JCC Payment Systems Ltd.

ΠΟΛΙΤΙΚΗ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΓΙΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΑΥΘΕΝΤΙΚΟΠΟΙΗΣΗΣ ΚΑΙ ΕΓΚΕΚΡΙΜΕΝΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΓΡΑΦΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΦΡΑΓΙΔΩΝ

Ισχύει από: 03 Ιουνίου 2025

Version 1.3

Ιστορικό Εγγράφου

Έκδοση	Ημερομηνία	Συγγραφέας	Λόγος Αλλαγής
1.0	20/07/2021	Πάρης Ερωτόκριτου	Αρχική έκδοση
1.1	03/06/2023	Πάρης Ερωτόκριτου	Αναθεώρηση, καμία αλλαγή
1.2	03/06/2024	Φανή Ευσταθίου	Αναθεώρηση, καμία αλλαγή
1.3	03/06/2025	Φανή Ευσταθίου	Αναθεώρηση, καμία αλλαγή

Εγκρίσεις Εγγράφου

Έκδοση	Ημερομηνία	Εγκρίθηκε από
1.0	20/07/2021	Διεύθυνση Πολιτικών Παρόχου Υπηρεσιών Εμπιστοσύνης
1.1	03/06/2023	Διεύθυνση Πολιτικών Παρόχου Υπηρεσιών Εμπιστοσύνης
1.2	03/06/2024	Μαρία Καλλή
1.3	03/06/2025	Μαρία Καλλή

Κατάλογος Διανομής Εγγράφου

Έκδοση	Date	Role/Name
1.0	20/07/2021	Όλο το προσωπικό παρόχου υπηρεσιών εμπιστοσύνης
1.1	03/06/2023	Όλο το προσωπικό παρόχου υπηρεσιών εμπιστοσύνης
1.2	03/06/2024	Όλο το προσωπικό παρόχου υπηρεσιών εμπιστοσύνης
1.3	03/06/2025	Όλο το προσωπικό παρόχου υπηρεσιών εμπιστοσύνης

Η Πολιτική Πιστοποιητικών της JCC Payment Systems Ltd για πιστοποιητικά αυθεντικοποίησης και για εγκεκριμένα πιστοποιητικά ηλεκτρονικών υπογραφών & ηλεκτρικών σφραγίδων.

Ανακοινώσεις περί εμπορικών σημάτων

Η JCC Payment Systems αποτελεί το κατατεθέν σήμα της JCC Payment Systems Ltd. Άλλες επωνυμίες δύνανται να αποτελούν εμπορικά σήματα των αντίστοιχων κατόχων αυτών.

Χωρίς περιορισμό επί των επιφυλασσόμενων ανωτέρω δικαιωμάτων και με εξαίρεση τις κατωτέρω επιτρεπόμενες περιπτώσεις, κανένα τμήμα της παρούσας δημοσίευσης δεν δύναται να αναπαραχθεί, να αποθηκευτεί ή να εισαχθεί σε σύστημα ανάκτησης ή να μεταδοθεί σε οποιαδήποτε μορφή ή με

οποιοδήποτε μέσο (μέσω ηλεκτρονικής, μηχανικής μετάδοσης, φωτοτύπησης, εγγραφής ή άλλου μέσου) χωρίς την πρότερη γραπτή άδεια της JCC Payment Systems Ltd.

Κατά παρέκκλιση των ανωτέρω, η άδεια χορηγείται για την αναπαραγωγή και διανομή της παρούσας Δήλωσης Πρακτικών Πιστοποίησης της JCC Payment Systems Ltd σε μη αποκλειστική βάση και άνευ υποχρέωσης καταβολής δικαιωμάτων με την προϋπόθεση ότι: (i) η ανωτέρω ανακοίνωση περί πνευματικής ιδιοκτησίας και οι αρχικές παράγραφοι αναγράφονται ευκρινώς σε κάθε αντίγραφο και (ii) το παρόν έγγραφο αναπαράγεται με ακρίβεια στο σύνολό του και ολοκληρώνεται με την απόδοση του εγγράφου στην JCC Payment Systems Ltd..

Τα αιτήματα για οποιαδήποτε άλλη άδεια αναπαραγωγής της παρούσας Δήλωσης Πρακτικών Πιστοποίησης της JCC Payment Systems (καθώς και αιτήματα για χορήγηση αντιγράφων από την JCC Payment Systems.) πρέπει να αποστέλλονται στην JCC Payment Systems., Σταδίου 1, 2571 Νήσου, Βιομηχανική Περιοχή, Λευκωσία, Κύπρος α Υπόψη: Αρχή Διαχείρισης Πολιτικών. Τηλ.: (+357) 22 868 500, Φαξ: (+357) 22 868 591, Email: trust-policies@jcc.com.cy

Table of Contents

1 ΕΙΣΑΓΩΓΗ

Το παρόν έγγραφο αποτελεί την Πολιτική Πιστοποιητικού της JCC Payment Systems Ltd (εφεξής «ΠΠ») για πιστοποιητικά αυθεντικοποίησης και για Εγκεκριμένα Πιστοποιητικά Ηλεκτρονικών Υπογραφών και Ηλεκτρονικών Σφραγίδων. Δηλώνει τις πρακτικές που εφαρμόζει ο Πάροχος Υπηρεσιών Εμπιστοσύνης (εφεξής «ΠΥΕ») της JCC Payment Systems σχετικά με την παροχή των πιστοποιητικών αυθεντικοποίησης και εγκεκριμένων πιστοποιητικών ηλεκτρονικών υπογραφών & ηλεκτρονικών σφραγίδων, σύμφωνα με, αλλά όχι περιοριστικά, τα Άρθρα 19, 24, 28, 38 και 45 του Κανονισμού (ΕΕ) Αρ. 910/2014 [eIDAS].

Το παρόν έγγραφο καθορίζει τις επιχειρηματικές, νομικές και τεχνικές απαιτήσεις για την έγκριση, έκδοση, διαχείριση, χρήση, ανάκληση και ανανέωση ψηφιακών πιστοποιητικών και την παροχή σχετικών υπηρεσιών εμπιστοσύνης. Αυτές οι απαιτήσεις ισχύουν για όλες τις Αρχές Πιστοποίησης (ΑΠ), τις Αρχές Εγγραφής (ΑΕ), τα Κέντρα Επεξεργασίας, τους Συνεργάτες, τους Συνδρομητές, τα Εμπιστευόμενα Μέρη και άλλες οντότητες ΥΔΚ που συνεργάζονται με την ΥΔΚ της JCC.

Αυτή η ΠΠ περιγράφει πώς η JCC Payment Systems πληρεί αυτές τις απαιτήσεις σύμφωνα με τον Κανονισμό (ΕΕ) αριθ. 910/2014 και περιγράφει τις πρακτικές και διαδικασίες που χρησιμοποιεί η JCC Payment Systems για:

- Ασφαλή διαχείριση της σχετικής υποδομής που υποστηρίζει την ΥΔΚ της JCC,
- Έκδοση, διαχείριση, ανάκληση και ανανέωση Εγκεκριμένων Πιστοποιητικών όπως ορίζεται στον Κανονισμό (ΕΕ) αριθ. 910/2014 και
- Έκδοση, διαχείριση, ανάκληση και ανανέωση πιστοποιητικών αυθεντικοποίησης και Ευρωπαϊκών Εγκεκριμένων Πιστοποιητικών Ηλεκτρονικής Υπογραφής για την Εθνική Ηλεκτρονική Ταυτότητα της Κύπρου

Αυτή η ΠΠ συμμορφώνεται με το RFC 3647 της Internet Engineering Task Force (IETF) για την κατασκευή της Δήλωσης Πρακτικών Πιστοποίησης.

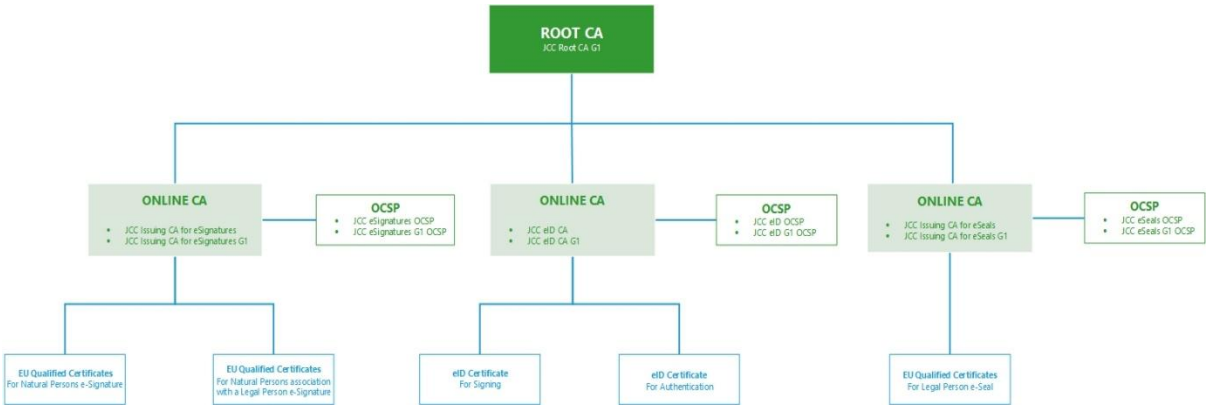
Η Διοίκηση μπορεί να κάνει εξαιρέσεις από αυτήν τη Δήλωση Πρακτικών Πιστοποίησης σε ατομική βάση, προκειμένου να μετριάσει ουσιαστικές, επικείμενες επιπτώσεις για τους πελάτες, συνεργάτες, εμπιστευόμενα μέρη και/ή άλλους εντός του οικοσυστήματος πιστοποιητικών, όταν δεν υπάρχουν πρακτικές λύσεις. Οποιεσδήποτε τέτοιες εξαιρέσεις από τη διοίκηση καταγράφονται, παρακολουθούνται και αναφέρονται ως μέρος της διαδικασίας ελέγχου.

1.1 *Επισκόπηση*

Αυτή η ΠΠ περιγράφει και ορίζει τις διαδικαστικές και επιχειρησιακές απαιτήσεις που καθορίζονται από τον Κανονισμό (ΕΕ) Αρ. 910/2014, τις οποίες ακολουθεί η JCC Payment Systems για την έκδοση, τη συντήρηση και τη διαχείριση του κύκλου ζωής των πιστοποιητικών αυθεντικοποίησης και των Εγκεκριμένων Πιστοποιητικών Ηλεκτρονικών Υπογραφών και ηλεκτρονικών σφραγίδων.

Οι εν λόγω πρακτικές και διαδικασίες συμμορφώνονται με το πρότυπο πολιτικής του Ευρωπαϊκού Ινστιτούτου Τηλεπικοινωνιακών Προτύπων ETSI EN 319 411-2 : «QCP-n-qsc d» για τα Εγκεκριμένα Πιστοποιητικά ηλεκτρονικών υπογραφών και την Πολιτική Πιστοποιητικού: QCP-l-qscd για τα Εγκεκριμένα Πιστοποιητικά ηλεκτρονικών σφραγίδων και το πρότυπο πολιτικής ETSI EN 319 411-1: εκτεταμένη κανονικοποιημένη πολιτική πιστοποιητικού (NCP+)

Η JCC Payment Systems εφαρμόζει την ακόλουθη σειρά έκδοσης πιστοποιητικού:



Η ΔΠΠ εφαρμόζεται ειδικά στις Αρχές Έκδοσης Πιστοποιητικών (Issuing CAs) της JCC Payment Systems, οι οποίες εκδίδουν:

- Εγκεκριμένα Πιστοποιητικά της ΕΕ για ηλεκτρονικές υπογραφές
- Εγκεκριμένα Πιστοποιητικά της ΕΕ για ηλεκτρονικές σφραγίδες
- Πιστοποιητικά Αυθεντικοποίησης για αυθεντικοποίηση

Οι Ιδιωτικές Αρχές Πιστοποίησης (Private CAs) ή οι υπηρεσίες που παρέχονται από την JCC Payment Systems σε άλλους Οργανισμούς εμπίπτουν επίσης στο πεδίο εφαρμογής της παρούσας ΠΠ.

Η JCC Payment Systems δημοσιεύει αυτή τη ΠΠ προκειμένου να συμμορφωθεί με τις συγκεκριμένες απαιτήσεις πολιτικής της ισχύουσας νομοθεσίας ή άλλων προτύπων και απαιτήσεων της βιομηχανίας.

Η ΠΠ αποτελεί μόνο ένα έγγραφο από το σύνολο εγγράφων που σχετίζονται με τις Υπηρεσίες Εμπιστοσύνης της JCC Payment Systems .

Τα εν λόγω έγγραφα περιλαμβάνουν τα εξής:

- Βοηθητικά εμπιστευτικά έγγραφα για την ασφάλεια και επιχειρησιακά έγγραφα[3] τα οποία συμπληρώνουν τη ΠΠ παρέχοντας πιο αναλυτικές απαιτήσεις, όπως τα εξής:
  - τον Οδηγό αναφοράς διαδικασίας παραγωγής κλειδιών, ο οποίος παρουσιάζει αναλυτικά τις λειτουργικές απαιτήσεις διαχείρισης των κλειδιών,

[3] Αν και τα συγκεκριμένα έγγραφα δεν διατίθενται στο ευρύ κοινό, οι προδιαγραφές τους περιλαμβάνονται στην Έκθεση Αξιολόγησης Συμμόρφωσης της JCC Payment Systems για τους Παρόχους Υπηρεσιών Εμπιστοσύνης που εκδίδουν Εγκεκριμένα Πιστοποιητικά και δύνανται να είναι διαθέσιμα στον πελάτη βάσει ειδικής συμφωνίας.

- την Πολιτική φυσικής και περιβαλλοντικής ασφάλειας της JCC Payment Systems η οποία ορίζει τις αρχές για την ασφάλεια που διέπουν την υποδομή της JCC Payment Systems,
- την Πολιτική ασφάλειας πληροφοριών της JCC Payment Systems η οποία δηλώνει τις απαιτήσεις όσον αφορά την υποδομή των Πληροφοριακών Συστημάτων για την ασφαλή λειτουργία και σύμφωνα με τις σχετικές νομοθετικές και συμβατικές απαιτήσεις,
- την Πολιτική διαχείρισης κρυπτογραφικών κλειδιών της JCC Payment Systems , η οποία παρουσιάζει αναλυτικά τις λειτουργικές απαιτήσεις διαχείρισης κλειδιών,

- την Δήλωση Πρακτικών Πιστοποίησης για τα Εγκεκριμένα Πιστοποιητικά της ΕΕ για ηλεκτρονικές υπογραφές & ηλεκτρονικές σφραγίδες
- την Δήλωση Πρακτικών Πιστοποίησης για την Εθνική Ηλεκτρονική Ταυτότητα
- τους Γενικούς Όρους και Προϋποθέσεις που επιβάλλονται από την JCC Payment Systems
  Οι συγκεκριμένοι Γενικοί Όροι και Προϋποθέσεις δεσμεύουν τους Πελάτες, τους Συνδρομητές και τα Βασιζόμενα Μέρη της JCC Payment Systems. Μεταξύ άλλων, οι Γενικοί Όροι και Προϋποθέσεις καλύπτουν ένα ευρύ φάσμα εμπορικών όρων ή ειδικών όρων που αφορούν τις Υπηρεσίες Εμπιστοσύνης της JCC Payment Systems.

Σε πολλές περιπτώσεις, η ΠΠ αναφέρεται στα συγκεκριμένα βοηθητικά έγγραφα για συγκεκριμένες, αναλυτικές πρακτικές για την εφαρμογή των πολιτικών της JCC Payment Systems όπου η συμπερίληψη των λεπτομερειών στη ΠΠ θα μπορούσε να διακυβεύσει την ασφάλεια της Αρχής Πιστοποίησης (ΑΠ) της JCC Payment Systems.

1.2 *Όνομα εγγράφου και Αναγνώριση*

Οι Αρχές Πιστοποίησης (ΑΠ) της JCC Payment Systems εκδίδονται με βάση τα ακόλουθα Αναγνωριστικά Αντικειμένου:

1.3.6.1.4.1.56511	Αναγνωριστικό αντικειμένου (OID) της JCC Payment Systems, καταχωρισμένη στο IANA
1.3.6.1.4.1.56511.1	Πάροχος Υπηρεσιών Εμπιστοσύνης
1.3.6.1.4.1.56511.1.1	Πολιτική Πιστοποίησης (ΠΠ) για Υπηρεσίες Εμπιστοσύνης
1.3.6.1.4.1.56511.1.1.1	Δήλωση Πρακτικών Πιστοποίησης (ΔΠΠ) για Εγκεκριμένα Πιστοποιητικά Ηλεκτρονικών Υπογραφών και Ηλεκτρονικών Σφραγίδων
1.3.6.1.4.1.56511.1.1.2	Δήλωση Πρακτικών Πιστοποίησης (ΔΠΠ) για την Κυπριακή Ηλεκτρονική Ταυτότητα
1.3.6.1.4.1.56511.1.1.1.0	Εγκεκριμένο Πιστοποιητικό Ηλεκτρονικής Υπογραφής QCP-n-qscd (0.4.0.194112.1.2)
1.3.6.1.4.1.56511.1.1.1.1	Εγκεκριμένο Πιστοποιητικό Ηλεκτρονικής Σφραγίδας QCP-l-qscd (0.4.0.194112.1.3)
1.3.6.1.4.1.56511.1.1.2.1	Πιστοποιητικό Υπογραφής της Ηλεκτρονικής Ταυτότητας QCP-n-qscd (0.4.0.194112.1.2)
1.3.6.1.4.1.56511.1.1.2.2	Πιστοποιητικό Αυθεντικοποίησης NCP+ (0.4.0.2042.1.2)

Η ισχύουσα και τρέχουσα ΠΠ (OID) θα εισάγεται μέσω αναφοράς σε κάθε Πολιτική Πιστοποιητικού που διέπεται από την ΠΠ της JCC Payment Systems.
Τα Αναγνωριστικά Αντικειμένων Πολιτικής Πιστοποιητικού (OID) χρησιμοποιούνται σύμφωνα με την παράγραφο 7.1.

1.3 *Συμμετέχοντες στην Υποδομή Δημόσιου Κλειδιού (ΥΔΚ)*

1.3.1 Αρχές Πιστοποίησης

Η αρχή την οποία εμπιστεύονται οι χρήστες των υπηρεσιών πιστοποίησης (δηλαδή οι συνδρομητές, καθώς και τα βασιζόμενα μέρη) για τη δημιουργία και την έκδοση πιστοποιητικών ονομάζεται Αρχή Πιστοποίησης (ΑΠ).

Η ΑΠ έχει τη συνολική ευθύνη για την παροχή των υπηρεσιών πιστοποίησης.

Η εν λόγω ιεραρχία ΑΠ αποτελείται από τις παρακάτω οντότητες:

ΑΠ Βάσης (Root)

A/A	Subject Distinguished Name	Certificate SHA-256 Fingerprint
1	CN=JCC Root CA G1 O = JCC PAYMENT SYSTEMS LTD C = CY	B55650C17CBCF1D4F8A38F0C0A58F434495941077A93E762D6C9E69D87A04351

Εκδότριες ΑΠ

A/A	Subject Distinguished Name	Certificate SHA-256 Fingerprint
1.	CN = JCC Issuing CA for eSignatures 2.5.4.97 = VATCY-10029914L O = JCC PAYMENT SYSTEMS LTD C = CY	0cf19de62187d68a51a8d0defd42f71ff73841300109c6647e7a05533bb8b3fa
2.	CN = JCC Issuing CA for eSeals 2.5.4.97 = VATCY-10029914L O = JCC PAYMENT SYSTEMS LTD C = CY	8522c10f0820633961bcf64f8d0eca32821d1a892ba6edc9cd469c265dd4f534
3.	CN = JCC Issuing CA for	8404181ebd08f48d07066ae7fdaacdd1fda1567da6ea1cc208ceae9f64727458

	eSignatures G1 2.5.4.97 = VATCY-10029914L O = JCC PAYMENT SYSTEMS LTD C = CY	
4.	CN = JCC Issuing CA for eSeals G1 2.5.4.97 = VATCY-10029914L O = JCC PAYMENT SYSTEMS LTD C = CY	17e473dc97721a8fddd4668c3c9e4e328a653f2a508a0819c5b2aa0dacfa0662
5.	CN = JCC eID CA 2.5.4.97 = VATCY-10029914L O = JCC PAYMENT SYSTEMS LTD C = CY	8653a6b2ec8aa847706c2d4048b58861cafaedca333b2c145e96111e966f8740
6.	CN = JCC eID CA G1 2.5.4.97 = VATCY-10029914L O = JCC PAYMENT SYSTEMS LTD C = CY	c23d300b481fce5440098e78edcdd9ff01e501471683b6ead8d9d893c18ee04e

1.3.2 Αρχές Εγγραφής

Η Αρχή Εγγραφής είναι μια οντότητα που διενεργεί την ταυτοποίηση και την επικύρωση των Συνδρομητών για την έκδοση Πιστοποιητικών, προβαίνει σε ή αποδέχεται αιτήσεις ανάκλησης πιστοποιητικών και εγκρίνει αιτήσεις για την επαναδημιουργία κλειδιών πιστοποιητικών για λογαριασμό της ΑΠ. Η JCC Payment Systems ενεργεί ως ΑΕ για όλα τα Πιστοποιητικά που εκδίδει.

Η JCC Payment Systems έχει την εξουσία να συνάψει συμβατική σχέση με ένα ή περισσότερα τρίτα μέρη προκειμένου να αναθέσει μέρος των αρμοδιοτήτων της ΑΕ, ειδικότερα όσον αφορά την ταυτοποίηση του Συνδρομητή και του Υποκείμενου. Στην περίπτωση αυτή, το τρίτο μέρος αποτελεί μια Τοπική Αρχή Εγγραφής (ΤΑΕ). Η ΤΑΕ εκπληρώνει τις αρμοδιότητές της σύμφωνα με την παρούσα ΠΠ, την ισχύουσα ΔΠΠ, τα σχετικά Σχέδια Ταυτοποίησης και τους όρους της Σύμβασης ΤΑΕ που υπεγράφη μεταξύ της ΤΑΕ και της JCC Payment Systems.

Η JCC Payment Systems εκπαιδεύει το εξουσιοδοτημένο προσωπικό όσον αφορά τη διαδικασία ταυτοποίησης και τις διαδικασίες ασφαλείας πριν από την έναρξη των σχετικών δραστηριοτήτων της ΤΑΕ. Σε μεταγενέστερο στάδιο, η JCC Payment Systems επανεκπαιδεύει σε ετήσια βάση τους εξουσιοδοτημένους υπαλλήλους της ΤΑΕ.

Η JCC Payment Systems διενεργεί ετησίως ελέγχους στις δραστηριότητες και διαδικασίες της ΤΑΕ προκειμένου να διασφαλίσει τη συμμόρφωση με την παρούσα ΠΠ, την ισχύουσα ΔΠΠ, τα Σχέδια Ταυτοποίησης και τη Σύμβαση ΤΑΕ.

Τρίτα μέρη τα οποία συνάπτουν συμβατική σχέση με τη JCC Payment Systems, μπορούν να λειτουργούν τη δική τους ΑΕ και να επιτρέπουν την έκδοση πιστοποιητικών από μια ΑΠ της JCC Payment Systems. Οι ΑΕ τρίτων μερών θα πρέπει να συμμορφώνονται με όλες τις απαιτήσεις της παρούσας ΠΠ, της ισχύουσας ΔΠΠ, τα Σχέδια Ταυτοποίησης και τους όρους της Σύμβασης ΑΕ που υπογράφεται μεταξύ της ΑΕ και της JCC Payment Systems.

Η επαλήθευση του μέρους του domain της διεύθυνσης email δεν μπορεί να ανατεθεί σε τρίτο μέρος και επικυρώνεται μόνο από την ΑΕ της Εκδρότριας Αρχής Πιστοποίησης (ΑΠ).

1.3.3 Τοπικές Αρχές Εγγραφής

Μια Τοπική Αρχή Εγγραφής είναι μια οντότητα που διενεργεί την ταυτοποίηση και την επικύρωση των Συνδρομητών και των Υποκειμένων, καθώς και την αρχική εξέταση των σχετικών εγγράφων τους για την έκδοση, την επαναδημιουργία κλειδιών και την ανάκληση Πιστοποιητικών. Η σχέση μεταξύ της ΤΑΕ και της ΑΕ περιγράφεται στη σύμβαση της ΤΑΕ και περιλαμβάνει, μεταξύ άλλων, τα ακόλουθα:

- τα πλήρη στοιχεία των εξουσιοδοτημένων υπαλλήλων της ΤΑΕ οι οποίοι θα εκτελούν τα καθήκοντα και τις δραστηριότητες της ΤΑΕ·
- την υποχρέωση της ΤΑΕ οι εξουσιοδοτημένοι υπάλληλοί της να λαμβάνουν εκπαίδευση από την JCC Payment Systems αναφορικά με τα καθήκοντα και τις δραστηριότητες της ΤΑΕ, καθώς και να αποδέχεται τη διενέργεια ετήσιων ελέγχων από την JCC Payment Systems αναφορικά με τις λειτουργίες και της διαδικασίες της ΤΑΕ·
- την υποχρέωση των εξουσιοδοτημένων υπαλλήλων της ΤΑΕ να χρησιμοποιούν πιστοποιητικά που εκδίδονται από την ΑΠ της JCC Payment Systems προκειμένου να διασφαλιστεί η ασφαλής επικοινωνία μεταξύ των μερών·
- την υποχρέωση της ΤΑΕ να διεκπεραιώνει τις αιτήσεις των Συνδρομητών αποκλειστικά μέσω των εξουσιοδοτημένων υπαλλήλων της ΤΑΕ.

