποιητικά που δημιουργούνται στο πλαίσιο της ΥΔΚ για σκοπούς εκτός

της διαχείρισης των προαναφερθέντων κλειδιών και πιστοποιητικών. Η τελική οντότητα μπορεί να είναι συνδρομητής ή συμβαλλόμενο μέρος.

Υπάλληλος. Κάθε άτομο το οποίο απασχολείται από την Ευρωπαϊκή Επιτροπή.

Υποδομή δημόσιου κλειδιού. Ένα δομημένο σύνολο υλισμικού, λογισμικού, προσώπων και πολιτικών που χρησιμοποιεί τεχνολογία ψηφιακής υπογραφής για να παράσχει στα συμβαλλόμενα μέρη τη δυνατότητα επαλήθευσης της σύνδεσης του δημόσιου συστατικού στοιχείου ενός ασύμμετρου ζεύγους κλειδιών με ένα συγκεκριμένο συνδρομητή.

Ψηφιακή υπογραφή. Το αποτέλεσμα της μετατροπής ενός μηνύματος μέσω ενός κρυπτογραφικού συστήματος που χρησιμοποιεί κλειδιά, έτσι ώστε το άτομο που έχει το αρχικό μήνυμα να μπορεί να προσδιορίσει:

(1) κατά πόσον η μετατροπή πραγματοποιήθηκε μέσω του κλειδιού που αντιστοιχεί στο κλειδί του υπογράφοντος και

(2) κατά πόσον το μήνυμα αλλοιώθηκε μετά τη μετατροπή του.

9.3. Έγγραφα αναφοράς

[EA1] Πολιτική ασφάλειας ΤΕΠ

[EA2] Αίτηση για σχολιασμό RFC 2527

[EA3] Κανονισμός αριθ. 45/2001 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 18ης Δεκεμβρίου