Η Τοπική Αρχή Εγγραφής υποβάλλει όλες τις αιτήσεις ή τα αιτήματα του Συνδρομητή, συνοδευόμενα με τα σχετικά έγγραφα, στην Αρχή Εγγραφής (ΑΕ) προς έγκριση ή απόρριψη όσον αφορά την έκδοση, την επαναδημιουργία κλειδιών ή την ανάκληση Πιστοποιητικών.

Η JCC Payment Systems λειτουργεί επίσης ως Τοπική Αρχή Εγγραφής για όλες τις ταυτοποιήσεις και επικυρώσεις των Συνδρομητών και των Υποκειμένων.

1.3.4 Συνδρομητές

Δύο διαφορετικοί όροι χρησιμοποιούνται στην παρούσα ΠΠ για να γίνει διάκριση μεταξύ των δύο αυτών ρόλων: Ο «Συνδρομητής» φέρει την τελική ευθύνη για τη χρήση του διαπιστευτηρίου αλλά το Υποκείμενο είναι το άτομο του οποίου η ταυτότητα επαληθεύεται όταν το διαπιστευτήριο προσκομίζεται.

Με τον όρο «Συνδρομητής» νοείται είτε ένα φυσικό είτε νομικό πρόσωπο στο οποίο η JCC Payment Systems παρέχει Υπηρεσίες Εμπιστοσύνης σύμφωνα με την παρούσα ΠΠ και την ισχύουσα ΔΠΠ.

Ο όρος «Υποκείμενο» νοείται:

- ένα φυσικό πρόσωπο,
- ένα φυσικό πρόσωπο που προσδιορίζεται σε σχέση με ένα νομικό πρόσωπο,
- ένα νομικό πρόσωπο.

Ο Συνδρομητής μπορεί να είναι ή να μην είναι το Υποκείμενο ενός πιστοποιητικού. Η σύνδεση μεταξύ του Συνδρομητή και του Υποκειμένου είναι μία από τις εξής:

- Για την αίτηση πιστοποιητικού για φυσικό πρόσωπο, ο Συνδρομητής είναι:
  α) το ίδιο το φυσικό πρόσωπο.
  β) ένα φυσικό πρόσωπο που έχει εξουσιοδοτηθεί να εκπροσωπεί το Υποκείμενο.
  γ) οποιαδήποτε οντότητα με την οποία το φυσικό πρόσωπο συνδέεται.

- Για την αίτηση πιστοποιητικού για νομικό πρόσωπο, ο Συνδρομητής είναι:
  α) οποιαδήποτε οντότητα επιτρέπεται από το σχετικό νομικό σύστημα να εκπροσωπεί το νομικό πρόσωπο.
  β) ένας νομικός εκπρόσωπος του νομικού προσώπου που εγγράφεται για θυγατρικές ή μονάδες ή τμήματα αυτού.

1.3.5 Βασιζόμενα Μέρη

Ως «Βασιζόμενο Μέρος» νοείται ένα άτομο ή οντότητα που ενεργεί βάσει ενός πιστοποιητικού και/ή ψηφιακής υπογραφής που έχει εκδοθεί υπό την ΑΠ. Το Βασιζόμενο Μέρος δύναται να είναι ή όχι Συνδρομητής.

1.3.6 Άλλοι Συμμετέχοντες

Δεν εφαρμόζεται.

1.4 *Χρήση Πιστοποιητικού*

Ένα Ψηφιακό Πιστοποιητικό είναι μορφοποιημένα δεδομένα που κρυπτογραφικά συνδέουν έναν αναγνωρισμένο Συνδρομητή με ένα Δημόσιο Κλειδί. Ένα Ψηφιακό Πιστοποιητικό επιτρέπει σε μια οντότητα που συμμετέχει σε μια ηλεκτρονική συναλλαγή να αποδείξει την ταυτότητά της σε άλλους συμμετέχοντες σε αυτή τη συναλλαγή. Τα Εγκεκριμένα Πιστοποιητικά για ηλεκτρονικές υπογραφές χρησιμοποιούνται συνήθως από φυσικά πρόσωπα για την υπογραφή και την κρυπτογράφηση ηλεκτρονικού ταχυδρομείου, καθώς και για σκοπούς αυθεντικοποίησης, υπό την προϋπόθεση ότι η χρήση δεν απαγορεύεται από το νόμο, από αυτή τη ΠΠ, από την ισχύουσα ΔΠΠ κάτω από την οποία εκδώθηκε το πιστοποιητικό και από οποιεσδήποτε συμφωνίες με τους Συνδρομητές.

Τα Εγκεκριμένα Πιστοποιητικά για ηλεκτρονικές σφραγίδες εκδίδονται σε οργανισμούς μετά από πιστοποίηση ότι ο Οργανισμός υφίσταται νομικά και ότι άλλα χαρακτηριστικά του Οργανισμού που περιλαμβάνονται στο πιστοποιητικό έχουν πιστοποιηθεί. Ένα Εγκεκριμένο Πιστοποιητικό για ηλεκτρονική σφραγίδα χρησιμοποιείται συνήθως για να εξασφαλίσει την ακεραιότητα και την προέλευση των δεδομένων με τα οποία συνδέεται, ή για άλλους σκοπούς, εφόσον η χρήση δεν απαγορεύεται διαφορετικά από το νόμο, από αυτήν την Πολιτική Πιστοποίησης (ΠΠ) ή από οποιεσδήποτε συμφωνίες με τους Συνδρομητές.

1.4.1 Κατάλληλες Χρήσεις των Πιστοποιητικών

1.4.1.1 Πιστοποιητικά που εκδίδονται για ηλεκτρονική υπογραφή

Τα πιστοποιητικά είναι συμμορφούμενα με τις πολιτικές πιστοποιητικού [NCP+] και [QCP-n-qscd].
Τα πιστοποιητικά που εκδίδονται σύμφωνα με τις συγκεκριμένες απαιτήσεις αποσκοπούν στην υποστήριξη των εγκεκριμένων ηλεκτρονικών υπογραφών με τη χρήση της Εγκεκριμένης Διάταξης Δημιουργίας Υπογραφής (ΕΔΔΥ), όπως ορίζεται στο άρθρο 3 παράγραφος 12 του κανονισμού (ΕΕ) αριθ. 910/2014 [i.1].

1.4.1.2 Πιστοποιητικά που εκδίδονται για αυθεντικοποίηση

Τα πιστοποιητικά είναι συμμορφούμενα με τις πολιτικές πιστοποιητικού [NCP+].
Τα πιστοποιητικά που εκδίδονται σύμφωνα με τις συγκεκριμένες απαιτήσεις αποσκοπούν στην υποστήριξη της αυθεντικοποίησης με τη χρήση της Εγκεκριμένης Διάταξης Δημιουργίας Υπογραφής (ΕΔΔΥ).
Το πιστοποιητικό Αυθεντικοποίησης δεν μπορεί να χρησιμοποιηθεί για τη δημιουργία εγκεκριμένων ηλεκτρονικών υπογραφών συμμορφούμενο με τον κανονισμό eIDAS.

1.4.1.3 Πιστοποιητικά που εκδίδονται για ηλεκτρονικές σφραγίδες.

Τα πιστοποιητικά πληρούν τις απαιτήσεις του NCP+ και του QCP-l-qscd.

Τα πιστοποιητικά που εκδίδονται σύμφωνα με αυτές τις απαιτήσεις έχουν σκοπό να υποστηρίξουν τις εγκεκριμένες ηλεκτρονικές σφραγίδες με τη χρήση Εγκεκριμένης Διάταξης Δημιουργίας Σφραγίδας όπως ορίζεται στο άρθρο 3 (27) του Κανονισμού (ΕΕ) αριθ. 910/2014 [i.1].

1.4.2 Απαγορευμένες χρήσεις πιστοποιητικών

Τα πιστοποιητικά δεν εγγυώνται ότι το Υποκείμενο είναι αξιόπιστο, έντιμο, με καλό όνομα στις επιχειρηματικές του συναλλαγές, ασφαλές για να συνεργαστείτε μαζί του ή ότι συμμορφώνεται με οποιουσδήποτε νόμους. Ένα πιστοποιητικό επιβεβαιώνει μόνο ότι οι πληροφορίες στο πιστοποιητικό είχαν επαληθευτεί ως λογικά σωστές τη στιγμή της έκδοσής του.

Τα Πιστοποιητικά χρησιμοποιούνται μόνο στον βαθμό που η εφαρμογή τους συνάδει με την ισχύουσα νομοθεσία και ειδικότερα μόνο στον βαθμό που επιτρέπεται από την εφαρμοστέα νομοθεσία περί εισαγωγών και εξαγωγών.

Τα Πιστοποιητικά που εκδίδονται από την JCC Payment Systems δεν μπορούν να χρησιμοποιηθούν για άλλες λειτουργίες πέραν της υποστήριξης όσων ορίζονται στο κεφάλαιο 1.4.1 της παρούσας ΠΠ.

Τα Πιστοποιητικά της ΑΠ δεν μπορούν να χρησιμοποιηθούν για άλλες λειτουργίες πέραν των λειτουργιών της ΑΠ.
Επιπλέον, τα Πιστοποιητικά του Συνδρομητή δεν πρέπει να χρησιμοποιούνται ως Πιστοποιητικά της ΑΠ.

Τα Βασιζόμενα Μέρη θα χρησιμοποιούν τα αναγνωριστικά αντικειμένου (OID) της Πολιτικής Πιστοποιητικού της JCC Payment Systems όπως καθορίζονται στο Πιστοποιητικό ώστε να αποδεχτούν ή να απορρίψουν κατάλληλα τη χρήση ενός Πιστοποιητικού.

1.5 *Διαχείριση της Πολιτικής*

1.5.1 Οργανισμός που διαχειρίζεται το έγγραφο

Η παρούσα ΠΠ και τα σχετικά έγγραφα που αναφέρονται σε αυτή διατηρούνται την Αρχή Διατήρησης Πολιτικών και τη Διεύθυνση της JCC, με τους οποίους η επικοινωνία μπορεί να γίνει ως ακολούθως:
JCC Payment Systems Ltd
Σταδίου 1, 2571
Βιομηχανική περιοχή Νήσου
Λευκωσία, Κύπρος

1.5.2 Υπεύθυνος επικοινωνίας

Υπεύθυνος Αρχής Διαχείρισης Πολιτικών του Παρόχου
Υπόψη JCC Payment Systems Ltd
Σταδίου 1, 2571
Βιομηχανική περιοχή Νήσου
Λευκωσία, Κύπρος

Αριθμός τηλεφώνου: (+357) 22 868 500
Φαξ: (+357) 22 868 591
trust-policies@jcc.com.cy

1.5.2.1 Υπεύθυνος Επικοινωνίας για Ανάκληση

Για αιτήματα ανάκλησης πιστοποιητικών, βλέπετε παράγραφο 4.9.3.

1.5.3 Πρόσωπο που προσδιορίζει την καταλληλόλητα της ΠΠ ως προς την πολιτική

Ο Υπεύθυνος Αρχής Διαχείρισης Πολιτικών του Παρόχου μαζί με τη Διεύθυνση της JCC Payment Systems προσδιορίζουν την καταλληλόλητα και την εφαρμοσιμότητα της παρούσας ΠΠ.

1.5.4 Διαδικασία έγκρισης της ΠΠ

Επακόλουθες τροποποιήσεις στην παρούσα ΠΠ πραγματοποιούνται από τον Υπεύθυνο Αρχής Διαχείρισης Πολιτικών της JCC Payment Systems, κατόπιν έγκρισης της Διεύθυνσης της JCC. Η αναθεωρημένη έκδοση της ΠΠ και οποιοδήποτε άλλο τεχνικό και επιχειρησιακό έγγραφο του Παρόχου Υπηρεσιών Εμπιστοσύνης (ΠΥΕ) πρέπει να εγκριθεί από την Αρχή Διαχείρισης Πολιτικών του Παρόχου, η οποία αποτελείται από τον Διευθυντή των Υπηρεσιών Εμπιστοσύνης, τον Διαχειριστή Ασφάλειας Πληροφοριών & Διαχείρισης Κινδύνων, τον Γενικό Διευθυντή Λειτουργικών Εργασιών ή τον Διευθύνοντα Σύμβουλο. Η Διαχείριση Πολιτικής του ΠΥΕ θα αποφασίσει εάν το έγγραφο χρειάζεται έγκριση από την ISSC. Οι τροποποιήσεις γίνονται είτε με τη μορφή ενός εγγράφου που περιέχει την τροποποιημένη μορφή της ΠΠ είτε με μια ειδοποίηση ενημέρωσης. Οι τροποποιημένες εκδόσεις ή οι ενημερώσεις δημοσιεύονται στον δικτυακό Χώρο Αποθήκευσης της JCC Payment Systems που βρίσκεται στη διεύθυνση: https://pki.jcc.com.cy/repository

Οι νέες εκδόσεις υπερισχύουν έναντι οποιωνδήποτε καθορισμένων ή αντίθετων διατάξεων της αναφερόμενης έκδοσης της ΠΠ. Η Αρχή Διαχείρισης Πολιτικών του Παρόχου προσδιορίζει εάν οι αλλαγές στην ΠΠ απαιτούν ή όχι αλλαγές στα αναγνωριστικά αντικειμένου των Πολιτικών Πιστοποιητικού.

1.6 *Ορισμοί και Ακρωνύμια*

Για τον πίνακα ακρωνυμίων και ορισμών, ανατρέξτε στο Παράρτημα Α.

2 ΔΗΜΟΣΙΕΥΣΗ ΚΑΙ ΥΠΟΧΡΕΣΩΣΕΙΣ ΤΟΥ ΧΩΡΟΥ ΑΠΟΘΗΚΕΥΣΗΣ

2.1 *Χώροι Αποθήκευσης*

Η JCC Payment Systems, ως Εκδότης Αρχής Πιστοποίησης (Issuer CA), θα δημοσιεύει όλα τα Πιστοποιητικά Αρχής Πιστοποίησης (ΑΠ) που θεωρούνται έμπιστα, τα οποία εκδίδονται προς και από την Εκδότρια Αρχή Πιστοποίησης (Issuer CA), τα δεδομένα ανακλήσεων για εκδοθέντα ψηφιακά

πιστοποιητικά, την Πολιτική Πιστοποίησης (ΠΠ), την Πολιτική Διαχείρισης Πιστοποίησης (ΔΠΠ), τη Δήλωση Προστασίας Προσωπικών Δεδομένων και τους Όρους και Προϋποθέσεις. Η JCC Payment Systems διασφαλίζει ότι το πιστοποιητικό βάσης και τα δεδομένα ανακλήσεων για τα εκδοθέντα πιστοποιητικά είναι τακτικά διαθέσιμα μέσω ενός διαδικτυακού αποθετηρίου.
Η JCC Payment Systems εκδίδει Καταλόγους Ανακληθέντων Πιστοποιητικών (ΚΑΠ) και παρέχει υπηρεσίες Πρωτοκόλλου Δικτυακού Ελέγχου κατάστασης Πιστοποιητικών (OCSP) σύμφωνα με τις διατάξεις της παρούσας ΠΠ.

Η JCC Payment Systems διασφαλίζει ότι ο χώρος αποθήκευσής της είναι διαθέσιμος 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα, με ελάχιστη συνολική διαθεσιμότητα 99,00% ανά έτος με τις προγραμματισμένες διακοπές λειτουργίας να μην υπερβαίνουν το ποσοστό του 0,5% ετησίως.

Σε περίπτωση βλάβης του συστήματος, εργασιών συντήρησης ή άλλων παραγόντων που δεν υπόκεινται στον έλεγχο της JCC Payment Systems , η JCC Payment Systems θα καταβάλλει κάθε δυνατή προσπάθεια προκειμένου να διασφαλίσει ότι η μη διαθεσιμότητα της συγκεκριμένης υπηρεσίας πληροφοριών δεν θα υπερβαίνει τον ανωτέρω δηλωθέντα χρόνο.

2.2 *Δημοσίευση πληροφοριών πιστοποιητικού*

Η JCC Payment Systems διατηρεί έναν δικτυακά προσπελάσιμο αποθηκευτικό χώρο σε ένα δημόσιο δίκτυο επικοινωνίας δεδομένων (https://pki.jcc.com.cy/repository) που επιτρέπει στα Βασιζόμενα Μέρη να υποβάλλουν διαδικτυακά ερωτήματα αναφορικά με την ανάκληση και άλλες πληροφορίες σχετικά με την κατάσταση του Πιστοποιητικού. Η JCC Payment Systems παρέχει στα Βασιζόμενα Μέρη πληροφορίες σχετικά με τον τρόπο αναζήτησης του κατάλληλου δικτυακού χώρου αποθήκευσης για τον έλεγχο της κατάστασης του Πιστοποιητικού, καθώς και τον τρόπο αναζήτησης του αποκριτή OCSP (OCSP responder).

Η JCC Payment Systems δημοσιεύει στον δημόσιο αποθηκευτικό χώρο πληροφοριών τουλάχιστον τις ακόλουθες πληροφορίες:

- Επισκόπηση της ιεραρχίας πιστοποίησης
- Δήλωση Πρακτικών Πιστοποίησης
- Πολιτικές πιστοποίησης
- Πιστοποιητικά, συμπεριλαμβανομένων των ΑΠ βάσης και των εκδοτριών ΑΠ.
- Προφίλ Πιστοποίησης
- Γενικοί Όροι και Προϋποθέσεις για τη χρήση πιστοποιητικών
- Σύνδεσμος Κατάλογου Ανακληθέντων Πιστοποιητικών

2.2.1 Πολιτικές δημοσίευσης και κοινοποίησης

Η παρούσα ΠΠ της JCC Payment Systems δημοσιεύεται στον δημόσιο χώρο αποθήκευσης πληροφοριών της JCC Payment Systems.
Η ΠΠ της JCC Payment Systems μαζί με τις ημερομηνίες εκτέλεσης δημοσιεύεται τουλάχιστον 30 ημέρες πριν από την έναρξη ισχύος.

2.2.2 Στοιχεία που δεν δημοσιεύονται στη Πολιτική Πιστοποίησης

Ανατρέξτε στην ενότητα 9.3.1 της παρούσας ΠΠ.

2.3 *Χρόνος ή συχνότητα δημοσίευσης*

Ανατρέξτε στην ενότητα 2.2.1 της τρέχουσας ΠΠ για ενημερώσεις της παρούσας ΠΠ. Οι Επικαιροποιήσεις των Γενικών Όρων και Προϋποθέσεων Συνδρομητή και Βασιζόμενων Μερών δημοσιεύονται όπως απαιτείται. Οι πληροφορίες αναφορικά με την κατάσταση των Πιστοποιητικών δημοσιεύονται σύμφωνα με την παρούσα ΠΠ.

2.4 *Έλεγχοι πρόσβασης σε χώρους αποθήκευσης*

Οι πληροφορίες που δημοσιεύονται στον χώρο αποθήκευσης του δικτυακού τόπου της JCC Payment Systems είναι δημοσίως προσβάσιμες, μόνο για ανάγνωση, χωρίς περιορισμό. Η JCC Payment Systems εφαρμόζει λογικά και φυσικά μέτρα ασφαλείας προκειμένου να αποτρέψει την προσθήκη, τη διαγραφή, ή την τροποποίηση των καταχωρήσεων στον χώρο αποθήκευσης από μη εξουσιοδοτημένα πρόσωπα, σύμφωνα με τις εφαρμοστέες πολιτικές ασφάλειας της JCC Payment Systems . Η JCC Payment Systems καθιστά τον χώρο αποθήκευσής της δημόσια διαθέσιμο αλλά μόνο για ανάγνωση και συγκεκριμένα στον ακόλουθο σύνδεσμο https://pki.jcc.com.cy/repository.

3 ΤΑΥΤΟΤΗΤΑ ΚΑΙ ΕΠΑΛΗΘΕΥΣΗ ΤΗΣ ΤΑΥΤΟΤΗΤΑΣ

3.1 *Ονοματοδοσία*

Η ονοματοδοσία των πιστοποιητικών πραγματοποιείται όπως προβλέπεται στη Σύσταση ITU-T X.509 [6] ή στο IETF RFC 5280 [7] και στο σχετικό μέρος του προτύπου ETSI EN 319 412.

3.1.1 Τύποι ονομάτων

Ο τύπος των ονομάτων που αποδίδονται στην ΑΠ και τους Συνδρομητές περιγράφεται στη σχετική δημοσίευση της τεκμηρίωσης του Προφίλ Πιστοποιητικού στον χώρο αποθήκευσης της JCC Payment Systems.

Τα Πιστοποιητικά της ΑΠ της JCC Payment Systems και του Συνδρομητή περιλαμβάνουν τα Διακριτικά Ονόματα X.501 στα πεδία Εκδότη και Υποκειμένου.

3.1.2 Η ανάγκη κατανόησης των ονομάτων

Τα Πιστοποιητικά του Συνδρομητή περιλαμβάνουν ονόματα με ευρέως κατανοητή σημασιολογία ώστε να επιτρέπουν τον προσδιορισμό της ταυτότητας του ατόμου ή του οργανισμού που αποτελεί το Υποκείμενο του Πιστοποιητικού.
Τα Πιστοποιητικά της ΑΠ της JCC Payment Systems περιλαμβάνουν ονόματα με ευρέως κατανοητή σημασιολογία δίνοντας τη δυνατότητα να προσδιοριστεί η ταυτότητα της ΑΠ που αποτελεί το Υποκείμενο του Πιστοποιητικού.

3.1.3 Ανωνυμία ή ψευδωνυμία συνδρομητών

Δεν επιτρέπεται

3.1.4 Κανόνες για την Ερμηνεία των Διαφόρων Τύπων Ονομάτων

Καμία διατύπωση.

3.1.5 Μοναδικότητα των Ονομάτων

Η JCC Payment Systems διασφαλίζει ότι τα Διακριτικά Ονόματα (ΔΟ) του Συνδρομητή είναι μοναδικά εντός του τομέα συγκεκριμένης ΑΠ μέσω αυτοματοποιημένων στοιχείων κατά τη διαδικασία εγγραφής του Συνδρομητή. Η μοναδικότητα του διακριτικού ονόματος για τις ηλεκτρονικές υπογραφές και η

αυθεντικότητά του εξασφαλίζεται από την χαρακτηριστική τιμή του σειριακού αριθμού στο πεδίο "Υποκείμενο" του πιστοποιητικού. Για τις ηλεκτρονικές σφραγίδες, εξασφαλίζεται από την τιμή του χαρακτηριστικού Οργανωτικός Αναγνωριστικός Κωδικός (Organizational Identifier) στο πεδίο του Υποκειμένου (Subject) του πιστοποιητικού.
Η διαδικασία για να διασφαλιστεί ότι οι τιμές που εισάγονται στο χαρακτηριστικό serialNumber (σειριακός αριθμός πιστοποιητικού) είναι μοναδικές, βασίζεται στη μοναδικότητα της αίτησης πιστοποιητικού κάθε συνδρομητή μέσα στην αίτηση.

3.1.6 Αναγνώριση, επαλήθευση ταυτότητας και ρόλος εμπορικών σημάτων

Οι αιτούντες για Πιστοποιητικό απαγορεύεται να χρησιμοποιούν στις Αιτήσεις τους για Πιστοποιητικό, ονόματα τα οποία παραβιάζουν τα Δικαιώματα Πνευματικής Ιδιοκτησίας τρίτων. Η JCC Payment Systems , ωστόσο, δεν δύναται να επαληθεύσει εάν κάποιος Αιτών για Πιστοποιητικό διαθέτει Δικαιώματα Πνευματικής Ιδιοκτησίας επί του ονόματος που αναγράφεται σε μία Αίτηση για Πιστοποιητικό, ούτε δύναται να λειτουργήσει ως διαιτητής ή διαμεσολαβητής ή με άλλον τρόπο να επιλύσει διαφορές που αφορούν την ιδιοκτησία οποιουδήποτε ονόματος τομέα, εμπορικής επωνυμίας, εμπορικού σήματος ή σήματος παροχής υπηρεσιών. Η JCC Payment Systems έχει το δικαίωμα, χωρίς ευθύνη προς οποιονδήποτε Αιτούντα Πιστοποιητικό, να απορρίψει ή να αναστείλει μία Αίτηση για Πιστοποιητικό λόγω μίας τέτοιας διαφοράς.

3.2 *Αρχική επαλήθευση ταυτότητας*

Η JCC Payment Systems μπορεί να χρησιμοποιήσει τις ακόλουθες μεθόδους που περιγράφονται στην παρούσα ενότητα για να εξακριβώσει την ταυτότητα ενός Συνδρομητή. Η JCC Payment Systems μπορεί να αρνηθεί να εκδώσει πιστοποιητικό κατά τη διακριτική της ευχέρεια, εάν η εξακρίβωση της ταυτότητας δεν είναι επιτυχής.
Η επαλήθευση ταυτότητας αποτελεί μέρος των διαδικασιών αίτησης πιστοποιητικού, έκδοσης πιστοποιητικού και παροχής συσκευής.

3.2.1 Μέθοδος απόδειξης της κατοχής ιδιωτικού κλειδιού

Η διαδικασία δημιουργίας κλειδιού διασφαλίζεται από την παρούσα ΠΠ σε συμμόρφωση με τα τεχνικά πρότυπα ETSI EN 319 401, ETSI EN 319 411-1 and ETSI EN 319 411-2.
Ο Αιτών για Πιστοποιητικό πρέπει να αποδείξει ότι νόμιμα κατέχει το ιδιωτικό κλειδί που αντιστοιχεί στο δημόσιο κλειδί που αναγράφεται στο Πιστοποιητικό. Η μέθοδος απόδειξης της κατοχής του ιδιωτικού κλειδιού είναι σύμφωνα με το PKCS #10 (Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού) ή άλλη ισοδύναμη κρυπτογραφικά μορφή ή άλλη μέθοδος αποδεκτή από την JCC Payment Systems.

3.2.2 Επαλήθευση ταυτότητας οργανισμού

Η Εκδότρια Αρχή Πιστοποίησης (Issuer CA) ή μια ΑΕ θα επαληθεύσει την ταυτότητα ενός ατόμου σύμφωνα με τη διαδικασία που έχει καθοριστεί στην αντίστοιχη ενότητα 3.2.2 της Δήλωσης Πρακτικών Πιστοποίησης (ΔΠΠ).
Εάν η αίτηση αφορά ένα Πιστοποιητικό που δηλώνει μια οργανωτική σχέση μεταξύ ενός ανθρώπου (Συνδρομητή) και ενός οργανισμού, Η JCC Payment Systems θα ζητήσει έγγραφα από τον οργανισμό που να αναγνωρίζουν τη σχέση αυτή.

3.2.3 Επαλήθευση Ταυτότητας Ατόμου

Η JCC Payment Systems, ως Εκδότης Αρχής Πιστοποίησης (Issuer CA) ή ΑΕ, θα επαληθεύσει την ταυτότητα ενός ατόμου σύμφωνα με τη διαδικασία που έχει καθοριστεί στην αντίστοιχη ενότητα 3.2.3

της Πολιτικής Πρακτικών Πιστοποίησης (ΔΠΠ), με την απόκτηση και επαλήθευση αποδεικτικών στοιχείων της ταυτότητας του ατόμου.
Σε περίπτωση που το άτομο που αιτείται το Πιστοποιητικό είναι εξουσιοδοτημένος υπάλληλος της ΑΕ ή της ΤΑΕ, η επαλήθευση ταυτότητας του συγκεκριμένου ατόμου δεν πρέπει να διενεργείται από το ίδιο το άτομο και πρέπει να περιλαμβάνει έναν από τους συναδέλφους του στην ΑΕ/ ΤΑΕ.

3.2.3.1 Επαλήθευση του Τομέα Ηλεκτρονικού Ταχυδρομείου

Η JCC Payment Systems επαληθεύει το δικαίωμα ενός Συνδρομητή να χρησιμοποιεί ή να ελέγχει μια διεύθυνση ηλεκτρονικού ταχυδρομείου που περιέχεται σε ένα Πιστοποιητικό που θα έχει το EKU "Secure Email" αποστέλλοντας ένα μήνυμα ηλεκτρονικού ταχυδρομείου έγκρισης στη διεύθυνση ηλεκτρονικού ταχυδρομείου που θα συμπεριληφθεί στο Πιστοποιητικό και αποστέλλοντας μια μοναδική τυχαία τιμή με SMS στον αριθμό κινητού τηλεφώνου που παρέχεται στο υπογεγραμμένο έντυπο αίτησης από τον Συνδρομητή.

3.2.4 Μη επαληθευμένες πληροφορίες συνδρομητή

Μη επαληθευμένες πληροφορίες συνδρομητή περιλαμβάνουν τα εξής:

- τα χαρακτηριστικά του πεδίου «Οργανωτικός Τομέας» (ΟΤ),
- οποιαδήποτε άλλη πληροφορία που ορίζεται ως μη επαληθεύσιμη στο Πιστοποιητικό.

3.2.5 Επικύρωση αρχής

Όποτε το όνομα ενός φυσικού προσώπου συνδέεται με το όνομα ενός νομικού προσώπου σε ένα πιστοποιητικό με τέτοιον τρόπο ώστε να υποδεικνύει τη σχέση ή την εξουσιοδότηση του ατόμου να ενεργεί εκ μέρους του νομικού προσώπου, η ΑΕ της JCC Payment Systems:

- Καθορίζει ότι το νομικό πρόσωπο υφίσταται χρησιμοποιώντας τουλάχιστον μία υπηρεσία ή βάση δεδομένων επαλήθευσης ταυτότητας τρίτου μέρους ή, εναλλακτικά, οργανωτικά έγγραφα που εκδίδονται από ή καταχωρούνται στην αρμόδια κυβέρνηση που επιβεβαιώνουν την ύπαρξη του νομικού προσώπου, και
- Χρησιμοποιεί πληροφορίες που περιέχονται στα αρχεία επιχειρήσεων ή σε βάσεις δεδομένων επιχειρηματικών πληροφοριών (καταλόγους υπαλλήλων ή πελατών) της ΑΕ που εγκρίνει πιστοποιητικά για τα δικά του συνδεδεμένα άτομα ή επιβεβαιώνει μέσω τηλεφώνου, επιβεβαιωτικού ταχυδρομείου ή συγκρίσιμης διαδικασίας προς το νομικό πρόσωπο, την απασχόληση του ατόμου με το νομικό πρόσωπο που υποβάλλει την Αίτηση Πιστοποιητικού και, όταν είναι απαραίτητο, την εξουσιοδότησή του να ενεργεί εκ μέρους του νομικού προσώπου.

3.2.6 Κριτήρια διαλειτουργικότητας

Καμία διατύπωση.

3.3 *Ταυτοποίηση και επαλήθευση ταυτότητας για αιτήματα επαναδημιουργίας κλειδιών*

Πριν από τη λήξη του υφιστάμενου Πιστοποιητικού, ο Συνδρομητής πρέπει να αποκτήσει ένα νέο πιστοποιητικό ώστε να εξασφαλίσει τη συνέχιση της χρήσης του Πιστοποιητικού. Η JCC Payment Systems γενικά, απαιτεί από τον Συνδρομητή να δημιουργήσει ένα νέο ζεύγος κλειδιών το οποίο θα αντικαθιστά το ζεύγος κλειδιών που λήγει (τεχνικά ορίζεται ως «επαναδημιουργία κλειδιών»).
Ανατρέξτε στις ενότητες 3.2.2 και 3.2.3 της παρούσας ΠΠ.

Επιπλέον, όλα τα απαιτούμενα έγγραφα μπορούν να αποσταλούν ηλεκτρονικά και υπογεγραμμένα ψηφιακά από το υφιστάμενο Εγκεκριμένο Πιστοποιητικό Ηλεκτρονικής Υπογραφής. Η επαλήθευση των ηλεκτρονικά υπογεγραμμένων δικαιολογητικών εγγραφής διεξάγεται αυτόματα μέσω της εφαρμογής adobe acrobat.

3.3.1 Ταυτοποίηση και επαλήθευση ταυτότητας για τακτική επαναδημιουργία κλειδιών

Δεν εφαρμόζεται

3.3.2 Ταυτοποίηση και επαλήθευση ταυτότητας για επαναδημιουργία κλειδιών μετά από ανάκληση

Ανατρέξτε στις ενότητες 3.2.2 και 3.2.3 της παρούσας ΠΠ.

3.4 *Ταυτοποίηση και επαλήθευση ταυτότητας για αίτημα ανάκλησης*

Η ΑΕ αυθεντικοποιεί όλα τα αιτήματα ανάκλησης.

Πριν από την ανάκληση ενός Πιστοποιητικού, η ΑΕ επαληθεύει ότι η ανάκληση έχει ζητηθεί από τον Συνδρομητή του Πιστοποιητικού.

Αποδεκτές διαδικασίες για την αυθεντικοποίηση των αιτημάτων ανάκλησης ενός Συνδρομητή περιλαμβάνονται στην παράγραφο 3.4 της ΔΠΠ που εφαρμόζεται.

Οι Διαχειριστές της ΑΕ της JCC Payment Systems δικαιούνται να ζητούν την ανάκληση Πιστοποιητικών. Η JCC Payment Systems αυθεντικοποιεί την ταυτότητα των Διαχειριστών μέσω ελέγχου πρόσβασης χρησιμοποιώντας SSL και αυθεντικοποίηση πελάτη πριν τους επιτραπεί να εκτελούν λειτουργίες ανάκλησης.

4 ΛΕΙΤΟΥΡΓΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΤΟΥ ΚΥΚΛΟΥ ΖΩΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

4.1 *Αίτηση για πιστοποιητικό*

4.1.1 Ποιος μπορεί να υποβάλει αίτηση για πιστοποιητικό;

Η αίτηση για Εγκρκριμένα Πιστοποιητικά της ΕΕ μπορεί να υποβληθεί από φυσικό ή νομικό πρόσωπο, και για Πιστοποιητικά Αυθεντικοποίησης από φυσικό πρόσωπο, το οποίο και στις δύο περιπτώσεις είναι ο Συνδρομητής του Πιστοποιητικού, υπό την προϋπόθεση ότι είναι νομικά επιλέξιμος. Οι αιτητές είναι υπεύθυνοι για οποιαδήποτε δεδομένα παρέχει ο αιτών ή οποιοδήποτε εξουσιοδοτημένο πρόσωπο από τον αιτούντα στην JCC Payment Systems.

4.1.2 Διαδικασία εγγραφής και υποχρεώσεις

JCC Payment Systems, ως Εκδότης Αρχής Πιστοποίησης (Issuer CA), είναι υπεύθυνη να διασφαλίζει ότι η ταυτότητα κάθε αιτούντος επαληθεύεται σύμφωνα με την παρούσα ΠΠ και την εφαρμοστέα ΔΠΠ πριν την έκδοση οποιουδήποτε τύπου Πιστοποιητικού, σύμφωνα με τις ισχύουσες νομικές συμφωνίες. Οι αιτούντες είναι υπεύθυνοι για την υποβολή επαρκών πληροφοριών και εγγράφων, προκειμένου η Εκδότρια Αρχή Πιστοποίησης (Issuer CA) ή η ΑΕ να μπορέσουν να πραγματοποιήσουν την απαιτούμενη επαλήθευση ταυτότητας πριν την έκδοση του Πιστοποιητικού.

4.2 *Επεξεργασία αίτησης πιστοποιητικού*

4.2.1 Εκτέλεση λειτουργιών ταυτοποίησης και επαλήθευση ταυτότητας

Η JCC Payment Systems διενεργεί την ταυτοποίηση και την επαλήθευση της ταυτότητας όλων των απαιτούμενων στοιχείων του Συνδρομητή σύμφωνα με την ενότητα 3.2.

Η JCC Payment Systems εκτελεί την ταυτοποίηση και αυθεντικοποίηση όλων των απαιτούμενων πληροφοριών του Συνδρομητή είτε α) με φυσική παρουσία, είτε β) χρησιμοποιώντας μια μέθοδο ισοδύναμη με τη φυσική παρουσία σύμφωνα με την ενότητα 3.2.
Εάν μια ΑΕ/ ΤΑΕ συμβάλλει στην επαλήθευση, η ΑΕ/ ΤΑΕ πρέπει να δημιουργεί και να διατηρεί αρχεία επαρκή για να αποδεικνύει ότι έχει εκτελέσει τις απαιτούμενες εργασίες επαλήθευσης και να επικοινωνεί την ολοκλήρωση αυτής της εκτέλεσης στην JCC Payment Systems. Μετά την ολοκλήρωση της επαλήθευσης, η JCC Payment Systems αξιολογεί τις πληροφορίες και αποφασίζει αν θα εκδώσει το Πιστοποιητικό ή όχι. Στο πλαίσιο αυτής της αξιολόγησης, η ΑΕ της JCC Payment Systems μπορεί να ελέγξει το Πιστοποιητικό σε μια εσωτερική βάση δεδομένων προηγουμένως ανακληθέντων Πιστοποιητικών και απορριφθέντων αιτημάτων πιστοποίησης για να εντοπίσει ύποπτα αιτήματα πιστοποιητικών.

4.2.2 Έγκριση ή απόρριψη αιτήσεων για αιτήσεις Πιστοποιητικού

Η JCC Payment Systems εγκρίνει την αίτηση για Πιστοποιητικό μόνο εφόσον πληρούνται τα ακόλουθα κριτήρια:

- η επιτυχής ταυτοποίηση και επαλήθευση της ταυτότητας όλων των απαιτούμενων στοιχείων του Συνδρομητή σύμφωνα με την ενότητα 3.2
- έχει ληφθεί η πληρωμή

Η JCC Payment Systems απορρίπτει μια αίτηση για πιστοποιητικό εάν:

- η ταυτοποίηση και η επαλήθευση της ταυτότητας όλων των απαιτούμενων στοιχείων του Συνδρομητή σύμφωνα με την ενότητα 3.2 δεν μπορεί να ολοκληρωθεί ή
- ο Συνδρομητής αδυνατεί να υποβάλλει τη σχετική τεκμηρίωση που του ζητείται ή
- ο Συνδρομητής αδυνατεί να ανταποκριθεί στις ειδοποιήσεις εντός του καθορισμένου χρόνου ή
- δεν έχει ληφθεί η πληρωμή
- η JCC Payment Systems θεωρεί ότι η έκδοση πιστοποιητικού στον Συνδρομητή θα βλάψει την υπόληψη της JCC Payment Systems.

Σε περίπτωση τοπικής Εγκεκριμένη Διάταξη Δημιουργίας Υπογραφής (ΕΔΔΥ), κατά την απόρριψη αίτησης για πιστοποιητικό, ο Συνδρομητής έχει το δικαίωμα είτε να επιστρέψει την ΕΔΔΥ σύμφωνα με την Ενότητα 9.1.5 είτε να την κρατήσει για μελλοντική χρήση υπό την πλήρη ευθύνη του.

Σε περίπτωση που η JCC Payment Systems απορρίψει μια αίτηση για πιστοποιητικό που σχετίζεται με εξ'αποστάσεως ΕΔΔΥ, ο αντίστοιχος λογαριασμός Συνδρομητή δεν δημιουργείται και δεν απαιτούνται άλλες ενέργειες από τον Συνδρομητή.

4.2.3 Χρόνος επεξεργασίας των αιτήσεων για Πιστοποιητικό

Η JCC Payment Systems ξεκινά την επεξεργασία των αιτήσεων για πιστοποιητικό μέσα σε 3 μέρες από την παραλαβή τους. Δεν υπάρχει χρονική διατύπωση ως προς την ολοκλήρωση της επεξεργασίας μιας αίτησης εκτός εάν άλλως υποδεικνύεται στους σχετικούς Γενικούς Όρους και Προϋποθέσεις, στη ΠΠ, στη ΔΠΠ ή σε άλλη συμφωνία.
Μια αίτηση για Πιστοποιητικό παραμένει ενεργή έως ότου να απορριφθεί.

4.3 *Έκδοση Πιστοποιητικού*

4.3.1 Ενέργειες της ΑΠ κατά την έκδοση πιστοποιητικών

Το Πιστοποιητικό δημιουργείται και εκδίδεται μετά την έγκριση Αίτησης για Πιστοποιητικό από την JCC Payment Systems. Η JCC Payment Systems δημιουργεί και εκδίδει Πιστοποιητικό στον Συνδρομητή Πιστοποιητικού βάσει των στοιχείων της Αίτησης για Πιστοποιητικό και κατόπιν της έγκρισης της σχετικής αίτησης.

4.3.2 Ειδοποίηση του συνδρομητή από την ΑΠ για την έκδοση του πιστοποιητικού

Η JCC Payment Systems ενημερώνει τους Συνδρομητές ότι έχουν δημιουργηθεί τα σχετικά Πιστοποιητικά και παρέχει πρόσβαση στα Πιστοποιητικά ενημερώνοντάς τους ότι τα Πιστοποιητικά τους είναι διαθέσιμα. Τα Πιστοποιητικά καθίστανται διαθέσιμα στους Συνδρομητές ενημερώνοντάς τους μέσω ενός μηνύματος ηλεκτρονικού ταχυδρομείου.

4.4 *Αποδοχή πιστοποιητικού*

4.4.1 Ενέργειες που αποτελούν αποδοχή πιστοποιητικού

Οι ακόλουθες ενέργειες συνιστούν αποδοχή του πιστοποιητικού:

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

4.4.2 Δημοσίευση του πιστοποιητικού από την ΑΠ

Η JCC Payment Systems δεν δημοσιεύει τα Πιστοποιητικά που εκδίδει σε δημοσίως προσβάσιμο διαδικτυακό χώρο αποθήκευσης.

4.4.3 Κοινοποίηση έκδοσης πιστοποιητικού από την ΑΠ προς άλλες οντότητες

Οι ΑΕ και οι ΤΑΕ δύνανται να λάβουν ενημέρωση για την έκδοση των πιστοποιητικών που εγκρίνουν.

4.5 *Χρήση ζεύγους κλειδιών και πιστοποιητικού*

4.5.1 Χρήση ιδιωτικού κλειδιού συνδρομητή και πιστοποιητικού

Η χρήση του ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί του Πιστοποιητικού επιτρέπεται μόνο εφόσον ο Συνδρομητής έχει συμφωνήσει με τους Γενικούς Όρους και Προϋποθέσεις και έχει αποδεχτεί το Πιστοποιητικό. Το Πιστοποιητικό πρέπει να χρησιμοποιείται νόμιμα σύμφωνα με τους Γενικούς Όρους και Προϋποθέσεις της JCC Payment Systems και με την σχετική ΔΠΠ. Η χρήση του Πιστοποιητικού πρέπει να συνάδει με τις επεκτάσεις του πεδίου «Χρήση Κλειδιού» (KeyUsage) που περιλαμβάνεται στο Πιστοποιητικό. Η χρήση κλειδιού του πιστοποιητικού είναι τύπου Β όπως ορίζεται στην παράγραφο 4.3.2 του πρότυπου ETSI EN 319 412-2.

Οι Συνδρομητές πρέπει να προστατεύουν τα ιδιωτικά κλειδιά τους από μη εξουσιοδοτημένη χρήση και πρέπει να διακόψουν τη χρήση των ιδιωτικών κλειδιών μετά τη λήξη ή ανάκληση του πιστοποιητικού. Μέρη άλλα πέραν του Συνδρομητή δεν αρχειοθετούν το Ιδιωτικό Κλειδί του Συνδρομητή.

4.5.2 Χρήση δημόσιου κλειδιού και πιστοποιητικών από βασιζόμενο μέρος

Τα βασιζόμενα μέρη πρέπει να συναινούν στους Γενικούς Όρους και Προϋποθέσεις της JCC Payment Systems ως προϋπόθεση για να βασιστούν σε ένα Πιστοποιητικό.

Η εμπιστοσύνη σε ένα Πιστοποιητικό πρέπει να είναι εύλογη βάσει των συνθηκών. Εάν οι συνθήκες υποδεικνύουν την ανάγκη για πρόσθετες διαβεβαιώσεις, το Βασιζόμενο Μέρος πρέπει να αποκτήσει αυτές τις διαβεβαιώσεις ώστε η εμπιστοσύνη σε ένα Πιστοποιητικό να θεωρηθεί εύλογη.

Πριν από οποιαδήποτε πράξη εμπιστοσύνης, τα Βασιζόμενα Μέρη πρέπει να αξιολογούν ανεξάρτητα τα ακόλουθα:

- την καταλληλότητα της χρήσης του Πιστοποιητικού για κάθε σκοπό και να επιβεβαιώσουν ότι το Πιστοποιητικό έχει πράγματι χρησιμοποιηθεί για έναν κατάλληλο σκοπό ο οποίος δεν απαγορεύεται ή άλλως περιορίζεται από την παρούσα ΠΠ και την αντίστοιχη ΔΠΠ. Η JCC Payment Systems δεν ευθύνεται για την καταλληλότητα της χρήσης του Πιστοποιητικού·
- ότι η χρήση του Πιστοποιητικού χρησιμοποιείται σύμφωνα με τις επεκτάσεις του πεδίου «Χρήση Κλειδιού» (KeyUsage) που περιλαμβάνεται στο Πιστοποιητικό·
- την κατάσταση του Πιστοποιητικού και όλων των ΑΠ στην αλυσίδα που εξέδωσε το Πιστοποιητικό. Εάν κάποιο από τα Πιστοποιητικά στην αλυσίδα Πιστοποιητικού έχει ανακληθεί, το Βασιζόμενο Μέρος είναι αποκλειστικά υπεύθυνο να αποφασίσει εάν η εμπιστοσύνη σε μια ψηφιακή υπογραφή από πλευράς Πιστοποιητικού Συνδρομητή τελικού χρήστη πριν από την ανάκληση του Πιστοποιητικού στην αλυσίδα Πιστοποιητικού, είναι εύλογη. Κάθε τέτοια εμπιστοσύνη γίνεται αποκλειστικά με κίνδυνο του ίδιου του Βασιζόμενου Μέρους.

Εάν υποτεθεί ότι η χρήση του Πιστοποιητικού είναι κατάλληλη, τα Βασιζόμενα Μέρη πρέπει να χρησιμοποιήσουν το κατάλληλο λογισμικό και/ή υλικό ώστε να μπορέσουν να εξακριβώσουν την υπογραφή ή άλλες κρυπτογραφικές λειτουργίες που επιθυμούν να διενεργήσουν, ως όρο αποδοχής ενός Πιστοποιητικού σε συνάρτηση με κάθε σχετική λειτουργία. Οι εν λόγω λειτουργίες περιλαμβάνουν την ταυτοποίηση της Αλυσίδας Πιστοποιητικών και την εξακρίβωση των ψηφιακών υπογραφών σε όλα τα Πιστοποιητικά της Αλυσίδας Πιστοποιητικών.

4.6 *Ανανέωση πιστοποιητικού*

Δεν εφαρμόζεται.

4.7 *Επαναδημιουργία κλειδιών πιστοποιητικού*

Η επαναδημιουργία κλειδιών πιστοποιητικού είναι η αίτηση για την έκδοση ενός νέου πιστοποιητικού που πιστοποιεί το νέο δημόσιο κλειδί.

4.7.1 Συνθήκες για την επαναδημιουργία κλειδιών πιστοποιητικού

Πριν από τη λήξη του υφιστάμενου Πιστοποιητικού του Συνδρομητή, ο Συνδρομητής πρέπει να επαναδημιουργήσει κλειδιά για το πιστοποιητικό ώστε να εξασφαλίσει τη συνέχιση της χρήσης του Πιστοποιητικού. Μπορεί να επαναδημιουργηθούν κλειδιά για το πιστοποιητικό και μετά τη λήξη του.

4.7.2 Ποιοι μπορούν να αιτηθούν την πιστοποίηση νέου δημόσιου κλειδιού

Μόνο ο Συνδρομητής δύναται να αιτηθεί την επαναδημιουργία κλειδιών για το Πιστοποιητικό.

4.7.3 Επεξεργασία αιτημάτων επαναδημιουργίας κλειδιών πιστοποιητικού

Οι διαδικασίες επαναδημιουργίας κλειδιών επιβεβαιώνουν ότι ο Συνδρομητής που επιθυμεί να ανανεώσει ένα Πιστοποιητικό Συνδρομητή είναι πράγματι ο Συνδρομητής (ή εξουσιοδοτημένος από τον Συνδρομητή) του Πιστοποιητικού.

Ο Συνδρομητής υποβάλλει μία αίτηση επαναδημιουργίας κλειδιών στην ΑΕ ή την ΤΑΕ της JCC Payment Systems και η ΑΕ ή η ΤΑΕ της JCC Payment Systems επαναβεβαιώνει την ταυτότητα του Συνδρομητή σύμφωνα με τις απαιτήσεις ταυτοποίησης και επαλήθευσης της ταυτότητας, όπως αυτές περιγράφονται στην ενότητα 3.3.1.

Εκτός της συγκεκριμένης διαδικασίας ή άλλης που έχει εγκριθεί από την JCC Payment Systems, οι απαιτήσεις για την επαλήθευση ταυτότητας μιας αρχικής Αίτησης για Πιστοποιητικό εφαρμόζονται για την επαναδημιουργία κλειδιών Πιστοποιητικού Συνδρομητή τελικού χρήστη.

4.7.4 Κοινοποίηση έκδοσης νέου πιστοποιητικού στον συνδρομητή

Η ενημέρωση του Συνδρομητή για την έκδοση του Πιστοποιητικού με επαναδημιουργημένα κλειδιά, πραγματοποιείται σύμφωνα με την ενότητα 4.3.2.

4.7.5 Ενέργεια που συνιστά αποδοχή του Πιστοποιητικού με επαναδημιουργημένα κλειδιά

Η ενέργεια που συνιστά αποδοχή του Πιστοποιητικού με επαναδημιουργημένα κλειδιά πραγματοποιείται σύμφωνα με την ενότητα 4.4.1.

4.7.6 Δημοσίευση του πιστοποιητικού με επαναδημιουργημένα κλειδιά από την ΑΠ

Το πιστοποιητικό με επαναδημιουργημένα κλειδιά δεν δημοσιεύεται στον δημοσίως προσβάσιμο χώρο αποθήκευσης της JCC Payment Systems.

4.7.7 Κοινοποίηση έκδοσης πιστοποιητικού από την ΑΠ προς άλλες οντότητες

Οι ΑΕ και οι ΤΑΕ δύνανται να λάβουν ενημέρωση για την έκδοση των Πιστοποιητικών που εγκρίνουν.

4.8 *Τροποποίηση πιστοποιητικού*

4.8.1 Συνθήκες για την τροποποίηση πιστοποιητικού

Η τροποποίηση Πιστοποιητικού αναφέρεται στην αίτηση για την έκδοση ενός νέου πιστοποιητικού λόγω αλλαγών στις πληροφορίες που περιέχονται στο υφιστάμενο πιστοποιητικό (άλλες εκτός από το δημόσιο κλειδί του συνδρομητή).

Δεν είναι δυνατή η τροποποίηση ενός πιστοποιητικού, το πιστοποιητικό θα πρέπει να ανακληθεί και να εκδοθεί ένα νέο διορθωμένο.

Η τροποποίηση Πιστοποιητικού νοείται ως η Αίτηση για Πιστοποιητικό, σύμφωνα με τους όρους της ενότητας 4.1.

4.8.2 Ποιος μπορεί να αιτηθεί τροποποίηση πιστοποιητικού

Ανατρέξτε στην ενότητα 4.1.1.

4.8.3 Επεξεργασία αιτημάτων τροποποίησης πιστοποιητικού

Η JCC Payment Systems διενεργεί την ταυτοποίηση και την επαλήθευση της ταυτότητας όλων των απαιτούμενων στοιχείων του Συνδρομητή σύμφωνα με την ενότητα 3.2.

4.8.4 Κοινοποίηση έκδοσης νέου πιστοποιητικού στον συνδρομητή

Ανατρέξτε στην ενότητα 4.3.2.

4.8.5 Ενέργεια που συνιστά αποδοχή του τροποποιημένου πιστοποιητικού

Ανατρέξτε στην ενότητα 4.4.1.

4.8.6 Δημοσίευση του τροποποιημένου πιστοποιητικού από την ΑΠ

Ανατρέξτε στην ενότητα 4.4.2.

4.8.7 Κοινοποίηση έκδοσης πιστοποιητικού από την ΑΠ προς άλλες οντότητες

Ανατρέξτε στην ενότητα 4.4.3.

4.9 *Αναστολή και ανάκληση πιστοποιητικού*

Η ανάκληση ενός πιστοποιητικού τερματίζει μόνιμα την περίοδο λειτουργίας του πιστοποιητικού πριν φτάσει στο τέλος της δηλωμένης περιόδου ισχύος του. Πριν από την ανάκληση ενός πιστοποιητικού, όλα τα αιτήματα ανάκλησης αυθεντικοποιούνται σύμφωνα με την παράγραφο 3.4.

Η ανάκληση πιστοποιητικών εκτελείται σύμφωνα με τις παρακάτω ενότητες.

4.9.1 Συνθήκες για ανάκληση πιστοποιητικού

Οι Γενικοί Όροι και Προϋποθέσεις της JCC Payment Systems προβλέπουν την υποχρέωση και/ή το δικαίωμα στον Συνδρομητή να αιτηθεί την ανάκληση ενός Πιστοποιητικού. Μόνο στις περιπτώσεις που αναφέρονται παρακάτω μπορεί ένα Πιστοποιητικό Συνδρομητή να ανακληθεί από την JCC Payment Systems (ή από τον Συνδρομητή) και να δημοσιευτεί σε έναν Κατάλογο Ανακληθέντων Πιστοποιητικών (ΚΑΠ).

Ένα Πιστοποιητικό Συνδρομητή ανακαλείται εφόσον:

- Η JCC Payment Systems ή ένας Συνδρομητής έχουν λόγο να πιστεύουν ή έχουν σοβαρές υπόνοιες ότι έχει υπάρξει Έκθεση του ιδιωτικού κλειδιού ενός Συνδρομητή σε Κίνδυνο. Σε περίπτωση που αναφέρεται η σύναψη συμβιβασμού από τρίτο μέρος, η JCC Payment Systems απαιτεί την αντίστοιχη επιβεβαίωση από τον Συνδρομητή.
- Η JCC Payment Systems έχει λόγο να πιστεύει ότι ο Συνδρομητής έχει αθετήσει ουσιώδη υποχρέωση, δήλωση ή εγγύηση σύμφωνα με τους ισχύοντες Γενικούς Όρους και Προϋποθέσεις όσον αφορά την χρήση Πιστοποιητικών
- Η JCC Payment Systems έχει λόγο να πιστεύει ότι το Πιστοποιητικό έχει εκδοθεί με τρόπο που δεν είναι ουσιαστικά σύμφωνος με τις διαδικασίες που απαιτούνται από την παρούσα ΔΠΠ, ότι το Πιστοποιητικό εκδόθηκε προς πρόσωπο διαφορετικό από αυτό που κατονομάζεται ως το Υποκείμενο του Πιστοποιητικού ή το Πιστοποιητικό εκδόθηκε χωρίς την εξουσιοδότηση του προσώπου που κατονομάζεται ως το Υποκείμενο του εν λόγω Πιστοποιητικού.
- Η JCC Payment Systems είναι ενήμερη για αλλαγές που επηρεάζουν την εγκυρότητα του πιστοποιητικού.
- Η χρησιμοποιούμενη κρυπτογραφία δεν διασφαλίζει πλέον τη σύνδεση μεταξύ του Υποκειμένου και του δημόσιου κλειδιού.

- Η JCC Payment Systems έχει λόγο να πιστεύει ότι κάποιο βασικό στοιχείο στην Αίτηση για Πιστοποιητικό είναι ψευδές.
- Η JCC Payment Systems αποφαίνεται ότι δεν πληρούται ή δεν αίρεται καμία βασική προϋπόθεση για την Έκδοση Πιστοποιητικού.
- Ο Συνδρομητής χάνει τη δικαιοπρακτική του ικανότητα, κηρύσσεται απών ή αποβιώσας, έχει ρευστοποιηθεί ή δηλώσει πτώχευση, λαμβάνοντας υπόψη ότι το Πιστοποιητικό είναι σε κάθε περίπτωση μη μεταβιβάσιμο.
- Ο Συνδρομητής χάνει την ικανότητα να χρησιμοποιήσει την τοπική Εγκεκριμένη Διάταξη Δημιουργίας Υπογραφής (ΕΔΔΥ) ή τη κινητή συσκευή που απαιτείται για την πρόσβαση σε εξ' αποστάσεως ΕΔΔΥ.
- Σε περίπτωση που το Υποκείμενο του Πιστοποιητικού είναι φυσικό πρόσωπο συνδεδεμένο με τον Συνδρομητή-νομικό πρόσωπο και ο Συνδρομητής ζητά την ανάκληση.
- Σε περίπτωση τελεσίδικης δικαστικής απόφασης που απαιτεί την εν λόγω ανάκληση ή ακύρωση.
- Το ιδιωτικό κλειδί της ΑΠ έχει παραβιαστεί.
- Ο Εποπτικός Φορέας ζητά την ανάκληση βάσει νόμου.
- Η ταυτότητα του Συνδρομητή δεν επανεπαληθεύεται με επιτυχία.
- Ο Συνδρομητής δεν έχει καταβάλει εγκαίρως το οφειλόμενο ποσό.
- Η συνέχιση της χρήσης του Πιστοποιητικού αυτού, ενδέχεται να είναι επιβλαβής για την JCC Payment Systems.

Όταν η JCC Payment Systems εξετάζει εάν η χρήση ενός Πιστοποιητικού είναι επιζήμια για αυτήν, συνεκτιμά, μεταξύ άλλων, τα ακόλουθα:

- τη φύση και των αριθμό των καταγγελιών που έχει λάβει,
- την ταυτότητα των καταγγελλόντων,
- τη σχετική ισχύουσα νομοθεσία,
- τις αποκρίσεις στην επικαλούμενη επιζήμια χρήση από πλευράς Συνδρομητή.

Η JCC Payment Systems δύναται επίσης να ανακαλέσει ένα Πιστοποιητικό Διαχειριστή εάν η εξουσία του Διαχειριστή βάσει της οποίας ενεργεί με την ιδιότητα αυτή, έχει τερματιστεί ή με άλλον τρόπο ολοκληρωθεί.

Οι Γενικοί Όροι και Προϋποθέσεις της JCC Payment Systems για τη χρήση Πιστοποιητικών της απαιτούν οι Συνδρομητές να ειδοποιούν αμέσως την JCC Payment Systems σχετικά με γνωστή ή πιθανολογούμενη έκθεση του ιδιωτικού τους κλειδιού σε κίνδυνο.

Μετά την έγκριση του αιτήματος για ανάκληση από πλευράς ΑΠ, το ανακληθέν Πιστοποιητικό δεν μπορεί να επανατεθεί σε ισχύ.

Ένα Πιστοποιητικό της Αρχή Πιστοποίησης (ΑΠ) ανακαλείται εάν, μεταξύ άλλων:

- Το ιδιωτικό κλειδί της ΑΠ έχει εκτεθεί σε κίνδυνο
- Η τελική δικαστική απόφαση απαιτεί τη σχετική ανάκληση ή ακύρωση
- Ο Εποπτικό Φορέας ζητεί την ανάκληση σύμφωνα με το νόμο

4.9.2 Ποιοι μπορούν να αιτηθούν την ανάκληση πιστοποιητικού

Αίτημα για την ανάκληση Εγκεκριμένου Πιστοποιητικού δύναται να υποβάλλει:

- Ένα φυσικό ή νομικό πρόσωπο, ή οι νόμιμοι εκπρόσωποί τους, που είναι ο Συνδρομητής του Πιστοποιητικού, ή ένας διάδοχος που επιθυμεί να ζητήσει την

ανάκληση σε περίπτωση θανόντος Συνδρομητή (φυσικό πρόσωπο), εφόσον είναι νομικά επιλέξιμος.

- Το αρμόδιο δικαστήριο ή Δημόσια Αρχή
- Ο Εποπτικός Φορέας.
- Η Αρχή Εγγραφής (ΑΕ) ή η Τοπική Αρχή Εγγραφής (ΤΑΕ)
- Η Αρχή Πιστοποίησης (ΑΠ)

4.9.3 Διαδικασία υποβολής αιτήματος ανάκλησης

4.9.3.1 Διαδικασία για υποβολή αιτήματος ανάκλησης πιστοποιητικού της Αρχής Πιστοποίησης

Σε περίπτωση υποβολής αιτήματος ανάκλησης πιστοποιητικού της Αρχής Πιστοποίησης,
.

4.9.3.2 Διαδικασία για υποβολή αιτήματος ανάκλησης πιστοποιητικού συνδρομητή

Σε περίπτωση που ένας Συνδρομητής δεν πραγματοποιήσει ο ίδιος την ανάκληση σύμφωνα με την ενότητα 3.4, μπορεί να αιτηθεί ανάκληση με την αποστολή μηνύματος ηλεκτρονικού ταχυδρομείου στη διεύθυνση revocation@jcc.com.cy ή τηλεφωνικώς στο (+357) 22 868 500. Η JCC Payment Systems θα ανακαλέσει άμεσα το σχετικό Πιστοποιητικό.
Η κοινοποίηση για τη σχετική αίτηση ανάκλησης θα είναι σύμφωνη με την ενότητα 3.4.

4.9.4 Περίοδος χάριτος του αιτήματος ανάκλησης

Τα αιτήματα ανάκλησης πρέπει να υποβάλλονται το συντομότερο δυνατό, σε εύλογο από εμπορικής άποψης χρονικό διάστημα.

4.9.5 Χρονικό διάστημα μέσα στο οποίο η ΑΠ θα πρέπει να επεξεργαστεί το αίτημα ανάκλησης

Η JCC Payment Systems λαμβάνει όλα τα εύλογα από εμπορικής άποψης βήματα προκειμένου να επεξεργαστεί τα αιτήματα ανάκλησης χωρίς καθυστέρηση και, σε κάθε περίπτωση, η μέγιστη καθυστέρηση από τη στιγμή που η JCC Payment Systems λαμβάνει το αίτημα ανάκλησης σύμφωνα με την ενότητα 4.9.3.1, ενώ παράλληλα η απόφαση να αλλάξει τις πληροφορίες κατάστασης που είναι διαθέσιμες σε όλα τα βασιζόμενα μέρη πρέπει να μην ξεπερνά τις 24 ώρες. Εάν, παρόλα αυτά, το αίτημα ανάκλησης δεν μπορεί να επιβεβαιωθεί εντός 24 ωρών, τότε η κατάσταση δεν πρέπει να αλλάξει.

Αμέσως μετά την έγκριση του αιτήματος ανάκλησης, η ΑΠ ενημερώνει τον Συνδρομητή και το Υποκείμενο του πιστοποιητικού για την εν λόγω ανάκληση μέσω μηνύματος ηλεκτρονικού ταχυδρομείου.

4.9.6 Απαιτήσεις ελέγχου κατάστασης ανακληθέντων πιστοποιητικών για βασιζόμενα μέρη

Τα Βασιζόμενα Μέρη πρέπει να ελέγχουν την κατάσταση του Πιστοποιητικού στο οποίο επιθυμούν να βασιστούν. Μία μέθοδος με την οποία τα Βασιζόμενα Μέρη μπορούν να ελέγξουν την κατάσταση του Πιστοποιητικού είναι να ανατρέξουν στον πιο πρόσφατο ΚΑΠ της ΑΠ που εξέδωσε το Πιστοποιητικό

αυτό, στο οποίο το Βασιζόμενο Μέρος επιθυμεί να βασιστεί. Εναλλακτικά, τα Βασιζόμενα Μέρη δύνανται να ελέγχουν την κατάσταση του Πιστοποιητικού χρησιμοποιώντας τον δικτυακό αποθηκευτικό χώρο της JCC Payment Systems ή χρησιμοποιώντας την υπηρεσία OCSP. Οι ΑΠ θα πρέπει να παρέχουν στα Βασιζόμενα Μέρη πληροφορίες σχετικά με τον τρόπο εξεύρεσης του κατάλληλου ΚΑΠ και του δικτυακού αποθηκευτικού χώρου ή του αποκριτή OCSP για τον έλεγχο της κατάστασης της ανάκλησης.
Λόγω των πολυάριθμων και διάφορων τοποθεσιών για τους αποθηκευτικούς χώρους του ΚΑΠ, συνιστάται στα βασιζόμενα μέρη να αποκτούν πρόσβαση στους ΚΑΠ με τη χρήση ενσωματωμένων διευθύνσεων URL στην επέκταση των Σημείων Διανομής ΚΑΠ ενός πιστοποιητικού.
Τοποθετείται ο κατάλληλος αποκριτής OCSP για ένα συγκεκριμένο πιστοποιητικό στην επέκταση Πρόσβασης Πληροφοριών Αρχής.

Οι πληροφορίες κατάστασης ανάκλησης θα είναι διαθέσιμες πέρα από την περίοδο ισχύος του πιστοποιητικού.

4.9.7 Συχνότητα έκδοσης ΚΑΠ

Οι ΚΑΠ για τα Πιστοποιητικά του Συνδρομητή εκδίδονται τουλάχιστον μία φορά ανά ημέρα. Οι ΚΑΠ για τα Πιστοποιητικά της ΑΠ εκδίδονται τουλάχιστον σε ετήσια βάση αλλά και όποτε ανακαλείται ένα Πιστοποιητικό της ΑΠ.

4.9.8 Μέγιστος χρόνος αναμονής για τους ΚΑΠ

Οι ΚΑΠ ανακοινώνονται στον χώρο αποθήκευσης εντός εμπορικώς εύλογου χρονικού διαστήματος από τη δημιουργία τους. Πρόκειται για μια κατά κανόνα αυτοματοποιημένη διαδικασία, η οποία πραγματοποιείται μερικά λεπτά μετά τη δημιουργία του ΚΑΠ.

4.9.9 Διαθεσιμότητα ανάκλησης/κατάστασης πιστοποιητικών σε απευθείας σύνδεση

Η ανάκληση σε σύνδεση και άλλες πληροφορίες της κατάστασης του Πιστοποιητικού είναι διαθέσιμες μέσω ενός δικτυακού χώρου αποθήκευσης και του OCSP. Πέραν της δημοσίευσης των ΚΑΠ, η JCC Payment Systems παρέχει πληροφορίες για την κατάσταση των Πιστοποιητικών μέσω λειτουργιών διερευνήσεων στον αποθηκευτικό χώρο της JCC Payment Systems .
Οι πληροφορίες για την κατάσταση των Πιστοποιητικών όσον αφορά των Πιστοποιητικών είναι διαθέσιμες στον αποθηκευτικό χώρο της JCC Payment Systems στην εξής διεύθυνση: https://pki.jcc.com.cy/repository
Η μέγιστη καθυστέρηση μεταξύ της επιβεβαίωσης της ανάκλησης ενός πιστοποιητικού να τεθεί σε ισχύ και της αλλαγής των πληροφοριών για την κατάσταση του συγκεκριμένου πιστοποιητικού που καθίστανται διαθέσιμες στα βασιζόμενα μέρη είναι το ανώτερο τα 60 λεπτά. Εάν παρόλο που το αίτημα ανάκλησης απαιτεί την ανάκληση εκ των προτέρων (π.χ. η προγραμματισμένη παύση του Υποκειμένου από τα καθήκοντά του σε συγκεκριμένη ημερομηνία), η προγραμματισμένη ημερομηνία μπορεί να θεωρηθεί ως ο χρόνος επαλήθευσης.

4.9.10 Απαιτήσεις ελέγχου κατάστασης ανακληθέντων πιστοποιητικών σε απευθείας σύνδεση

Ένα βασιζόμενο μέρος πρέπει να ελέγχει την κατάσταση ενός πιστοποιητικού στο οποίο επιθυμεί να βασιστεί. Εάν ένα Βασιζόμενο Μέρος δεν ελέγχει την κατάσταση ενός Πιστοποιητικού στο οποίο το Βασιζόμενο Μέρος επιθυμεί να βασιστεί ανατρέχοντας στον πιο πρόσφατο σχετικό ΚΑΠ, το Βασιζόμενο Μέρος ελέγχει την κατάσταση του Πιστοποιητικού ανατρέχοντας στον αποθηκευτικό χώρο της JCC Payment Systems ή ζητώντας την κατάσταση του Πιστοποιητικού χρησιμοποιώντας τον ισχύοντα αποκριτή OCSP.

4.9.11 Άλλες διαθέσιμες μορφές αναγγελίας ανάκλησης

Δεν εφαρμόζεται.

4.9.12 Ειδικές απαιτήσεις σχετικά με την έκθεση του κλειδιού σε κίνδυνο

Η JCC Payment Systems καταβάλλει κάθε εύλογη από εμπορικής άποψης προσπάθεια προκειμένου να ειδοποιήσει τα πιθανά Βασιζόμενα Μέρη εάν ανακαλύψει ή έχει λόγο να πιστεύει ότι έχει υπάρξει Έκθεση σε Κίνδυνο του ιδιωτικού κλειδιού μιας εκ των ΑΠ της.

4.9.13 Συνθήκες για αναστολή πιστοποιητικού

Δεν εφαρμόζεται.

4.9.14 Ποιοι μπορούν να αιτηθούν την αναστολή πιστοποιητικού

Δεν εφαρμόζεται.

4.9.15 Διαδικασία υποβολής αιτήματος αναστολής

Δεν εφαρμόζεται.

4.9.16 Περιορισμός για την περίοδο αναστολής

Δεν εφαρμόζεται.

4.10 *Υπηρεσίες κατάστασης πιστοποιητικού*

4.10.1 Λειτουργικά χαρακτηριστικά

Οι πληροφορίες κατάστασης πιστοποιητικών είναι διαθέσιμες μέσω του ΚΑΠ και του ανταποκριτή OCSP. Ο αύξων αριθμός του πιστοποιητικού που έχει ανακληθεί παραμένει στον ΚΑΠ μέχρι να δημοσιευθεί ένας επιπλέον ΚΑΠ μετά τη λήξη της περιόδου ισχύος του πιστοποιητικού. Οι πληροφορίες OCSP για τα πιστοποιητικά συνδρομητών ενημερώνονται σύμφωνα με την ενότητα.

4.10.2 Διαθεσιμότητα υπηρεσιών

Η JCC Payment Systems διασφαλίζει ότι οι Υπηρεσίες Κατάστασης Πιστοποιητικών είναι διαθέσιμες 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα, με ελάχιστη συνολική διαθεσιμότητα 99% ανά έτος με τις προγραμματισμένες διακοπές λειτουργίας να μην υπερβαίνουν το ποσοστό του 0,5% ετησίως.

4.10.3 Προαιρετικά χαρακτηριστικά

Δεν εφαρμόζεται.

4.11 *Τερματισμός συνδρομής*

Ένας Συνδρομητής μπορεί να τερματίσει τη συνδρομή του για ένα Εγκεκριμένο Πιστοποιητικό της JCC Payment Systems με τους εξής τρόπους:

- επιτρέποντας τη λήξη του Εγκεκριμένου Πιστοποιητικού χωρίς την επαναδημιουργία κλειδιών για το συγκεκριμένο Πιστοποιητικό,
- ανακαλώντας το Εγκεκριμένο Πιστοποιητικό πριν από τη λήξη του χωρίς να προχωρήσει σε αντικατάστασή του.

4.12 *Παρακαταθήκη και ανάκτηση κλειδιού*

Δεν εφαρμόζεται.

4.12.1 Πολιτικές και πρακτικές για την παρακαταθήκη και την ανάκτηση κλειδιού

Δεν εφαρμόζεται.

4.12.2 Πολιτικές και πρακτικές για την ενθυλάκωση και την ανάκτηση του κλειδιού της περιόδου

Δεν εφαρμόζεται.

5 ΜΕΤΡΑ ΕΛΕΓΧΟΥ ΤΩΝ ΕΓΚΑΤΑΣΤΑΣΕΩΝ ΤΗΣ ΔΙΑΧΕΙΡΙΣΗΣ ΚΑΙ ΤΗΣ ΛΕΙΤΟΥΡΓΙΑΣ

5.1 *Φυσικοί έλεγχοι*

Η JCC Payment Systems εφαρμόζει την Πολιτική Φυσικής Ασφάλειας (Physical Security Policy) της JCC Payment Systems, η οποία υποστηρίζει τις απαιτήσεις ασφαλείας που παρατίθενται στην παρούσα ΠΠ. Η συμμόρφωση με τις συγκεκριμένες πολιτικές αποτελεί μέρος των απαιτήσεων ελέγχου συμμόρφωσης της JCC Payment Systems , όπως αυτές περιγράφονται στην ενότητα 8. Η Πολιτική Φυσικής Ασφάλειας της JCC Payment Systems περιέχει ευαίσθητες πληροφορίες για την ασφάλεια και διατίθεται μόνο κατόπιν συμφωνίας με την JCC Payment Systems. Μια περίληψη των απαιτήσεων αυτών, παρατίθεται κατωτέρω.
Η JCC Payment Systems αναθέτει τη λειτουργία της ΑΠ στην ADACOM SA η οποία είναι Εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης εγγεγραμμένος στην Ελλάδα και καταχωρισμένος στην Ευρωπαική Λίστα Παρόχων Εμπιστοσύνης. Όλοι οι έλεγχοι λειτουργίας, διαχείρισης και λειτουργίας που σχετίζονται με την JCC Payment Systems ΑΠ και περιγράφονται παρακάτω παρέχονται από την ADACOM SA.

5.1.1 Τοποθεσία και κατασκευή του χώρου

Οι λειτουργίες των ΑΠ και ΑΕ της JCC Payment Systems διενεργούνται εντός ενός φυσικά προστατευόμενου περιβάλλοντος το οποίο αποτρέπει, προλαμβάνει και εντοπίζει τη μη εξουσιοδοτημένη χρήση και πρόσβαση σε εσωτερικά ή εξωτερικά συστήματα και ευαίσθητες πληροφορίες ή την αποκάλυψη αυτών.

Η JCC Payment Systems διατηρεί εγκαταστάσεις Αποκατάστασης Καταστροφών όσον αφορά τις λειτουργίες ΑΠ. Οι εγκαταστάσεις Αποκατάστασης Καταστροφών της JCC Payment Systems προστατεύονται από πολλαπλά επίπεδα φυσικής ασφάλειας συγκρίσιμα προς αυτά της κύριας εγκατάστασης της JCC Payment Systems.

5.1.2 Φυσική πρόσβαση

Τα συστήματα της ΑΠ της JCC Payment Systems προστατεύονται από επτά (7) επίπεδα φυσικής ασφάλειας, όπου απαιτείται η απόκτηση πρόσβασης στο χαμηλότερο επίπεδο ασφάλειας πριν δοθεί η πρόσβαση σε υψηλότερο επίπεδο.

Η προοδευτική περιοριστική προνομιακή φυσική πρόσβαση ελέγχει την πρόσβαση σε κάθε επίπεδο ασφάλειας. Οι ευαίσθητες λειτουργίες της ΑΠ, κάθε δραστηριότητα που σχετίζεται με τον κύκλο ζωής της διαδικασίας πιστοποίησης, όπως η πιστοποίηση γνησιότητας, η εξακρίβωση και η έκδοση, διενεργούνται εντός ενός αυστηρώς περιορισμένου φυσικού χώρου. Η πρόσβαση σε κάθε επίπεδο απαιτεί τη χρήση ειδικής κάρτας πρόσβασης (proximity card) από τους υπαλλήλους. Η φυσική πρόσβαση καταγράφεται και βιντεοσκοπείται αυτόματα. Για τη φυσική πρόσβαση σε ορισμένα επίπεδα ασφάλειας απαιτείται η ταυτόχρονη χρήση των ειδικών καρτών πρόσβασης και των βιομετρικών στοιχείων (επαλήθευση ταυτότητας με δύο παραμέτρους). Δεν επιτρέπεται η πρόσβαση προσωπικού άνευ συνοδείας, συμπεριλαμβανομένων των μη έμπιστων υπαλλήλων ή επισκεπτών, σε αυτούς τους χώρους ασφάλειας.

Το σύστημα φυσικής ασφάλειας περιλαμβάνει επίπεδα για την ασφάλεια της διαχείρισης των κλειδιών τα οποία εξυπηρετούν για την προστασία τόσο της αποθήκευσης με σύνδεση (online) όσο και της αποθήκευσης εκτός σύνδεσης (offline) των Κρυπτογραφικών Μονάδων Υπογραφών (ΚΜΥ) και του υλικού δημιουργίας κλειδιών. Οι χώροι που χρησιμοποιούνται για τη δημιουργία και την αποθήκευση κρυπτογραφικού υλικού απαιτούν διπλό έλεγχο, ο κάθε έλεγχος διενεργείται μέσω της ταυτόχρονης χρήσης των ειδικών καρτών πρόσβασης και των βιομετρικών στοιχείων. Οι ΚΜΥ σε σύνδεση (Online) προστατεύονται μέσω της χρήσης κλειδωμένων ερμαριών. Οι ΚΜΥ εκτός σύνδεσης (Offline) προστατεύονται μέσω της χρήσης κλειδωμένων θυρίδων, ερμαριών και κιβωτίων. Η πρόσβαση στις ΚΜΥ και το υλικό δημιουργίας κλειδιών είναι περιορισμένη σύμφωνα με τις απαιτήσεις που αφορούν τον διαχωρισμό των καθηκόντων της JCC Payment Systems . Το άνοιγμα και το κλείσιμο των ερμαριών και θυρίδων στα εν λόγω επίπεδα, καταγράφεται για τους σκοπούς του ελέγχου συμμόρφωσης.

Οι λειτουργίες της ΑΕ της JCC Payment Systems προστατεύονται με χρήση ελέγχου φυσικής πρόσβασης καθιστώντας την προσβάσιμη μόνο από τους εξουσιοδοτημένους υπαλλήλους. Η πρόσβαση σε ασφαλείς χώρους του κτιρίου απαιτεί τη χρήση κάρτας πρόσβασης και κωδικού πρόσβασης. Η χρήση της κάρτας πρόσβασης καταγράφεται στο κεντρικό σύστημα ελέγχου του κτιρίου.

Η καταγραφή της κάρτας πρόσβασης καθώς και το υλικό των καμερών παρακολουθούνται σε πραγματικό χρόνο, σε βάση 24Χ7, από φύλακα, καθώς περιοδικά ελέγχονται και από το τμήμα Απάτης & Ασφάλειας. Επιπλέον ο χώρος εργασίας της ΑΕ προστατεύεται με PIR και κλειδώνεται με συναγερμό. Η JCC Payment Systems, αποθηκεύει με ασφάλεια όλα τα χαρτιά που περιέχουν ευαίσθητες πληροφορίες σε μορφή απλού κειμένου σχετικά με τις λειτουργείες της ΑΕ, σε ένα ασφαλή χώρο.

Η JCC Payment Systems αποθηκεύει με ασφάλεια τις Κρυπτογραφικές Μονάδες Υπογραφών (ΚΜΥ) που χρησιμοποιούνται για τη δημιουργία και αποθήκευση των ιδιωτικών κλειδιών των εξ αποστάσεως Ψηφιακών Υπογραφών και της ταυτοποίησης των Συνδρομητών. Η πρόσβαση στους χώρους που χρησιμοποιούνται για την αποθήκευση και δημιουργία των κλειδιών ελέγχεται και καταγράφεται από το κεντρικό σύστημα ελέγχου πρόσβασης του κτιρίου. Οι καταγραφές χρήσης καρτών και αρχείων εικόνας ελέγχονται συστηματικά.

5.1.3 Παροχή ηλεκτρικού ρεύματος και κλιματισμός

Οι ασφαλείς εγκαταστάσεις της JCC Payment Systems είναι εξοπλισμένες με κύρια και εφεδρικά:

- συστήματα παροχής ισχύος για την εξασφάλιση της συνεχούς και αδιάλειπτης παροχής ηλεκτρικού ρεύματος και
- συστήματα θέρμανσης/ εξαερισμού/ κλιματισμού για τον έλεγχο της θερμοκρασίας και της σχετικής υγρασίας.

5.1.4 Έκθεση σε νερό

Όλες οι ασφαλείς εγκαταστάσεις είναι εξοπλισμένες με συστήματα παρακολούθησης, για την ανίχνευση υπερβολικής υγρασίας και την ελαχιστοποίηση της επίδρασης της έκθεσης του νερού

5.1.5 Πρόληψη και προστασία από πυρκαγιά

Όλες οι ασφαλείς εγκαταστάσεις είναι εξοπλισμένες με μηχανισμούς καταστολής πυρκαγιάς για την πρόληψη και την κατάσβεση πυρκαγιών ή άλλου είδους επιβλαβή έκθεση σε φλόγα ή καπνό.

5.1.6 Αποθήκευση μέσων

Όλα τα μέσα που περιέχουν τις πληροφορίες για το λογισμικό και τα δεδομένα παραγωγής, για τους ελέγχους, τα αρχεία ή τα εφεδρικά αντίγραφα αποθηκεύονται εντός των εγκαταστάσεων της JCC Payment Systems ή σε ασφαλή εγκατάσταση αποθήκευσης, εκτός του χώρου εγκατάστασης της JCC Payment Systems η οποία διαθέτει τα απαραίτητα φυσικά και λογικά μέτρα ελέγχου πρόσβασης. Τα μέτρα αυτά έχουν σχεδιαστεί ώστε να περιορίζουν την πρόσβαση αποκλειστικά σε εξουσιοδοτημένο προσωπικό και να προστατεύουν τα εν λόγω μέσα αποθήκευσης έναντι οιασδήποτε τυχαίας καταστροφής (π.χ. από νερό, φωτιά).

5.1.7 Διάθεση αποβλήτων

Τα ευαίσθητα έγγραφα και υλικά περνάνε σε καταστροφέα εγγράφων πριν από την απόρριψή τους. Τα μέσα που χρησιμοποιήθηκαν για τη συλλογή ή τη μεταβίβαση ευαίσθητων πληροφοριών καθίστανται μη αναγνώσιμα πριν από την απόρριψή τους. Οι διατάξεις κρυπτογράφησης καταστρέφονται με τρόπο ή διαγράφονται τα δεδομένα τους σύμφωνα με τις οδηγίες του κατασκευαστή πριν από την απόρριψή τους.

5.1.8 Δημιουργία εφεδρικών αντιγράφων ασφαλείας εκτός του χώρου εγκατάστασης

Η JCC Payment Systems δημιουργεί σε τακτά διαστήματα εφεδρικά αντίγραφα για τα δεδομένα των κυριότερων συστημάτων, τα δεδομένα αρχείων καταγραφής ελέγχου και άλλων ευαίσθητων πληροφοριών. Τα εφεδρικά αντίγραφα αποθηκεύονται με φυσικά μέσα προστασίας, χρησιμοποιώντας την Εγκατάσταση Αποκατάστασης Καταστροφών της JCC Payment Systems.
Τα εφεδρικά αντίγραφα ασφαλείας των ιδιωτικών κλειδιών της ΑΠ και τα δεδομένα ενεργοποίησης αποθηκεύονται για λόγους αποκατάστασης με φυσικά μέσα προστασίας, χρησιμοποιώντας την Εγκατάσταση Αποκατάστασης Καταστροφών της ADACOM.

5.1.9 Εξωτερικά Συστήματα Αρχής Εγγραφής

Όλες οι απαιτήσεις φυσικού ελέγχου, σύμφωνα με την ενότητα 5.1 ισχύουν εξίσου για οποιοδήποτε εξωτερικό σύστημα ΑΕ

5.2 *Διαδικαστικοί έλεγχοι*

5.2.1 Ρόλοι εμπιστοσύνης

Ως Έμπιστα Πρόσωπα θεωρούνται όλοι οι υπάλληλοι οι οποίοι έχουν πρόσβαση ή ελέγχουν τις λειτουργίες επαλήθευσης ταυτότητας ή τις κρυπτογραφικές λειτουργίες και οι οποίοι θα μπορούσαν να επηρεάσουν σε σημαντικό βαθμό τα εξής:

- την επικύρωση των στοιχείων στις Αιτήσεις για Πιστοποιητικό,

- την αποδοχή, την απόρριψη ή άλλη επεξεργασία των Αιτήσεων για Πιστοποιητικό, των αιτημάτων για ανάκληση ή των αιτημάτων για επαναδημιουργία κλειδιών ή των πληροφοριών εγγραφής,
- την έκδοση ή την ανάκληση Πιστοποιητικών, συμπεριλαμβανομένου του προσωπικού που έχει πρόσβαση στα τμήματα περιορισμένης πρόσβασης του χώρου αποθήκευσής της,
- τον χειρισμό των στοιχείων ή των αιτημάτων των Συνδρομητών.

Ως Έμπιστα Πρόσωπα θεωρούνται ενδεικτικά:

- το προσωπικό της ΑΕ και της ΤΑΕ,
- το προσωπικό που εμπλέκεται στις διαδικασίες διαχείρισης κλειδιών,
- το προσωπικό ασφαλείας,
- το προσωπικό διαχείρισης συστημάτων, και
- τα στελέχη στα οποία έχει ανατεθεί η διαχείριση της αξιοπιστίας της υποδομής.

Η JCC Payment Systems θεωρεί τις κατηγορίες του προσωπικού που προσδιορίζονται στην παρούσα ενότητα ως Έμπιστα Πρόσωπα τα οποία κατέχουν Θέση Εμπιστοσύνης. Τα πρόσωπα που επιθυμούν να αποκτήσουν την ιδιότητα του Έμπιστου Προσώπου αποκτώντας μια Θέση Εμπιστοσύνης πρέπει να πληρούν επιτυχώς τις απαιτήσεις ελέγχου ασφαλείας της παρούσας ΠΠ και της σχετικής ΔΠΠ.

Οι λειτουργίες και τα καθήκοντα που εκτελούνται από άτομα σε αξιόπιστους ρόλους κατανέμονται έτσι ώστε κανένα άτομο μόνο του να μην μπορεί να παρακάμψει τα μέτρα ασφαλείας ή να υπονομεύσει την ασφάλεια και την αξιοπιστία των λειτουργιών της ΥΔΚ.

5.2.2 Αριθμός προσώπων που απαιτούνται ανά τομέα εργασίας

Η JCC Payment Systems έχει θεσπίσει, διατηρεί και επιβάλλει αυστηρές διαδικασίες ελέγχου προκειμένου να διασφαλίσει τον διαχωρισμό των καθηκόντων βάσει των αρμοδιοτήτων κάθε θέσης εργασίας και να εξασφαλίσει ότι για την εκτέλεση ευαίσθητων εργασιών απαιτείται η συμμετοχή πολλών Έμπιστων Προσώπων.

Εφαρμόζονται πολιτικές και διαδικασίες ελέγχου προκειμένου να διασφαλιστεί ο διαχωρισμός των καθηκόντων βάσει των αρμοδιοτήτων κάθε θέσης εργασίας. Οι πιο ευαίσθητες εργασίες, όπως είναι η πρόσβαση και ο χειρισμός του κρυπτογραφικού εξοπλισμού (ΑΚΜ) της ΑΠ και του σχετικού υλικού των κλειδιών, απαιτούν τη συμμετοχή πολλών Έμπιστων Προσώπων.

Αυτές οι εσωτερικές διαδικασίες ελέγχου έχουν σχεδιαστεί με τρόπο τέτοιο ώστε να διασφαλίζουν ότι τουλάχιστον δύο Έμπιστα Πρόσωπα του προσωπικού πρέπει να διαθέτουν φυσική ή λογική πρόσβαση στη διάταξη. Η πρόσβαση στον κρυπτογραφικό εξοπλισμό της ΑΠ πραγματοποιείται αυστηρά από πολλαπλά Έμπιστα Πρόσωπα καθ' όλη τη διάρκεια ζωής του, από την παραλαβή και τον έλεγχό του μέχρι την τελική λογική ή/και φυσική καταστροφή του. Μόλις μια μονάδα ενεργοποιηθεί με τα κλειδιά λειτουργίας, εφαρμόζονται περαιτέρω μέτρα ελέγχου πρόσβασης ώστε να υπάρχει διαμοιρασμένος έλεγχος τόσο της φυσικής όσο και της λογικής πρόσβασης στη διάταξη. Τα πρόσωπα που έχουν φυσική πρόσβαση σε μονάδες δεν κατέχουν «Μερίδια Απορρήτου» και αντιστρόφως.

5.2.3 Ταυτοποίηση και επαλήθευση της ταυτότητας για κάθε ρόλο

Για τα μέλη του προσωπικού που επιθυμούν να καταστούν Έμπιστα Πρόσωπα, η εξακρίβωση της ταυτότητας διενεργείται μέσω της διαδικασίας του Ανθρώπινου Δυναμικού της JCC Payment Systems βάσει ελέγχων ευρέως αναγνωρισμένων μορφών ταυτοποίησης (π.χ., διαβατήρια ή δελτία ταυτότητας). Η ταυτότητα επαληθεύεται περαιτέρω με τις διαδικασίες ελέγχου του ιστορικού, σύμφωνα με την ενότητα 5.3.2.

Η JCC Payment Systems διασφαλίζει ότι το προσωπικό έχει αποκτήσει την ιδιότητα του Έμπιστου και έχει ήδη χορηγηθεί η έγκριση του αρμόδιου τμήματος, προτού στο συγκεκριμένο προσωπικό:

- εκδοθούν διατάξεις πρόσβασης και χορηγηθούν άδειες πρόσβασης στις απαιτούμενες εγκαταστάσεις,

- εκδοθούν ηλεκτρονικά διαπιστευτήρια για την πρόσβαση και την τέλεση συγκεκριμένων λειτουργιών της ΑΠ, της ΑΕ ή άλλων πληροφοριακών συστημάτων της JCC Payment Systems.

Η JCC Payment Systems έχει υλοποιήσει ένα σύστημα ελέγχου πρόσβασης το οποίο ταυτοποιεί τις αρχές και καταχωρεί όλους τους χρήστες των πληροφοριακών συστημάτων της JCC Payment Systems κατά τρόπο αξιόπιστο.

Δημιουργούνται λογαριασμοί χρηστών για το προσωπικό σε συγκεκριμένους ρόλους που απαιτούν πρόσβαση στο σχετικό σύστημα. Όλοι οι χρήστες πρέπει να συνδέονται με συγκεκριμένο λογαριασμό και οι εντολές διαχείρισης είναι διαθέσιμες μόνο με ρητή άδεια και έλεγχο της εκτέλεσης. Οι άδειες του συστήματος αρχείων, καθώς και άλλες διαθέσιμες δυνατότητες στο μοντέλο ασφάλειας του λειτουργικού συστήματος χρησιμοποιούνται για να αποτραπεί οποιαδήποτε άλλη χρήση.

Οι λογαριασμοί χρηστών κλειδώνονται το συντομότερο δυνατό όταν το επιβάλει η αλλαγή των ρόλων. Οι κανόνες που αφορούν την ασφάλεια ελέγχονται ετησίως.

5.2.4 Ρόλοι που απαιτούν διαχωρισμό καθηκόντων

Οι ρόλοι που απαιτούν τον διαχωρισμό καθηκόντων περιλαμβάνουν, ενδεικτικά, τα εξής:

- την επικύρωση και τον χειρισμό των στοιχείων στις Αιτήσεις για Πιστοποιητικό,
- την αποδοχή, την απόρριψη ή άλλη επεξεργασία των Αιτήσεων για Πιστοποιητικό, των αιτημάτων για ανάκληση ή των αιτημάτων για επαναδημιουργία κλειδιών ή των πληροφοριών εγγραφής,
- τη δημιουργία, την έκδοση ή την καταστροφή ενός πιστοποιητικού της ΑΠ,
- Την πρόσβαση σε εξ αποστάσεως ΕΔΔΥ

Για την επίτευξη αυτού του διαχωρισμού καθηκόντων, η JCC Payment Systems ορίζει άτομα σε αξιόπιστους ρόλους, περιορίζοντας έναν υπάλληλο από το να αναλάβει πολλαπλούς ρόλους, αποτρέποντας έτσι το να έχει περισσότερες από μία ταυτότητες.

5.3 *Έλεγχοι προσωπικού*

Το προσωπικό που πρόκειται να αποκτήσει την ιδιότητα του Έμπιστου Προσώπου πρέπει να προσκομίζει το απαιτούμενο υπόβαθρο του, τα τυπικά του προσόντα και την εμπειρία που απαιτούνται για την εκτέλεση των καθηκόντων της επιδιωκόμενης θέσης με επαρκή και ικανοποιητικό τρόπο, καθώς και αποδεικτικά στοιχεία από κρατική εξουσιοδότηση, εάν υπάρχει, που είναι απαραίτητη για την εκτέλεση υπηρεσιών πιστοποίησης δυνάμει κρατικών συμβάσεων. Για το προσωπικό που κατέχει Θέσεις Εμπιστοσύνης, οι έλεγχοι ιστορικού επαναλαμβάνονται τουλάχιστον κάθε πέντε (5) έτη.

5.3.1 Απαιτήσεις σχετικά με τα προσόντα, την εμπειρία και την εξουσιοδότηση

Η JCC Payment Systems ζητά από το προσωπικό που πρόκειται να αποκτήσει την ιδιότητα του Έμπιστου Προσώπου να προσκομίσει τα απαραίτητα αποδεικτικά στοιχεία για το ιστορικό του, τα τυπικά του προσόντα και την εμπειρία που απαιτούνται για την εκτέλεση των καθηκόντων της επιδιωκόμενης θέσης, όπως ορίζονται στα έγγραφα της σύμβασης απασχόλησης, της περιγραφής της θέσης εργασίας και των ρόλων και αρμοδιοτήτων με επαρκή και ικανοποιητικό τρόπο, καθώς και αποδεικτικά στοιχεία από κρατική εξουσιοδότηση, εάν υπάρχει, που είναι απαραίτητη για την εκτέλεση των υπηρεσιών πιστοποίησης δυνάμει κρατικών συμβάσεων προτού εκτελεστεί οποιαδήποτε επιχειρησιακή λειτουργία ή λειτουργία για την ασφάλεια.

Οι συμβάσεις απασχόλησης που είναι υπογεγραμμένες από τους υπαλλήλους της JCC Payment Systems προβλέπουν τις ακόλουθες υποχρεώσεις:

- τη διατήρηση του απορρήτου των εμπιστευτικών πληροφοριών που έχουν λάβει γνώση κατά την εκτέλεση των καθηκόντων τους,
- την αποτροπή κατοχής επιχειρηματικών συμφερόντων σε μια εταιρεία που μπορεί να επηρεάσει την κρίση τους όσον αφορά την παροχή της υπηρεσίας και τη διασφάλιση ότι δεν έχουν τιμωρηθεί για έγκλημα που έχουν διαπράξει με δόλο.

- Όλα τα μέλη του προσωπικού σε Ρόλους Εμπιστοσύνης δεν έχουν συμφέροντα που δύνανται να επηρεάσουν την αμεροληψία τους αναφορικά με τις δραστηριότητες της JCC Payment Systems .

5.3.2 Διαδικασίες ελέγχου ιστορικού

Πριν από την έναρξη απασχόλησης σε Ρόλο Εμπιστοσύνης, η JCC Payment Systems διενεργεί έλεγχο ιστορικού ο οποίος περιλαμβάνει τα ακόλουθα:

- την επαλήθευση της ταυτότητας,
- τον έλεγχο της προηγούμενης απασχόλησης και των επαγγελματικών συστάσεων (εφόσον είναι διαθέσιμες),
- την επιβεβαίωση του ανώτερου ή του πιο πρόσφατου πτυχίου εκπαίδευσης,
- την βεβαίωση ότι οι υπάλληλοι πληρούν τις απαιτήσεις γνώσεων, δεξιοτήτων, αξιοπιστίας και εμπειρίας.

Στο μέτρο που οι απαιτήσεις που επιβάλλονται από την παρούσα ενότητα δεν δύνανται να ικανοποιηθούν εξαιτίας απαγόρευσης ή περιορισμού της ισχύουσας νομοθεσίας ή άλλων συνθηκών, η JCC Payment Systems θα χρησιμοποιήσει μια υποκατάστατη διερευνητική τεχνική η οποία επιτρέπεται από τον νόμο και παρέχει παρόμοιες πληροφορίες.

Στοιχεία που αποκαλύπτονται κατά τον έλεγχο ιστορικού και τα οποία μπορούν να αποτελέσουν τη βάση για απόρριψη υποψηφίων από Θέσεις Εμπιστοσύνης ή για τη λήψη μέτρων κατά υφιστάμενου Έμπιστου Προσώπου περιλαμβάνουν γενικά (ενδεικτικά) τα εξής:

- τις ψευδείς δηλώσεις που πραγματοποίησε ο υποψήφιος ή το Έμπιστο Πρόσωπο,
- τις ιδιαίτερα δυσμενείς ή αναξιόπιστες προσωπικές συστάσεις, και
- τις καταδίκες για ορισμένα ποινικά αδικήματα

Οι αναφορές που περιλαμβάνουν τέτοιου είδους πληροφορίες αξιολογούνται από το προσωπικό της διεύθυνσης ανθρώπινου δυναμικού και του τομέα ασφάλειας, το οποίο προσδιορίζει τις απαραίτητες ενέργειες ανάλογα με τη μορφή, τη σπουδαιότητα, και τη συχνότητα της συμπεριφοράς που αποκαλύπτεται από τον έλεγχο του ιστορικού. Οι ενέργειες αυτές δύνανται να περιλαμβάνουν μέτρα που αφορούν έως και την ακύρωση της προσφοράς εργασίας στον υποψήφιο για τη Θέση Εμπιστοσύνης ή την καταγγελία της σύμβασης των υφιστάμενων Έμπιστων Προσώπων.

Η χρήση των πληροφοριών που αποκαλύπτονται κατά τον έλεγχο του ιστορικού ώστε να ληφθούν οι σχετικές ενέργειες, υπόκειται στην ισχύουσα νομοθεσία.

5.3.3 Απαιτήσεις εκπαίδευσης

Η JCC Payment Systems , με την πρόσληψη, παρέχει στο προσωπικό της εκπαίδευση, καθώς και κατά τη διάρκεια της εργασίας, η οποία κρίνεται απαραίτητη για την εκτέλεση των εργασιακών καθηκόντων τους με επαρκή και ικανοποιητικό τρόπο. Η JCC Payment Systems διατηρεί αρχεία για τις εκπαιδεύσεις αυτές. Η JCC Payment Systems αναθεωρεί και βελτιώνει περιοδικά τα εκπαιδευτικά της προγράμματα ανάλογα με τις ανάγκες της.

Τα εκπαιδευτικά προγράμματα της JCC Payment Systems είναι προσαρμοσμένα στις αρμοδιότητες του ατόμου και περιλαμβάνουν τα ακόλουθα:

- τις βασικές έννοιες της ΥΔΚ,
- τις αρμοδιότητες των θέσεων εργασίας,
- την πολιτική και τις διαδικασίες ασφάλειας και λειτουργίας της JCC Payment Systems ,
- τη χρήση και λειτουργία του εξοπλισμού και λογισμικού που έχει αναπτυχθεί,
- την αναφορά και αντιμετώπιση περιστατικών και της Έκθεσης σε Κίνδυνο και
- την αποκατάσταση καταστροφών και τις διαδικασίες συνέχισης επιχειρηματικής δραστηριότητας.

5.3.4 Συχνότητα και απαιτήσεις επανεκπαίδευσης

Η JCC Payment Systems παρέχει επανεκπαίδευση και ενημέρωση για τις σύγχρονες εξελίξεις στο προσωπικό της στον βαθμό και τη συχνότητα που απαιτείται προκειμένου να διασφαλιστεί ότι το εν λόγω προσωπικό διατηρεί το απαιτούμενο επίπεδο επάρκειας γνώσεων ώστε να εκτελεί τα καθήκοντα του με επαρκή και ικανοποιητικό τρόπο.

Η JCC Payment Systems παρέχει επανεκπαίδευση στο εξουσιοδοτημένο προσωπικό της ΑΕ και της ΤΑΕ σε ετήσια βάση.

5.3.5 Συχνότητα και ακολουθία εναλλαγής θέσεων εργασίας

Η εναλλαγή θέσεων δεν εφαρμόζεται.

5.3.6 Κυρώσεις για μη εξουσιοδοτημένες ενέργειες

Λαμβάνονται κατάλληλες πειθαρχικές ενέργειες για υπαλλήλους και πράκτορες που δεν συμμορφώνονται με την παρούσα ΠΠ και την εφαρμοστέα ΔΠΠ, για μη εξουσιοδοτημένες ενέργειες ή άλλες παραβιάσεις των πολιτικών και διαδικασιών της JCC Payment Systems. Οι πειθαρχικές ενέργειες μπορεί να περιλαμβάνουν μέτρα μέχρι και την απόλυση και είναι ανάλογες με τη συχνότητα και τη σοβαρότητα των μη εξουσιοδοτημένων ενεργειών.

5.3.7 Απαιτήσεις ανεξάρτητου αναδόχου

Σε περιορισμένες περιπτώσεις, ανεξάρτητοι ανάδοχοι ή σύμβουλοι δύνανται να χρησιμοποιούνται για την πλήρωση Θέσεων Εμπιστοσύνης. Οποιοσδήποτε σχετικός ανεξάρτητος ανάδοχος ή σύμβουλος υπόκειται στα ίδια λειτουργικά κριτήρια και κριτήρια ασφαλείας που ισχύουν και για τους εργαζομένους της JCC Payment Systems που κατέχουν ανάλογη θέση.

Σε ανεξάρτητους αναδόχους και συμβούλους για τους οποίους δεν έχουν ολοκληρωθεί οι διαδικασίες ελέγχου του ιστορικού που προσδιορίζονται στην ενότητα 5.3.2, η πρόσβαση στις ασφαλείς εγκαταστάσεις της JCC Payment Systems επιτρέπεται μόνον εφόσον οι ανωτέρω αναφερόμενοι συνοδεύονται και επιβλέπονται άμεσα και συνεχώς από Έμπιστα Πρόσωπα.

5.3.8 Έντυπα που διατίθενται στο προσωπικό

Η JCC Payment Systems παρέχει στους υπαλλήλους της την απαιτούμενη εκπαιδευτική και άλλη τεκμηρίωση που είναι απαραίτητη για την εκτέλεση των αρμοδιοτήτων της θέσης εργασίας τους με επαρκή και ικανοποιητικό τρόπο, συμπεριλαμβανομένου αντιγράφου της παρούσας ΠΠ και άλλων τεχνικών και επιχειρησιακών εγγράφων που απαιτούνται για τη διατήρηση της ακεραιότητας των λειτουργιών της ΑΠ της JCC Payment Systems. Οι εργαζόμενοι έχουν επίσης πρόσβαση σε πληροφορίες σχετικά με τα εσωτερικά συστήματα και την ασφάλεια, τις διαδικασίες επαλήθευσης ταυτότητας (ταυτοποίησης) και άλλες σχετικές πληροφορίες.

5.4 *Διαδικασίες καταγραφής ελέγχου*

5.4.1 Τύποι συμβάντων που καταγράφονται

Η JCC Payment Systems διασφαλίζει ότι όλες οι σχετικές πληροφορίες που αφορούν τη λειτουργία των Υπηρεσιών Εμπιστοσύνης καταγράφονται για την παροχή αποδεικτικών στοιχείων για τον σκοπό νομικών διαδικασιών. Οι εν λόγω πληροφορίες περιλαμβάνουν την τήρηση αρχείων που απαιτείται για την απόδειξη της εγκυρότητας της λειτουργίας της Υπηρεσίας Εμπιστοσύνης.

Η JCC Payment Systems καταγράφει είτε αυτόματα είτε όχι (χειροκίνητα) τα ακόλουθα σημαντικά περιστατικά:

- Συμβάντα διαχείρισης του πιστοποιητικού της ΑΠ και του κύκλου ζωής κλειδιού της, συμπεριλαμβανομένων των εξής:
  - της παραγωγής, δημιουργίας εφεδρικών αντιγράφων, αποθήκευσης, ανάκτησης, αρχειοθέτησης, και καταστροφής κλειδιών,
  - των αλλαγών σε στοιχεία ή κλειδιά της ΑΠ,
  - των συμβάντων διαχείρισης του κύκλου ζωής κρυπτογραφικής διάταξης.
- Συμβάντα διαχείρισης πιστοποιητικών Συνδρομητών και του κύκλου ζωής των κλειδιών τους, συμπεριλαμβανομένων των εξής:
  - δημιουργία κλειδιών, εφεδρικού αντιγράφου ασφαλείας, αποθήκευση, ανάκτηση, αρχειοθέτηση και καταστροφή
  - των Αιτήσεων για Πιστοποιητικό, της ανανέωσης, της επαναδημιουργίας κλειδιού και της ανάκλησης,
  - της επιτυχούς ή μη επιτυχούς επεξεργασίας αιτημάτων,
  - των αλλαγών στις πολιτικές δημιουργίας πιστοποιητικών,
  - της παραγωγής και έκδοσης Πιστοποιητικών και ΚΑΠ.
- Συμβάντα σχετικά με Έμπιστους Υπάλληλους, συμπεριλαμβανομένων των εξής:
  - των προσπαθειών σύνδεσης και αποσύνδεσης,
  - των προσπαθειών δημιουργίας, αφαίρεσης, ορισμού κωδικών πρόσβασης ή της αλλαγής των δικαιωμάτων συστήματος οποιουδήποτε προνομιούχου χρήστη,
  - των αλλαγών στο προσωπικό.
- Όλα τα σημαντικά συμβάντα που σχετίζονται με την ασφάλεια, συμπεριλαμβανομένων των εξής:
  - των επιτυχών και μη επιτυχών προσπαθειών πρόσβασης στο σύστημα της ΥΔΚ,
  - της έναρξης και του τερματισμού των συστημάτων και των εφαρμογών,
  - της κατοχής δεδομένων ενεργοποίησης για τις λειτουργίες του ιδιωτικού κλειδιού της ΑΠ,
  - των αλλαγών διαμόρφωσης και της συντήρησης του συστήματος,
  - των ενεργειών του συστήματος ασφαλείας και της ΥΔΚ οι οποίες εκτελούνται από το προσωπικό της JCC Payment Systems ,
  - της ανάγνωσης, της εγγραφής ή διαγραφής ευαίσθητων από άποψη ασφάλειας φακέλων ή αρχείων,
  - των αλλαγών των ρυθμίσεων της πολιτικής ασφάλειας,
  - των σφαλμάτων του συστήματος, της αποτυχίας υλικού και άλλων ανωμαλιών,
  - της δραστηριότητας του τείχους προστασίας και του δρομολογητή,
  - Έλεγχος εισόδου/εξόδου εγκαταστάσεων εξ αποστάσεως ΕΔΔΥ

Οι καταχωρίσεις των αρχείων καταγραφής περιλαμβάνουν τα ακόλουθα στοιχεία:

- την ημερομηνία και την ώρα της καταχώρισης
- τον σειριακό ή αύξοντα αριθμό καταχώρισης, για αυτόματες καταχωρίσεις,
- τα στοιχεία ταυτότητας του προσώπου που κάνει την καταχώριση,
- το είδος καταχώρισης.

Η ΑΕ και η ΤΑΕ της JCC Payment Systems καταγράφει τα στοιχεία των Αιτήσεων για Πιστοποιητικό, συμπεριλαμβανομένων των εξής:

- του είδους του(των) εγγράφου(ων) ταυτοποίησης που προσκομίζεται(ονται) από τον Αιτούντα Πιστοποιητικό·
- της καταγραφής των αποκλειστικών αναγνωριστικών δεδομένων, των αριθμών ή του συνδυασμού των συγκεκριμένων εγγράφων ταυτοποίησης (π.χ. του αριθμού του δελτίου ταυτότητας του Αιτούντος Πιστοποιητικό), εφόσον ισχύει· της τοποθεσίας αποθήκευσης των αντιγράφων των αιτήσεων και των εγγράφων ταυτοποίησης για τα Εγκεκριμένα Πιστοποιητικά·
- οποιωνδήποτε συγκεκριμένων επιλογών στην Αίτηση για Πιστοποιητικό·
- της ταυτότητας της οντότητας που αποδέχεται την αίτηση και, στην περίπτωση των εγκεκριμένων ηλεκτρονικών σφραγίδων , της ταυτότητας του φυσικού προσώπου που εκπροσωπεί το νομικό πρόσωπο στο οποίο παρέχεται το Εγκεκριμένο Πιστοποιητικό ηλεκτρονικών σφραγίδων ·

- της μεθόδου που εφαρμόστηκε για την επικύρωση των εγγράφων ταυτοποίησης, εφόσον υπάρχει·
- του ονόματος της λαμβάνουσας ΑΠ ή της υποβάλλουσας ΑΕ και ΤΑΕ, εφόσον ισχύει.

5.4.2 Συχνότητα επεξεργασίας των αρχείων καταγραφής

Τα συστήματα της JCC Payment Systems παρακολουθούνται συνεχώς παρέχοντας σε πραγματικό χρόνο ειδοποιήσεις για σημαντικά συμβάντα ασφάλειας και λειτουργίας για τους σκοπούς του ελέγχου μέσω εξουσιοδοτημένου προσωπικού υπεύθυνου για την ασφάλεια του συστήματος. Οι μηνιαίες ανασκοπήσεις των αρχείων καταγραφής περιλαμβάνουν την επαλήθευση ότι δεν έχει σημειωθεί παραποίηση των αρχείων καταγραφής και διενεργείται ενδελεχής έλεγχος για τυχόν προειδοποιήσεις ή παρατυπίες στα αρχεία καταγραφής. Οι ενέργειες που λαμβάνονται βάσει των ανασκοπήσεων των αρχείων καταγραφής ελέγχου επίσης τεκμηριώνονται.

5.4.3 Περίοδος διατήρησης αρχείου καταγραφής ελέγχων

Τα αρχεία καταγραφής ελέγχων τηρούνται τουλάχιστον για δύο (2) μήνες μετά την επεξεργασία και, στη συνέχεια, αρχειοθετούνται σύμφωνα με την ενότητα 5.5.

Τα φυσικά ή ψηφιακά αρχεία σχετικά με τις αιτήσεις για πιστοποιητικά, τις πληροφορίες εγγραφής και τα αιτήματα ή τις αιτήσεις για ανάκληση φυλάσσονται για τουλάχιστον επτά (7) έτη μετά τη λήξη ισχύος οποιουδήποτε πιστοποιητικού βάσει των εν λόγω αρχείων.

Σε περίπτωση τερματισμού της λειτουργίας της ΑΠ, τα αρχεία καταγραφής και τα αρχεία της JCC Payment Systems φυλάσσονται και είναι προσβάσιμα έως την ανωτέρω αναφερόμενη περίοδο διατήρησης σύμφωνα με την ενότητα 5.8.

5.4.4 Προστασία του αρχείου καταγραφής ελέγχου

Τα αρχεία καταγραφής ελέγχων προστατεύονται από ένα ηλεκτρονικό σύστημα αρχείων καταγραφής ελέγχου το οποίο περιλαμβάνει μηχανισμούς προστασίας των αρχείων καταγραφής από τη μη-εξουσιοδοτημένη προβολή, τροποποίηση, διαγραφή ή άλλη παραποίηση.

5.4.5 Διαδικασίες εφεδρικών αντιγράφων των αρχείων καταγραφής ελέγχων

Επαυξητικοί (incremental backups) ή άλλοι τύποι αντιγράφων ασφαλείας των αρχείων καταγραφής ελέγχων δημιουργούνται καθημερινά ενώ πλήρη αντίγραφα ασφαλείας παράγονται σε εβδομαδιαία βάση.

5.4.6 Σύστημα συλλογής αρχείων ελέγχου (Εσωτερικό - Εξωτερικό)

Αυτοματοποιημένα δεδομένα ελέγχου παράγονται και καταγράφονται σε επίπεδο εφαρμογής, δικτύου και λειτουργικού συστήματος. Τα μη αυτοματοποιημένα δεδομένα ελέγχου καταγράφονται από το προσωπικό της JCC Payment Systems οι οποίοι κατέχουν Ρόλους Εμπιστοσύνης.

5.4.7 Κοινοποίηση στο υποκείμενο που προκάλεσε το συμβάν

Στην περίπτωση καταγραφής συμβάντος από το σύστημα συλλογής ελέγχων, δεν είναι απαραίτητη η ειδοποίηση του φυσικού προσώπου, του οργανισμού, της διάταξης ή της εφαρμογής που προκάλεσε το συμβάν, εκτός και εάν η σχετική ειδοποίηση είναι υποχρεωτική βάσει νόμου.

Εάν τα αρχεία αφορούν τη λειτουργία των υπηρεσιών που απαιτούνται για τους σκοπούς της παροχής αποδεικτικών στοιχείων για την ορθή λειτουργία των υπηρεσιών και για τους σκοπούς των νομικών διαδικασιών, καθίστανται διαθέσιμα στις δικαστικές αρχές και/ή στα άτομα που έχουν το νόμιμο δικαίωμα πρόσβασης.

5.4.8 Αξιολογήσεις ευπάθειας

Τα συμβάντα καταγράφονται, εν μέρει, στη διαδικασία ελέγχου για την παρακολούθηση των ευπαθειών του συστήματος. Οι εκτιμήσεις ευπάθειας εκτελούνται και αναθεωρούνται ετησίως για τον εντοπισμό και την εκτίμηση ευλόγως προβλέψιμων εσωτερικών και εξωτερικών απειλών που θα μπορούσαν να οδηγήσουν σε μη εξουσιοδοτημένη πρόσβαση, αποκάλυψη, κατάχρηση, τροποποίηση ή καταστροφή οποιωνδήποτε δεδομένων των πιστοποιητικών ή της διαδικασίας έκδοσης των πιστοποιητικών. Η JCC Payment Systems αξιολογεί επίσης τακτικά την επάρκεια των πολιτικών, διαδικασιών, πληροφοριακών συστημάτων, τεχνολογιών και άλλων διαδικασιών που έχει τεθεί για τον έλεγχο τέτοιων κινδύνων. Η αξιολόγηση ευπάθειας και η εκτίμηση κινδύνου αποτελούν μέρος του ετήσιου ελέγχου συμμόρφωσης της JCC Payment Systems. Οι Μηνιαίες Αξιολογήσεις Ευπάθειας θα αποτελούν στοιχείο εισόδου στον ετήσιο έλεγχο της JCC Payment Systems.

5.5 *Τήρηση αρχείων*

5.5.1 Είδη τηρούμενων αρχείων

Η JCC Payment Systems τηρεί αρχεία για:

- όλα τα δεδομένα ελέγχου που συλλέγονται σύμφωνα με την ενότητα 5.4,
- τις πληροφορίες σχετικά με τις αιτήσεις για πιστοποιητικά,
- την υποστηρικτική τεκμηρίωση για τις αιτήσεις πιστοποιητικών,
- τις πληροφορίες σχετικά με τον κύκλο ζωής των πιστοποιητικών,

5.5.2 Περίοδος διατήρησης αρχείων

Η περίοδος διατήρησης των αρχείων περιγράφεται στην ενότητα 5.4.3.

5.5.3 Προστασία του Αρχείου

Η JCC Payment Systems προστατεύει τα αρχεία έτσι ώστε μόνο τα εξουσιοδοτημένα Έμπιστα Πρόσωπα έχουν τη δυνατότητα απόκτησης πρόσβασης στο Αρχείο. Το Αρχείο προστατεύεται έναντι της μη εξουσιοδοτημένης προβολής, τροποποίησης, διαγραφής ή άλλης παραποίησης μέσω της αποθήκευσης σε ένα αξιόπιστο σύστημα. Τα μέσα που φυλάσσουν τα δεδομένα του Αρχείου και των εφαρμογών που απαιτούνται για την επεξεργασία των δεδομένων του Αρχείου διατηρούνται προκειμένου να διασφαλιστεί η δυνατότητα προσπέλασής τους, για το χρονικό διάστημα που προσδιορίζεται στην παρούσα ΠΠ.

5.5.4 Διαδικασίες εφεδρικών αντιγράφων του Αρχείου

Σε καθημερινή βάση, δημιουργούνται επαυξητικοί (incremental backups) ή άλλοι τύποι αντιγράφων ασφαλείας για τα ηλεκτρονικά αρχεία και, σε εβδομαδιαία βάση, δημιουργούνται πλήρη αντίγραφα ασφαλείας.

5.5.5 Απαιτήσεις για τη χρονοσήμανση των αρχείων

Τα Πιστοποιητικά, οι ΚΑΠ καθώς και οι άλλες καταχωρίσεις ανάκλησης στη βάση δεδομένων περιλαμβάνουν πληροφορίες σχετικά με την ώρα και την ημερομηνία. Τα εν λόγω στοιχεία χρονοσήμανσης δεν είναι κρυπτογραφημένα.

5.5.6 Σύστημα συλλογής αρχείων (Εσωτερικό ή Εξωτερικό)

Η ADACOM λειτουργεί ένα εσωτερικό σύστημα συλλογής αρχείων για τις λειτουργείες της ΑΠ και η JCC Payment Systems για τις υπόλοιπες λειτουργίες που σχετίζονται με την ΠΥΕ.

5.5.7 Διαδικασίες για την πρόσβαση και την επαλήθευση πληροφοριών αρχείου

Μόνο το εξουσιοδοτημένο Έμπιστο Προσωπικό έχει τη δυνατότητα απόκτησης πρόσβασης στο Αρχείο. Η ακεραιότητα των πληροφοριών εξακριβώνεται όταν αποκαθίσταται.

Εάν τα αρχεία αφορούν τη λειτουργία των υπηρεσιών που απαιτούνται για τους σκοπούς της παροχής αποδεικτικών στοιχείων για την ορθή λειτουργία των υπηρεσιών και για τους σκοπούς των νομικών διαδικασιών, καθίστανται διαθέσιμα στις δικαστικές αρχές και/ή στα άτομα που έχουν νόμιμο δικαίωμα πρόσβασης.

5.6 *Αντικατάσταση κλειδιών*

Τα ζεύγη κλειδιών ΑΠ της JCC Payment Systems αποσύρονται με το πέρας του αντίστοιχου ανώτατου χρόνου ζωής τους όπως ορίζεται στην παρούσα ΔΠΠ. Τα Πιστοποιητικά ΑΠ της JCC Payment Systems δύνανται να ανανεωθούν εφόσον ο αθροιστικός πιστοποιημένος χρόνος ζωής του ζεύγους κλειδιών μιας ΑΠ δεν υπερβαίνει τον ανώτατο χρόνο ζωής αυτού του ζεύγους κλειδιών. Νέα ζεύγη κλειδιών της ΑΠ παράγονται ανάλογα με τις ανάγκες, για παράδειγμα για την αντικατάσταση ζεύγους κλειδιών ΑΠ τα οποία αποσύρονται, ώστε να συμπληρωθούν τα υφιστάμενα, ενεργά ζεύγη κλειδιών και να υποστηριχτούν νέες υπηρεσίες.

Πριν από τη λήξη του Πιστοποιητικού της ΑΠ για μια ιεραρχικά Ανώτερη ΑΠ, εφαρμόζονται διαδικασίες αντικατάστασης των κλειδιών ώστε να διευκολυνθεί η ομαλή μετάβαση όσον αφορά οντότητες εντός της ιεραρχίας της Ανώτερης ΑΠ, από το παλαιό ζεύγος κλειδιών στο(-α) νέο(-α) ζεύγος(-η) κλειδιών. Η διαδικασία αντικατάστασης κλειδιών της ΑΠ της JCC Payment Systems προϋποθέτει ότι:

- Η ιεραρχικά Ανώτερη ΑΠ διακόπτει την έκδοση νέων Πιστοποιητικών των ιεραρχικά Υφιστάμενων ΑΠ το αργότερο έως τις 60 ημέρες πριν από το χρονικό σημείο (εφεξής «Ημερομηνία Διακοπής Έκδοσης») όπου ο εναπομένων χρόνος ζωής του ζεύγους κλειδιών της ιεραρχικά Ανώτερης ΑΠ είναι ίσος με την Περίοδο Ισχύος του εγκριθέντος Πιστοποιητικού για τη(τις) συγκεκριμένη(-ες) μορφή(-ές) Πιστοποιητικών που εκδίδονται από τις Υφιστάμενες ΑΠ στην ιεραρχία της Ανώτερης ΑΠ.
- Τα Πιστοποιητικά, κατά την αποδοχή Αιτήματος για Πιστοποιητικό Υφιστάμενης ΑΠ (ή Συνδρομητή τελικού χρήστη) που λαμβάνεται μετά την «Ημερομηνία Διακοπής Έκδοσης», θα υπογράφονται με το νέο ζεύγος κλειδιών της ΑΠ.

Η ιεραρχικά Ανώτερη ΑΠ συνεχίζει να εκδίδει ΚΑΠ υπογεγραμμένες με το αρχικό ιδιωτικό κλειδί της Ανώτερης ΑΠ έως την επέλευση της ημερομηνίας λήξεως του τελευταίου Πιστοποιητικού που εκδόθηκε με τη χρήση αυτού του αρχικού ζεύγους κλειδιών.

5.7 *Έκθεση σε κίνδυνο και αποκατάσταση καταστροφής*

5.7.1 Διαδικασίες χειρισμού περιστατικών και έκθεσης σε κίνδυνο

Αντίγραφα ασφαλείας των πληροφοριών της ΑΠ φυλάσσονται σε αποθήκη εκτός του κύριου χώρου εγκαταστάσεων και καθίστανται διαθέσιμα σε περίπτωση Έκθεσης σε κίνδυνο ή καταστροφής: Δεδομένα των Αιτήσεων για Πιστοποιητικό, δεδομένα ελέγχων και αρχεία της βάσης δεδομένων για όλα τα εκδοθέντα Πιστοποιητικά. Αντίγραφα ασφαλείας των ιδιωτικών κλειδιών της ΑΠ δημιουργούνται και διατηρούνται σύμφωνα με την ενότητα 6.2.4 της παρούσας ΠΠ.

5.7.2 Φθορά υπολογιστικών πόρων, λογισμικού και/ή δεδομένων

Σε περίπτωση φθοράς των υπολογιστικών πόρων, του λογισμικού και/ή των δεδομένων, τα σχετικά περιστατικά αναφέρονται στο τμήμα Ασφάλειας της JCC Payment Systems και εφαρμόζονται οι διαδικασίες διαχείρισης περιστατικών ασφάλειας της JCC Payment Systems . Οι διαδικασίες αυτές απαιτούν την κατάλληλη κλιμάκωση, διερεύνηση και απόκριση στο περιστατικό. Εφόσον κριθεί απαραίτητο, θα τεθούν σε εφαρμογή οι διαδικασίες της JCC Payment Systems για την έκθεση του κλειδιού σε κίνδυνο ή την αποκατάσταση καταστροφής.

5.7.3 Διαδικασίες σχετικά με την έκθεση ιδιωτικού κλειδιού οντότητας σε κίνδυνο

Κατά την υποπτευόμενη ή πραγματική Έκθεση σε Κίνδυνο του ιδιωτικού κλειδιού ΑΠ της JCC Payment Systems , υπηρεσιών υποδομής ή Πελάτη ΑΠ, η JCC Payment Systems ακολουθεί το σχέδιο ενεργειών που περιγράφονται στη διαδικασία Διαχείρισης Περιστατικών Ασφαλείας.

Εφόσον απαιτείται ανάκληση του Πιστοποιητικού της ΑΠ, εκτελούνται από την ADACOM οι ακόλουθες διαδικασίες:

- η κατάσταση ανάκλησης του Πιστοποιητικού κοινοποιείται στα Βασιζόμενα Μέρη μέσω του Χώρου Αποθήκευσης της JCC Payment Systemsσύμφωνα με την ενότητα 4.9.9·
- θα καταβληθεί κάθε εύλογη από εμπορικής άποψης προσπάθεια προκειμένου να παρασχεθεί πρόσθετη ενημέρωση σχετικά με την ανάκληση προς όλους τους επηρεαζόμενους Συμμετέχοντες και
- η ΑΠ θα παραγάγει ένα νέο ζεύγος κλειδιών σύμφωνα με την ενότητα 5.6, εκτός της περίπτωσης που η λειτουργία της ΑΠ τερματίζεται σύμφωνα με την ενότητα 5.8.

Η παράγραφος αυτή ισχύει επίσης σε περίπτωση που αλγόριθμοι ΥΔΚ γίνουν ανεπαρκείς για την υπολειπόμενη αποσκοπούμενη χρήση.

5.7.4 Δυνατότητες επιχειρησιακής συνέχειας έπειτα από καταστροφή

Η JCC Payment Systems διατηρεί ένα Σχέδιο Επιχειρησιακής Συνέχειας (ΣΕΣ) προκειμένου να καθορίσει τις διαδικασίες αποκατάστασης των κρίσιμων επιχειρηματικών λειτουργιών της έπειτα από μια καταστροφή.

Οι ακόλουθοι στόχοι έχουν οριστεί για το συγκεκριμένο σχέδιο:

- Μεγιστοποίηση της αποτελεσματικότητας των λειτουργιών εκτάκτου ανάγκης μέσω ενός καταρτισμένου σχεδίου το οποίο απαρτίζεται από τις ακόλουθες φάσεις:
    - Η φάση ειδοποίησης/ενεργοποίησης η οποία εντοπίζει και αξιολογεί τη ζημιά και ενεργοποιεί το σχέδιο.
    - Η φάση αποκατάστασης η οποία αποκαθιστά τις προσωρινές λειτουργίες των πληροφοριακών συστημάτων και αποκαθιστά τη ζημιά που έχει υποστεί το αρχικό σύστημα.
- Προσδιορισμός των δραστηριοτήτων, των πόρων και των διαδικασιών που είναι απαραίτητες για τη διενέργεια των λειτουργιών των Πιστοποιητικών και της ΑΠ της JCC Payment Systems κατά τη διάρκεια παρατεταμένων διακοπών των συνήθων λειτουργιών.
- Ανάθεση αρμοδιοτήτων στο εξουσιοδοτημένο προσωπικό της JCC Payment Systems και καθοδήγηση όσον αφορά τις διαδικασίες αποκατάστασης της JCC Payment Systems κατά τη διάρκεια παρατεταμένων περιόδων διακοπών των συνήθων λειτουργιών.
- Εξασφάλιση του συντονισμού με άλλο προσωπικό της JCC Payment Systems το οποίο θα συμμετάσχει στις στρατηγικές σχεδιασμού έκτακτης ανάγκης. Εξασφάλιση του συντονισμού με εξωτερικά σημεία επικοινωνίας και προμηθευτές που θα συμμετάσχουν στις στρατηγικές σχεδιασμού έκτακτης ανάγκης.

Η JCC Payment Systems έχει τη δυνατότητα επαναφοράς ή αποκατάστασης των βασικών λειτουργιών της εντός είκοσι τεσσάρων (24) ωρών μετά την επέλευση της καταστροφής παρέχοντας τουλάχιστον υποστήριξη για τις ακόλουθες υπηρεσίες:

- ανάκληση πιστοποιητικών,
- δημοσίευση πληροφοριών ανάκλησης.

Η JCC Payment Systems διατηρεί πρόσθετο υλικό και εφεδρικά αντίγραφα της ΑΠ και του λογισμικού συστημάτων υποδομής στην Εγκατάσταση Αποκατάστασης έπειτα από καταστροφή. Επιπλέον, δημιουργούνται αντίγραφα ασφαλείας για τα ιδιωτικά κλειδιά της ΑΠ και φυλάσσονται για τους σκοπούς της αποκατάστασης έπειτα από καταστροφή σύμφωνα με την ενότητα 6.2.4.

5.8 *Διακοπή λειτουργίας ΑΠ ή ΑΕ*

Διακόπτεται η λειτουργία της ΑΠ με τα ακόλουθα:

- απόφαση του Διοικητικού Συμβουλίου της JCC Payment Systems ,
- απόφαση της αρχής η οποία εποπτεύει την παροχή της υπηρεσίας,
- δικαστική απόφαση,
- εκκαθάριση ή διακοπή των λειτουργιών της JCC Payment Systems .

Η JCC Payment Systems διασφαλίζει ότι ελαχιστοποιούνται οι πιθανές διαταραχές στους Συνδρομητές και τα Βασιζόμενα Μέρη λόγω της διακοπής των υπηρεσιών της JCC Payment Systems και, συγκεκριμένα, διασφαλίζει τη συνεχή διατήρηση των πληροφοριών που απαιτούνται για την επαλήθευση της ορθότητας των Υπηρεσιών Εμπιστοσύνης.

Στην περίπτωση που είναι απαραίτητη η διακοπή λειτουργίας μιας ΑΠ της JCC Payment Systems , η JCC Payment Systems καταβάλλει εύλογες από εμπορικής άποψης προσπάθειες ώστε να ειδοποιήσει τους Συνδρομητές, τα Βασιζόμενα Μέρη και άλλες οντότητες που επηρεάζονται από τη σχετική διακοπή πριν από τη διακοπή λειτουργίας της ΑΠ. Στην περίπτωση που η διακοπή λειτουργίας μίας ΑΠ κριθεί απαραίτητη, η JCC Payment Systems θα θέσει σε εφαρμογή το τεκμηριωμένο «Σχέδιο Διακοπής Εργασιών της JCC Payment Systems », ώστε να ελαχιστοποιήσει την αναστάτωση των Πελατών, των Συνδρομητών και των Βασιζόμενων Μερών. Το σχέδιο αυτό, προβλέπει, ανάλογα με την περίπτωση, τα ακόλουθα:

- την ειδοποίηση των μερών που επηρεάζονται από τη διακοπή λειτουργίας, όπως είναι οι Συνδρομητές, τα Βασιζόμενα Μέρη και οι Πελάτες, ενημερώνοντάς τους για την κατάσταση της ΑΠ,
- την αντιμετώπιση του κόστους της σχετικής ειδοποίησης,
- την ανάκληση του Πιστοποιητικού που εκδόθηκε στην ΑΠ από την JCC Payment Systems
- τη διατήρηση των αρχείων και των εγγράφων της ΑΠ για τα χρονικά διαστήματα που απαιτούνται από την παρούσα ΠΠ και την αντίστοιχη ΔΠΠ,
- τη συνεχή παροχή των υπηρεσιών υποστήριξης Συνδρομητή και του Πελατών,
- τη συνεχή παροχή των υπηρεσιών ανάκλησης, όπως είναι η έκδοση των ΚΑΠ ή η υποστήριξη υπηρεσιών δικτυακού ελέγχου κατάστασης Πιστοποιητικών,
- την ανάκληση των Πιστοποιητικών Συνδρομητών τελικών χρηστών και των υφιστάμενων ΑΠ τα οποία δεν έχουν λήξει ή ανακληθεί, εφόσον είναι απαραίτητο,
- την επιστροφή χρημάτων (εφόσον κριθεί απαραίτητη) προς τους Συνδρομητές των οποίων τα Πιστοποιητικά δεν έχουν λήξει ή ανακληθεί, αλλά ανακλήθηκαν στα πλαίσια της διακοπής λειτουργίας ή εναλλακτικά την αντικατάσταση των Πιστοποιητικών εκδίδοντας νέα από διάδοχη ΑΠ,
- τη διάθεση του ιδιωτικού κλειδιού της ΑΠ, συμπεριλαμβανομένου του εφεδρικού κλειδιού και των διακριτικών υλικού που περιλαμβάνουν το εν λόγω ιδιωτικό κλειδί,
- τις απαραίτητες ρυθμίσεις για τη μετάβαση των υπηρεσιών της ΑΠ προς τη διάδοχη ΑΠ, όπου είναι δυνατό,
- την ειδοποίηση των αρμόδιων αρχών, όπως οι εποπτικοί φορείς,
- τη μεταφορά των υποχρεώσεων σε αξιόπιστο μέρος όσον αφορά τη διατήρηση όλων των πληροφοριών που είναι απαραίτητες για την απόδειξη της λειτουργίας των Υπηρεσιών Εμπιστοσύνης για ένα εύλογο χρονικό διάστημα, εκτός και εάν μπορεί να καταδειχθεί ότι η JCC Payment Systems δεν έχει στην κατοχή της τις σχετικές πληροφορίες,
- την υποβολή του αρχείου και των εγγράφων της ΑΠ της JCC Payment Systems σε άλλον συμβατικό Πάροχο Υπηρεσιών Πιστοποίησης όσον αφορά τα Πιστοποιητικά για τα χρονικά διαστήματα που απαιτούνται βάσει νομοθεσίας.

Κατά την τερματισμό των δραστηριοτήτων της ΑΠ ή της παύσης των υπηρεσιών της ΑΕ, για οποιονδήποτε λόγο, οποιεσδήποτε συμβάσεις που αναθέτουν μέρος των ευθυνών του Παρόχου Υπηρεσιών Εμπιστοσύνης σε τρίτα μέρη θα λήξουν αυτομάτως. Για το σκοπό αυτό, τα τρίτα μέρη θα πρέπει να εξασφαλίσουν τη μεταφορά των αρχείων και εγγράφων που σχετίζονται με τις ανατεθείσες ευθύνες, σύμφωνα με την ισχύουσα νομοθεσία.

6 ΤΕΧΝΙΚΟΙ ΕΛΕΓΧΟΙ ΑΣΦΑΛΕΙΑΣ

6.1 *Παραγωγή και εγκατάσταση ζεύγους κλειδιών*

6.1.1 Παραγωγή ζεύγους κλειδιών

Η παραγωγή κλειδιών για τις ΑΠ της JCC Payment Systems, η αποθήκευση τους και η επακόλουθη χρήση τους διενεργείται από την ADACOM SA, Οι κρυπτογραφικές μονάδες που χρησιμοποιούνται για την παραγωγή κλειδιών πληρούν τις προδιαγραφές του επιπέδου 3 του FIPS 140-2. Η παραγωγή ζεύγους κλειδιών της ΑΠ διενεργείται από πολλαπλά, προεπιλεγμένα, εκπαιδευμένα και έμπιστα πρόσωπα, χρησιμοποιώντας αξιόπιστα συστήματα και διαδικασίες οι οποίες εγγυώνται την ασφάλεια και την απαραίτητη κρυπτογραφική ισχύ για τα παραγόμενα κλειδιά.

Όλα τα ζεύγη κλειδιών της ΑΠ παράγονται σε προκαθορισμένες Διαδικασίες Παραγωγής Κλειδιών (Key Ceremonies) σύμφωνα με τις απαιτήσεις των εγγράφων του «Οδηγού Αναφοράς Διαδικασίας Παραγωγής Κλειδιών» (Key Ceremony Reference Guide) και του «Οδηγού Χρήσης του Εργαλείου Διαχείρισης Κλειδιών της ΑΠ» (CA Key Management Tool User's Guide). Οι ενέργειες που πραγματοποιούνται σε κάθε διαδικασία παραγωγής κλειδιών καταγράφονται, αρχειοθετούνται και υπογράφονται από όλα τα εμπλεκόμενα πρόσωπα. Τα αρχεία αυτά τηρούνται για τους σκοπούς του ελέγχου και της ανίχνευσης για το χρονικό διάστημα που έχει κριθεί ως απαραίτητο από την ADACOM S.A. και την JCC Payment Systems.

Η παραγωγή ζεύγους κλειδιών Συνδρομητή τελικού χρήστη διενεργείται εν γένει από τον Συνδρομητή. Ο Συνδρομητής χρησιμοποιεί μια πιστοποιημένη κρυπτογραφική μονάδα ΕΔΔΥ η οποία συμμορφώνεται με τις απαιτήσεις του κανονισμού eIDAS.

Η παραγωγή, αποθήκευση και περαιτέρω χρήση των κλειδιών των εξ αποστάσεως Εγκεκριμένων Ψηφιακών Πιστοποιητικών γίνεται από την JCC Payment Systems χρησιμοποιώντας αποκλειστικά συσκευές πιστοποιημένες σύμφωνα με τις απαιτήσεις του άρθρου 30.3 του Κανονισμού eIDAS. οι οποίες εμπεριέχονται στη λίστα εγκεκριμένων συσκευών που τηρεί η Ευρωπαϊκή Επιτροπή σε συμμόρφωση με τα άρθρα 30, 31 και 39 του Κανονισμού eIDAS.

6.1.2 Παράδοση ιδιωτικού κλειδιού στον συνδρομητή

Όταν τα ζεύγη κλειδιών Συνδρομητή παράγονται σε ΕΔΔΥ από τον Συνδρομητή, δεν ισχύει η παράδοση ιδιωτικού κλειδιού στον Συνδρομητή.

6.1.3 Παράδοση δημόσιου κλειδιού στον εκδότη του πιστοποιητικού

Οι Συνδρομητές υποβάλλουν ηλεκτρονικά το δημόσιο κλειδί τους στην JCC Payment Systems για πιστοποίηση με τη χρήση του Αιτήματος Υπογραφής Πιστοποιητικού (ΑΥΠ), κατά το πρότυπο PKCS # 10 ή άλλη ηλεκτρονικά υπογεγραμμένη μορφή, σε ασφαλή σύνδεση μέσω TLS (Transport Layer Security -Επιπέδου Ασφαλών Μεταφορών).

6.1.4 Παράδοση δημόσιου κλειδιού της ΑΠ σε βασιζόμενα μέρη

Η JCC Payment Systems καθιστά διαθέσιμα τα Πιστοποιητικά ΑΠ Βάσης και Εκδότριας ΑΠ στους Συνδρομητές και τα Βασιζόμενα Μέρη μέσω του χώρου αποθήκευσης της.

Σε γενικές γραμμές, η JCC Payment Systems παρέχει την πλήρη αλυσίδα πιστοποιητικών της (συμπεριλαμβανομένων των εκδοτριών ΑΠ και οποιασδήποτε ΑΠ στην αλυσίδα) στον Συνδρομητή με την έκδοση του Πιστοποιητικού.

Οι Συνδρομητές, κατά τη διαδικασία λήψης του πιστοποιητικού, πραγματοποιούν αυτόματα τη λήψη και εγκαθιστούν στον υπολογιστή τους, τα δημόσια κλειδιά των ενδιάμεσων και εκδοτριών ΑΠ. Σε κάθε περίπτωση, εφόσον ένας χρήστης επιθυμεί να επαληθεύσει και/ή να πραγματοποιήσει τη λήψη του δημόσιου κλειδιού της ΑΠ, αυτό μπορεί να το κάνει μέσωτου διαδικτυακού χώρου αποθήκευσης της JCC Payment Systems (https://pki.jcc.com.cy/repository).

6.1.5 Μέγεθος κλειδιού

Τα ζεύγη κλειδιών θα πρέπει να διαθέτουν ικανοποιητικό μέγεθος ώστε να αποτρέπουν τρίτους να καθορίσουν το ιδιωτικό κλειδί του ζεύγους κλειδιών χρησιμοποιώντας την κρυπτανάλυση κατά την αναμενόμενη διάρκεια χρήσης των κλειδιών αυτών. Το πρότυπο της JCC Payment Systems όσον αφορά το ελάχιστο μέγεθος κλειδιών είναι η χρήση ενός ζεύγους κλειδιών ισχύος τουλάχιστον με 4096 bit για τα πιστοποιητικά των ΑΠ και 2048 bit RSA για τα πιστοποιητικά του Συνδρομητή.

Στο παρόν στάδιο, η JCC Payment Systems δημιουργεί και χρησιμοποιεί τουλάχιστον τα εξής ελάχιστα μεγέθη κλειδιών, αλγόριθμους υπογραφής και αλγόριθμους κατακερματισμού για την υπογραφή Πιστοποιητικών, ΚΑΠ και αποκρίσεων διακομιστών κατάστασης πιστοποιητικών:

- Κλειδιά RSA με μέγεθος μονάδας σε bits που διαιρείται με το 8 και είναι τουλάχιστον 2048.
- Αλγόριθμοι κατακερματισμού: SHA-256, SHA-384 ή SHA-512.

6.1.6 Δημιουργία παραμέτρων και έλεγχος ποιότητας δημόσιων κλειδιών

Η ποιότητα των δημόσιων κλειδιών διασφαλίζεται με τη χρήση ασφαλούς δημιουργίας τυχαίων αριθμών και την on-board δημιουργία δημοσίων κλειδιών. Τα ζεύγη κλειδιών δημιουργούνται χρησιμοποιώντας ασφαλείς αλγόριθμους και παραμέτρους που βασίζονται σε τρέχοντα ερευνητικά και βιομηχανικά πρότυπα σύμφωνα με τις συστάσεις του προτύπου ETSI TS 119 312.

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

Ανατρέξτε στην ενότητα 7.

6.2 *Προστασία ιδιωτικού κλειδιού και μηχανικοί έλεγχοι κρυπτογραφικής μονάδας*

Η JCC Payment Systems εφαρμόζει συνδυασμό φυσικών, λογικών, και διαδικαστικών μέτρων τα οποία εγγυώνται την ασφάλεια των ιδιωτικών κλειδιών των ΑΠ της. Επίσης, οι Συνδρομητές πρέπει να λαμβάνουν τα μέτρα προφύλαξης ώστε να αποτρέψουν την απώλεια, την αποκάλυψη, την τροποποίηση, ή τη μη εξουσιοδοτημένη χρήση ιδιωτικών κλειδιών.

6.2.1 Πρότυπα και έλεγχοι για τις κρυπτογραφικές μονάδες

Για την παραγωγή ζεύγους κλειδιών της ΑΠ και την αποθήκευση ιδιωτικών κλειδιών της ΑΠ, η JCC Payment Systems χρησιμοποιεί κρυπτογραφικές μονάδες υλικού οι οποίες είναι πιστοποιημένες ή πληρούν τις προδιαγραφές του επιπέδου 3 του FIPS 140-2.

Τα ιδιωτικά κλειδιά του Συνδρομητή παράγονται σε ΕΔΔΥ που συμμορφώνεται με τις απαιτήσεις του κανονισμού eIDAS.

Η JCC Payment Systems επιβλέπει την κατάσταση του πιστοποιητικού ΕΔΔΥ τουλάχιστον ετησίως, μέχρι τη λήξη ισχύος του πιστοποιητικού που συνδέεται με την αντίστοιχη ΕΔΔΥ. Σε περίπτωση τροποποίησης της κατάστασης του πιστοποιητικού της ΕΔΔΥ, η JCC Payment Systems θα παύσει να εκδίδει πιστοποιητικά σε αυτές τις συσκευές.

6.2.2 Έλεγχος του ιδιωτικού κλειδιού από πολλαπλά πρόσωπα (m από n)

Η JCC Payment Systems εφαρμόζει τεχνικούς και διαδικαστικούς μηχανισμούς της ADACOM, οι οποίοι απαιτούν τη συμμετοχή πολλαπλών έμπιστων προσώπων για την εκτέλεση ευαίσθητων κρυπτογραφικών εφαρμογών της ΑΠ. Οι μηχανισμοί αυτοί εφαρμόζουν την πολιτική «Διαμοιρασμού Απορρήτου», διαχωρίζοντας τα δεδομένα ενεργοποίησης που είναι απαραίτητα για τη χρήση ενός ιδιωτικού κλειδιού ΑΠ σε διακριτά μέρη τα οποία καλούνται «Μερίδια Απορρήτου» και τα οποία βρίσκονται στην κατοχή εκπαιδευμένων και έμπιστων προσώπων που ονομάζονται «Κάτοχοι Μεριδίων». Απαιτείται ένας κατώτατος οριακός αριθμός Μεριδίων Απορρήτου (m) εκ του συνολικού αριθμού των Μεριδίων Απορρήτου που δημιουργήθηκαν και διανεμήθηκαν για μια συγκεκριμένη κρυπτογραφική μονάδα υλικού (n) ώστε να ενεργοποιηθεί το ιδιωτικό κλειδί της ΑΠ που είναι αποθηκευμένο στη μονάδα.

Ο κατώτατος αριθμός των Μεριδίων που απαιτούνται για να υπογραφεί ένα Πιστοποιητικό ΑΠ είναι 3. Θα πρέπει να σημειωθεί ότι ο αριθμός των μεριδίων που διανέμονται για τα διακριτικά αποκατάστασης καταστροφής μπορεί να είναι μικρότερος από τον αριθμό μεριδίων που διανεμήθηκαν για τα λειτουργικά διακριτικά (tokens), ενώ ο κατώτατος αριθμός των απαιτούμενων μεριδίων παραμένει ο ίδιος. Τα Μερίδια Απορρήτου προστατεύονται σύμφωνα με την παρούσα ΠΠ.

Κανένας έλεγχος πολλαπλών προσώπων δεν εφαρμόζεται στα ιδιωτικά κλειδιά του Συνδρομητή.

6.2.3 Παρακαταθήκη ιδιωτικού κλειδιού

Τα ιδιωτικά κλειδιά της ΑΠ της JCC Payment Systems και των Συνδρομητών δεν δίνονται για φύλαξη.

6.2.4 Δημιουργία αντίγραφου ασφαλείας ιδιωτικού κλειδιού

Η ADACOM SA δημιουργεί αντίγραφα ασφαλείας για τα ιδιωτικά κλειδιά της ΑΠ και η JCC Payment Sytems δημιουργεί αντίγραφα ασφαλείας για τα ιδιωτικά κλειδιά των Συνδρομητών που δημιουργούνται και αποθηκεύονται από μία εξ αποστάσεως ΕΔΔΥ, για τους σκοπούς της τακτικής ανάκτησης και της αποκατάστασης από καταστροφή. Τα κλειδιά αυτά αποθηκεύονται σε κρυπτογραφημένη μορφή σε κρυπτογραφικές μονάδες υλικού και σε συσκευές που συνδέονται με την αποθήκευση κλειδιών. Οι κρυπτογραφικές μονάδες που χρησιμοποιούνται για την αποθήκευση των ιδιωτικών κλειδιών συμμορφώνονται με τις απαιτήσεις της παρούσας ΠΠ.

Οι μονάδες που περιέχουν τα αντίγραφα ασφαλείας των ιδιωτικών κλειδιών ΑΠ εντός του κύριου χώρου εγκαταστάσεων υπόκεινται στις προδιαγραφές της παρούσας ΔΠΠ. Οι μονάδες που περιέχουν τα αντίγραφα ασφαλείας των ιδιωτικών κλειδιών ΑΠ όσον αφορά την αποκατάσταση από καταστροφή υπόκεινται στις προδιαγραφές της παρούσας ΠΠ.

Σε περίπτωση τοπικής ΕΔΔΥ, τα Ιδιωτικά Κλειδιά του Συνδρομητή δεν μπορούν να εξαχθούν, να δημιουργηθούν αντίγραφα ασφαλείας ή να αποκατασταθούν από την ΕΔΔΥ.

6.2.5 Αρχειοθέτηση ιδιωτικών κλειδιών

Με το τέλος της περιόδου ισχύος ενός Πιστοποιητικού της ΑΠ της JCC Payment Systems , τα ζεύγη κλειδιών που συνδέονται με το πιστοποιητικό, διατηρούνται για χρονικό διάστημα τουλάχιστον 5 ετών με ασφαλή τρόπο χρησιμοποιώντας κρυπτογραφικές μονάδες υλικού οι οποίες πληρούν τις απαιτήσεις της παρούσας ΠΠ. Τα συγκεκριμένα ζεύγη κλειδιών της ΑΠ δεν χρησιμοποιούνται για την υπογραφή κανενός συμβάντος μετά την ημερομηνία λήξης του αντίστοιχου Πιστοποιητικού ΑΠ, εκτός και εάν το σχετικό Πιστοποιητικό ΑΠ έχει ανανεωθεί σύμφωνα με τους όρους της παρούσας ΠΠ.

Τα ιδιωτικά κλειδιά του Συνδρομητή δεν μπορούν να εξαχθούν ή να αποκατασταθούν από την ΕΔΔΥ και δεν αρχειοθετούνται.

6.2.6 Μεταφορά ιδιωτικού κλειδιού προς/από την κρυπτογραφική μονάδα

Η ADACOM SA δημιουργεί ζεύγη κλειδιών της ΑΠ για τις κρυπτογραφικές μονάδες υλικού στις οποίες θα χρησιμοποιηθούν τα κλειδιά. Επίσης, η ADACOM SA δημιουργεί αντίγραφα των σχετικών ζευγών κλειδιών για τους σκοπούς της τακτικής αποκατάστασης και αποκατάστασης από καταστροφή. Όταν για τα ζεύγη κλειδιών των ΑΠ δημιουργούνται αντίγραφα ασφάλειας σε άλλες κρυπτογραφικές μονάδες υλικού, η μεταφορά τους μεταξύ των μονάδων πραγματοποιείται σε κρυπτογραφημένη μορφή.

Η JCC Payment Systems δημιουργεί ζεύγη κλειδιών Συνδρομητή στις κρυπτογραφικές μονάδες υλικού στις οποίες θα χρησιμοποιηθούν τα κλειδιά. η JCC Payment Systems δημιουργεί αντίγραφα των σχετικών ζευγών κλειδιών για σκοπούς υψηλής διαθεσιμότητας και αποκατάστασης από καταστροφή. Όταν για τα ζεύγη κλειδιών του Συνδρομητή δημιουργούνται αντίγραφα ασφάλειας σε άλλες κρυπτογραφικές μονάδες υλικού, η μεταφορά τους μεταξύ των μονάδων πραγματοποιείται σε κρυπτογραφημένη μορφή.

6.2.7 Αποθήκευση ιδιωτικού κλειδιού σε κρυπτογραφική μονάδα

Τα ιδιωτικά κλειδιά που βρίσκονται σε κρυπτογραφικές μονάδες υλικού, τηρούνται σε κρυπτογραφημένη μορφή.

6.2.8 Μέθοδος ενεργοποίησης ιδιωτικού κλειδιού

Όλοι οι Συνδρομητές της JCC Payment Systems είναι απαραίτητο να προστατεύουν τα δεδομένα ενεργοποίησης των ιδιωτικών τους κλειδιών έναντι απώλειας, κλοπής, τροποποίησης, μη εξουσιοδοτημένης γνωστοποίησης ή χρήσης.

Η παραγωγή των δεδομένων ενεργοποίησης περιγράφεται στην ενότητα 6.4.1

Τα Ιδιωτικά Κλειδιά του Συνδρομητή στην Τοπική ΕΔΔΥ προστατεύονται από κωδικούς PIN. Οι κανόνες ορίζονται στην ενότητα 6.2.8 της σχετικής ΔΠΠ.

Τα ιδιωτικά κλειδιά των Συνδρομητών που δημιουργούνται και αποθηκεύονται σε εξ αποστάσεως ΕΔΔΥ, προστατεύονται από όνομα χρήστη, κωδικό πρόσβασης και εξουσιοδότηση μέσω κωδικού ή βιομετρικών. Οι κανόνες ορίζονται στην παράγραφο 6.2.8 της σχετικής ΔΠΠ.

Ένα ιδιωτικό κλειδί της ΑΠ ενεργοποιείται από έναν ορισμένο αριθμό Κατόχων Μεριδίων, όπως ορίζεται στην ενότητα 6.2.2, παρέχοντας τα δεδομένα ενεργοποίησης (τα οποία είναι αποθηκευμένα σε ασφαλή μέσα). Μόλις ενεργοποιηθεί το ιδιωτικό κλειδί, μπορεί να παραμείνει ενεργό για απεριόριστο χρονικό διάστημα έως ότου απενεργοποιηθεί όταν η ΑΠ βρεθεί εκτός σύνδεσης (offline). Παρομοίως, ένας ορισμένος αριθμός Κατόχων Μεριδίων πρέπει να παράσχει τα δεδομένα ενεργοποίησής τους προκειμένου να ενεργοποιηθεί το ιδιωτικό κλειδί της ΑΠ που βρίσκεται εκτός σύνδεσης (offline). Μόλις ενεργοποιηθεί το ιδιωτικό κλειδί, παραμένει ενεργό μόνο για μία μόνο σύνδεση.

6.2.9 Μέθοδος απενεργοποίησης ιδιωτικού κλειδιού

Τα ιδιωτικά κλειδιά της ΑΠ της JCC Payment Systems απενεργοποιούνται με τη διακοπή της τροφοδοσίας της κρυπτογραφικής μονάδας.

Τα ιδιωτικά κλειδιά Συνδρομητών μπορούν να απενεργοποιηθούν μετά από κάθε λειτουργία, αποσυνδέοντας το σύστημά τους ή αφαιρώντας την τοπική ΕΔΔΥ από τον σταθμό εργασίας, ή κατά την αποσύνδεση από την εξ αποστάσεως ΕΔΔΥ. Σε κάθε περίπτωση, οι Συνδρομητές έχουν υποχρέωση να προστατεύουν επαρκώς το(τα) ιδιωτικό(-ά) κλειδί(-ιά) τους σύμφωνα με την παρούσα ΠΠ και την ΔΠΠ.

6.2.10 Μέθοδος καταστροφής ιδιωτικού κλειδιού

Όταν απαιτείται, η JCC Payment Systems καταστρέφει τα ιδιωτικά κλειδιά της ΑΠ και των Συνδρομητών κατά τρόπο που εύλογα να διασφαλίζεται ότι δεν θα παραμείνουν μέρη του κλειδιού τα οποία θα μπορούσαν να οδηγήσουν στην ανασύνθεσή του. Η JCC Payment Systems χρησιμοποιεί τη λειτουργία διαγραφής ευαίσθητων παραμέτρων των κρυπτογραφικών μονάδων υλικού της καθώς και άλλα κατάλληλα μέσα ώστε να εξασφαλίσει την ολοκληρωτική καταστροφή των ιδιωτικών κλειδιών. Οι ενέργειες καταστροφής κλειδιών της ΑΠ καταγράφονται κατά την εκτέλεσή τους.

Τα Ιδιωτικά Κλειδιά του Συνδρομητή σε μια τοπική ΕΔΔΥ μπορούν να καταστραφούν με τη φυσική καταστροφή ή ζημιά της ΕΔΔΥ.

6.2.11 Αξιολόγηση κρυπτογραφικής μονάδας

Ανατρέξτε στην ενότητα 6.2.1.

6.3 *Άλλα θέματα διαχείρισης του ζεύγους κλειδιών*

6.3.1 Αρχειοθέτηση δημόσιου κλειδιού

Για τα Πιστοποιητικά των Συνδρομητών της JCC Payment Systems δημιουργούνται αντίγραφα ασφαλείας τα οποία αρχειοθετούνται ως μέρος της τακτικής διαδικασίας δημιουργίας αντιγράφων της JCC Payment Systems .

Όλα τα δημόσια κλειδιά των Συνδρομητών φυλάσσονται στη βάση δεδομένων της JCC Payment Systems και της ADACOM SA και μπορούν να αρχειοθετηθούν για τουλάχιστον επτά (7) ημέρες μετά τη λήξη της ΑΠ που έχει εκδώσει τα πιστοποιητικά.

6.3.2 Λειτουργικές περίοδοι πιστοποιητικών και περίοδος χρήσης ζεύγους κλειδιών

Η Λειτουργική Περίοδος ενός Πιστοποιητικού ολοκληρώνεται με τη λήξη ή την ανάκλησή του. Η Λειτουργική Περίοδος για ζεύγη κλειδιών είναι ίδια με τη Λειτουργική Περίοδο των συσχετιζόμενων Πιστοποιητικών, εκτός από το ότι τα ιδιωτικά κλειδιά μπορούν να συνεχίσουν να χρησιμοποιούνται για επαλήθευση υπογραφής. Οι μέγιστες Λειτουργικές Περίοδοι των Πιστοποιητικών της JCC Payment Systems για Πιστοποιητικά που εκδίδονται κατά ή μετά την ημερομηνία έναρξης ισχύος της παρούσας ΠΠ παρατίθενται στον ακόλουθο Πίνακα.

Πιστοποιητικό που εκδόθηκε από:	***Περίοδος ισχύος***
ΑΠ βάσης ΠΑΠ	Συνήθως έως και 30 έτη
Εκδότρια ΑΠ της JCC Payment Systems	Συνήθως έως και 8 έτη
Πιστοποιητικά Συνδρομητή	Συνήθως έως και 3 έτη

Επιπρόσθετα, οι ΑΠ της JCC Payment Systems παύουν να εκδίδουν νέα Πιστοποιητικά στην ανάλογη ημερομηνία (επιπλέον μέγιστη περίοδο ισχύος 60 ημερών των εκδοθέντων Πιστοποιητικών) πριν από τη λήξη του Πιστοποιητικού των ΑΠ, έτσι ώστε κανένα Πιστοποιητικό το οποίο εκδίδεται από ιεραρχικά Υφιστάμενη ΑΠ να μη λήγει μετά τη λήξη οποιουδήποτε Πιστοποιητικού της ιεραρχικά Ανώτερης ΑΠ. Η διάρκεια ζωής των πιστοποιητικών των Συνδρομητών δεν θα υπερβαίνει τη διάρκεια ζωής του πιστοποιητικού υπογραφής της ΑΠ.

Οι Συνδρομητές παύουν τη χρήση των ζευγών κλειδιών τους μετά τη λήξη των περιόδων χρήσης τους.

Εάν ένα αλγόριθμος ή το ανάλογο μήκος κλειδιού δεν προσφέρει επαρκή ασφάλεια κατά την περίοδο ισχύος του πιστοποιητικού, το εν λόγω πιστοποιητικό θα ανακαλείται και θα δρομολογείται μια νέα

αίτηση για πιστοποιητικό. Η εφαρμοσιμότητα των κρυπτογραφικών αλγορίθμων και παραμέτρων εποπτεύεται συνεχώς από τη Διεύθυνση της JCC Payment Systems.

6.4 *Δεδομένα ενεργοποίησης*

6.4.1 Παραγωγή και εγκατάσταση δεδομένων ενεργοποίησης

Τα δεδομένα ενεργοποίησης (Μερίδια Απορρήτου) που χρησιμοποιούνται για την προστασία των ΚΜΥ που περιέχουν τα ιδιωτικά κλειδιά των ΑΠ της JCC Payment Systems παράγονται σύμφωνα με τις απαιτήσεις της ενότητας 6.2.2 και του «Οδηγού Αναφοράς Διαδικασίας Παραγωγής Κλειδιών (Key Ceremony Reference Guide)». Η δημιουργία και η διανομή των σχετικών Μεριδίων Απορρήτου καταγράφεται.

Τα δεδομένα ενεργοποίησης που χρησιμοποιούνται (κωδικοί PIN) για την προστασία της Τοπικής ΕΔΔΥ που περιέχει τα ιδιωτικά κλειδιά του Υποκείμενου δημιουργούνται σύμφωνα με το εγχειρίδιο χρήστη της ΕΔΔΥ.

- Όταν τα ζεύγη κλειδιών δημιουργούνται από το Υποκείμενο, τα προ-καθορισμένα δεδομένα ενεργοποίησης πρέπει να αλλάξουν αμέσως πριν από τη δημιουργία των κλειδιών.

Τα δεδομένα ενεργοποίησης που χρησιμοποιούνται (όνομα χρήστη, κωδικός πρόσβασης, εξουσιοδότηση αιτήματος μέσω εφαρμογής στο κινητό με χρήση κωδικού ή βιομετρικών) για την προστασία των εξ αποστάσεως ΕΔΔΥ που περιέχουν τα ιδιωτικά κλειδιά του Υποκειμένου, παράγονται σύμφωνα με το εγχειρίδιο της ΕΔΔΥ.

Η JCC Payment Systems θα μεταδίδει δεδομένα ενεργοποίησης μόνο μέσω κατάλληλα προστατευμένου καναλιού και σε χρόνο και τόπο που διαφέρει από την παράδοση της σχετικής κρυπτογραφικής μονάδας.

6.4.2 Προστασία δεδομένων ενεργοποίησης

Οι Κάτοχοι Μεριδίων της JCC Payment Systems πρέπει να διαφυλάσσουν τα προσωπικά τους Μερίδια Απορρήτου και τα Μερίδια Απορρήτου της εξ αποστάσεως ΕΔΔΥ και να υπογράψουν σύμβαση αναγνωρίζοντας τις αρμοδιότητες του Κατόχου Μεριδίων.

Ο Συνδρομητής απομνημονεύει τους κωδικούς ενεργοποίησης, (PIN, όνομα χρήστη, κωδικός πρόσβασης και εξουσιοδότηση μέσω εφαρμογής στο κινητό χρησιμοποιώντας κωδικό ή βιομετρικά) και δεν τους κοινοποιεί σε κανέναν άλλον.

Η JCC Payment Systems εφαρμόζει την επαλήθευση ταυτότητας πολλαπλών παραγόντων (multi-factor authentication) για όλους τους λογαριασμούς που μπορούν να προκαλέσουν την έκδοση πιστοποιητικών ή λειτουργίες Αρχής Εγγραφής ή λειτουργίες εξουσιοδοτημένου τρίτου μέρους ή την εφαρμογή τεχνικών ελέγχων που εκτελούνται από την ΑΠ για περιορισμό της έκδοσης πιστοποιητικών μέσω του λογαριασμού σε περιορισμένο αριθμό προεγκεκριμένων τομέων ή διευθύνσεων ηλεκτρονικού ταχυδρομείου.

6.4.3 Άλλα θέματα για τα δεδομένα ενεργοποίησης

6.4.3.1 Μετάδοση δεδομένων ενεργοποίησης

Στην περίπτωση μετάδοσης των δεδομένων ενεργοποίησης των ιδιωτικών κλειδιών, οι Συμμετέχοντες προστατεύουν τη μετάδοση χρησιμοποιώντας μεθόδους που παρέχουν προστασία από απώλεια, κλοπή, τροποποίηση, μη εξουσιοδοτημένη γνωστοποίηση ή χρήση των εν λόγω ιδιωτικών κλειδιών.

6.4.3.2 Καταστροφή των δεδομένων ενεργοποίησης

Τα δεδομένα ενεργοποίησης των ιδιωτικών κλειδιών τίθενται εκτός λειτουργίας χρησιμοποιώντας μεθόδους που παρέχουν προστασία από απώλεια, κλοπή, τροποποίηση, μη εξουσιοδοτημένη γνωστοποίηση ή χρήση των ιδιωτικών κλειδιών που προστατεύονται από τα εν λόγω δεδομένα ενεργοποίησης. Μετά το πέρας των περιόδων διατήρησης των αρχείων σύμφωνα με την ενότητα 5.5.2, η JCC Payment Systems καταστρέφει τα δεδομένα ενεργοποίησης αντικαθιστώντας τα με καινούργια και/ή μέσω της φυσικής καταστροφής τους.

6.5 *Έλεγχοι ασφάλειας υπολογιστών*

Η JCC Payment Systems εκτελεί όλες τις λειτουργίες των ΑΠ και ΑΕ χρησιμοποιώντας αξιόπιστα συστήματα που πληρούν τις απαιτήσεις του Συστήματος Διαχείρισης Ασφάλειας Πληροφοριών (Information Security Management System - ISMS) της JCC Payment Systems και του ISMS της ADACOM.

6.5.1 Ειδικές τεχνικές απαιτήσεις για την ασφάλεια των υπολογιστών

Η JCC Payment Systems διασφαλίζει ότι τα συστήματα που διατηρούν τα αρχεία δεδομένων και το λογισμικό της ΑΠ είναι αξιόπιστα συστήματα τα οποία είναι ασφαλή από τη μη εξουσιοδοτημένη πρόσβαση. Επιπλέον, η JCC Payment Systems περιορίζει την πρόσβαση στους διακομιστές παραγωγής εξουσιοδοτώντας μόνο τα άτομα που έχουν βάσιμο επαγγελματικό λόγο. Οι χρήστες γενικών εφαρμογών δεν διαθέτουν λογαριασμούς στους διακομιστές παραγωγής.

Το δίκτυο παραγωγής της JCC Payment Systems διαχωρίζεται λογικά από τα άλλα στοιχεία. Ο διαχωρισμός αυτός επιτρέπει την πρόσβαση στο δίκτυο μόνο μέσω καθορισμένων διαδικασιών εφαρμογών. Η JCC Payment Systems χρησιμοποιεί τείχη προστασίας (firewalls) για την προστασία του δικτύου παραγωγής από εσωτερική και εξωτερική διείσδυση, καθώς και για τον περιορισμό της φύσης και της πηγής των δραστηριοτήτων, οι οποίες θα μπορούσαν να προσπελάσουν τα συστήματα παραγωγής.

Όλα τα κρίσιμα στοιχεία λογισμικού εγκαθίστανται και ενημερώνονται μόνο από αξιόπιστες πηγές. Υπάρχουν επίσης και εσωτερικές διαδικασίες για την προστασία της ακεραιότητας των στοιχείων υπηρεσιών πιστοποίησης από ιούς, κακόβουλο και μη εξουσιοδοτημένο λογισμικό.

Επαληθεύεται η ταυτότητα των μελών του προσωπικού της JCC Payment Systems πριν από τη χρήση κρίσιμων εφαρμογών που σχετίζονται με τις υπηρεσίες. Δημιουργούνται λογαριασμοί χρηστών για το προσωπικό σε συγκεκριμένους ρόλους που απαιτούν πρόσβαση στο σχετικό σύστημα. Οι άδειες του συστήματος αρχείων, καθώς και άλλες διαθέσιμες δυνατότητες στο μοντέλο ασφάλειας του λειτουργικού συστήματος χρησιμοποιούνται για να αποτραπεί οποιαδήποτε άλλη χρήση. Οι λογαριασμοί χρηστών αφαιρούνται το συντομότερο δυνατό όταν το επιβάλει η αλλαγή των ρόλων. Οι κανόνες που αφορούν την ασφάλεια ελέγχονται ετησίως.

Η JCC Payment Systems απαιτεί τη χρήση κωδικών πρόσβασης με ελάχιστο αριθμό χαρακτήρων και συνδυασμό αλφαριθμητικών και ειδικών χαρακτήρων. Η JCC Payment Systems απαιτεί οι κωδικοί πρόσβασης να αλλάζουν σε περιοδική βάση.

Η άμεση πρόσβαση σε βάσεις δεδομένων της JCC Payment Systems που υποστηρίζουν τις Λειτουργίες της ΑΠ, είναι περιορισμένη σε Έμπιστα Πρόσωπα που έχουν βάσιμο επαγγελματικό λόγο για την πρόσβαση αυτή.

Η διαχείριση των στοιχείων του συστήματος υπηρεσιών πιστοποίησης της JCC Payment Systems διενεργείται σύμφωνα με τις καθορισμένες διαδικασίες διαχείρισης αλλαγών. Οι εν λόγω διαδικασίες περιλαμβάνουν τη δοκιμή του συστήματος σε ένα απομονωμένο περιβάλλον δοκιμής και την απαίτηση ότι η αλλαγή πρέπει να εγκρίνεται από τον Υπεύθυνο Ασφάλειας. Η έγκριση τεκμηριώνεται για περαιτέρω αναφορά.

Όλα τα μέσα που περιέχουν τα δεδομένα και το λογισμικό του περιβάλλοντος παραγωγής, τις πληροφορίες για τον έλεγχο, το αρχείο ή τα αντίγραφα ασφαλείας αποθηκεύονται εντός της JCC Payment Systems με τους κατάλληλους ελέγχους λογικής και φυσικής πρόσβασης. Τα μέσα που περιέχουν Ευαίσθητες Πληροφορίες οι οποίες διαγράφονται με ασφάλεια όταν δεν είναι πλέον απαραίτητες.

Οι διαδικασίες διαχείρισης ευπάθειας και αντιμετώπισης συμβάντων τεκμηριώνονται σε εσωτερικό έγγραφο. Το σύστημα παρακολούθησης εντοπίζει και ειδοποιεί για μη αναμενόμενες δραστηριότητες του συστήματος που υποδεικνύουν πιθανή παραβίαση της ασφάλειας, συμπεριλαμβανομένης της εισβολής στο δίκτυο.

Τα έγγραφα και υλικά με Ευαίσθητες Πληροφορίες περνάνε σε καταστροφέα εγγράφων πριν από την απόρριψή τους. Τα μέσα που χρησιμοποιήθηκαν για τη συλλογή ή τη μεταβίβαση ευαίσθητων πληροφοριών καθίστανται μη αναγνώσιμα πριν από την απόρριψή τους.

Οι ΑΕ πρέπει να εξασφαλίζουν ότι τα συστήματα που διατηρούν λογισμικό και αρχεία δεδομένων είναι αξιόπιστα συστήματα, προστατεύονται από μη εξουσιοδοτημένη πρόσβαση και είναι λογικά διαχωρισμένα από άλλα στοιχεία. Οι ΑΕ πρέπει να χρησιμοποιούν τείχη προστασίας για να προστατεύσουν το δίκτυο από εσωτερικές και εξωτερικές εισβολές και να περιορίσουν τη φύση και την πηγή των δραστηριοτήτων που μπορούν να έχουν πρόσβαση στα εν λόγω συστήματα και πληροφορίες.

6.5.2 Αξιολόγηση ασφάλειας υπολογιστών

Καμία διατύπωση.

6.6 *Τεχνικοί έλεγχοι κατά τον κύκλο ζωής*

6.6.1 Έλεγχοι ανάπτυξης συστήματος

Νέες εκδόσεις λογισμικού αναπτύσσονται και εφαρμόζονται σύμφωνα με τη διαδικασία διαχείρισης αλλαγών.

Καινούριο ή ενημερωμένο λογισμικό το οποίο όταν φορτώνεται για πρώτη φορά παρέχει μια μέθοδο επαλήθευσης ότι το λογισμικό στο σύστημα προέρχεται από έμπιστη πηγή, δεν έχει τροποποιηθεί πριν από την εγκατάσταση και αποτελεί την έκδοση που προορίζεται για τη σχετική χρήση.

6.6.2 Έλεγχοι διαχείρισης ασφάλειας

Η JCC Payment Systems διαθέτει μηχανισμούς και/ή πολιτικές για τον έλεγχο και την παρακολούθηση της διαμόρφωσης των συστημάτων της ΑΠ.

Η JCC Payment Systems ακολουθεί τις κατευθυντήριες γραμμές για την ασφάλεια δικτύου της ενότητας 7.8 του ETSI EN 319 401. Μετά την εγκατάσταση και, έκτοτε, σε περιοδική βάση, η JCC Payment Systems επικυρώνει την ακεραιότητα των συστημάτων των ΑΠ της.
Μόνο το λογισμικό που χρησιμοποιείται απευθείας για την εκτέλεση των εργασιών, χρησιμοποιείται για το πληροφοριακό σύστημα.

6.6.3 Έλεγχοι ασφάλειας κατά τον κύκλο ζωής του πιστοποιητικού

Οι πολιτικές και τα περιουσιακά στοιχεία της JCC Payment Systems ελέγχονται σε προγραμματισμένα χρονικά διαστήματα ή όταν συντελούνται σημαντικές αλλαγές προκειμένου να διασφαλιστεί η συνέχιση της καταλληλότητας, επάρκειας και αποτελεσματικότητάς τους.

Οι διαμορφώσεις των συστημάτων της JCC Payment Systems ελέγχονται σε τακτικά διαστήματα για τυχόν αλλαγές που παραβιάζουν τις πολιτικές ασφάλειας της JCC Payment Systems . Ο Υπεύθυνος Ασφάλειας εγκρίνει τις αλλαγές που επηρεάζουν το επίπεδο ασφάλειας που παρέχεται.

Η JCC Payment Systems διαθέτει διαδικασίες για τη διασφάλιση ότι οι ενημερώσεις κώδικα ασφαλείας εφαρμόζονται στο σύστημα πιστοποίησης σε εύλογο χρονικό διάστημα αφού καταστούν διαθέσιμες αλλά το αργότερο εντός έξι μηνών μετά τη διαθεσιμότητα των ενημερώσεων κώδικα ασφαλείας. Οι λόγοι για τη μη εφαρμογή ουδεμίας ενημέρωσης κώδικα ασφαλείας θα τεκμηριώνονται.

Η JCC Payment Systems διαχειρίζεται την καταχώριση των πηγών πληροφοριών και ταξινομεί όλες τις πληγές πληροφοριών σύμφωνα με τα αποτελέσματα της τακτικής ανάλυσης για την ασφάλεια σχετικά με την αξιολόγηση κινδύνων.

6.7 *Έλεγχοι ασφάλειας δικτύου*

Η JCC Payment Systems εκτελεί όλες τις λειτουργίες των ΑΠ και ΑΕ της, χρησιμοποιώντας δίκτυα που είναι ασφαλή σύμφωνα με το ISMS της JCC Payment Systems και το ISMS της ADACOM για την αποτροπή της μη εξουσιοδοτημένης πρόσβασης και άλλων κακόβουλων ενεργειών. Η JCC Payment Systems προστατεύει την κοινοποίηση ευαίσθητων πληροφοριών μέσω της κρυπτογράφησης και των ψηφιακών υπογραφών.

Το επίπεδο ασφαλείας του εσωτερικού δικτύου και των εξωτερικών συνδέσεων παρακολουθείται συνέχεια προκειμένου να αποτραπεί η πρόσβαση σε πρωτόκολλα και υπηρεσίες που δεν απαιτούνται για τη λειτουργία των Υπηρεσιών Εμπιστοσύνης.

Η JCC Payment Systems εκτελεί μια αξιολόγηση για την ευπάθεια σε περιοδική βάση σε δημόσιες και ιδιωτικές διευθύνσεις IP. Επίσης δοκιμές διείσδυσης διενεργούνται στα συστήματα πιστοποίησης ετησίως ή κατόπιν σημαντικών αλλαγών.

6.8 *Χρονοσήμανση*

Τα Πιστοποιητικά, οι ΚΑΠ καθώς και οι άλλες καταχωρίσεις ανάκλησης στη βάση δεδομένων περιλαμβάνουν πληροφορίες σχετικά με την ώρα και την ημερομηνία.

Ο χρόνος συστήματος στους υπολογιστές της JCC Payment Systems ενημερώνεται χρησιμοποιώντας το πρωτόκολλο χρόνου δικτύου (Network Time Protocol - NTP) για συγχρονισμό των ρολογιών του συστήματος τουλάχιστον μία φορά κάθε μία ώρα.

7 ΠΡΟΦΙΛ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ, ΚΑΠ ΚΑΙ OCSP

7.1 *Προφίλ Πιστοποιητικού*

Το προφίλ πιστοποιητικού είναι σύμφωνο με το X.509 έκδοση 3, το RFC 5280 της Ομάδας Μελέτης του Internet (IETF) και το άρθρο 6.6.1 του προτύπου ETSI EN 319 411-1.

7.1.1 Αριθμός Έκδοσης

Όλα τα πιστοποιητικά είναι X.509 έκδοση 3.

7.1.2 Επεκτάσεις Πιστοποιητικού

Κάθε πιστοποιητικό που εκδίδεται περιέχει επεκτάσεις όπως ορίζονται για τα X.509v3 Πιστοποιητικά.

Τα πιστοποιητικά της τεχνικά περιορισμένης Εκδότριας ΑΠ της JCC Payment Systems περιέχει επέκταση Extended Key Usage (EKU) η οποία εξειδικεύει όλες τις επεκτεινόμενες χρήσεις κλειδιού για τις οποίες το Πιστοποιητικό της Εκδότριας ΑΠ εξουσιοδοτείται να εκδίδει πιστοποιητικά. Το anyExtendedKeyUsage KeyPurposeId δεν εμφανίζεται στην επέκταση EKU των πιστοποιητικών της JCC Payment System.

Παρακάτω υπάρχει λίστα των επεκτάσεων που χρησιμοποιούνται από την JCC Payment Systems για κάθε τύπο πιστοποιητικού:

7.1.2.1 Για ΑΠ Βάσης

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.56511.1.1**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.jcc.com.cy/repository**
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the Root Certificate.*

7.1.2.2 Για τις Εκδότριες ΑΠ για Ηλεκτρονικές Υπογραφές (JCC Issuing CA for eSignatures)

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	Subject Type	**CA**

	Maximum Path Length	**0**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.56511.1.1.1**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.jcc.com.cy/cps**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl.jcc.com.cy/ca/root.crl**
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://pki.jcc.com.cy/certs/root.crt**
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Authority Key Identifier	Directory Address	CN=PRIVATE-4096-8

7.1.2.3 Για τις Εκδότριες ΑΠ για Ηλεκτρονικές Σφραγίδες (JCC Issuing CA for eSeals)

Κανονική Επέκταση	***Πεδίο***	***Τιμή***
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**0**
Certificate Policies	**Cert Policy ID**	1.3.6.1.4.1.56511.1.1.1
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/cps
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://crl.jcc.com.cy/ca/root.crl
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	http://pki.jcc.com.cy/certs/root.crt
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Subject Alternative Name	Directory Address	*CN=PRIVATE-4096-9*

7.1.2.4 Για τις Εκδότριες ΑΠ για Ηλεκτρονική Ταυτότητα (JCC eID CA)

Κανονική Επέκταση	***Πεδίο***	***Τιμή***

Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**0**
Certificate Policies	**Cert Policy ID**	1.3.6.1.4.1.56511.1.1.2
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.jcc.com.cy/cps**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl.jcc.com.cy/ca/root.crl**
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://pki.jcc.com.cy/certs/root.crt**
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*
Authority Key Identifier	Directory Address	CN=PRIVATE-4096-10

7.1.2.5 Για τις Εκδότριες ΑΠ για Ηλεκτρονικές Υπογραφές (JCC Issuing CA for eSignatures G1)

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**0**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.56511.1.1.1**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	**https://pki.jcc.com.cy/cps**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	**http://crl.jcc.com.cy/ca/root.crl**
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	**http://pki.jcc.com.cy/certs/root.crt**
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*

7.1.2.6 Για τις Εκδότριες ΑΠ για Ηλεκτρονικές Σφραγίδες (JCC Issuing CA for eSeals G1)

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**0**
Certificate Policies	**Cert Policy ID**	**1.3.6.1.4.1.56511.1.1.1**
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/repository
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://crl.jcc.com.cy/ca/root.crl
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	http://pki.jcc.com.cy/certs/root.crt
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*

7.1.2.7 Για τις Εκδότριες ΑΠ για Ηλεκτρονική Ταυτότητα (JCC eID CA G1)

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	Subject Type	**CA**
	Maximum Path Length	**0**
Certificate Policies	**Cert Policy ID**	1.3.6.1.4.1.56511.1.1.2
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CP/CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/repository
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://crl.jcc.com.cy/ca/root.crl
Key Usage	Certificate Signing	**Set**
	Off-line CRL Signing	**Set**
	CRL Signing	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	http://pki.jcc.com.cy/certs/root.crt
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*

7.1.2.8 Για τις Ηλεκτρονικές Υπογραφές Φυσικού Προσώπου

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/cps
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.1**
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.1.0**
	Cert Policy ID	**0.4.0.194112.1.2**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://pki.jcc.com.cy/crl/eSignature/LatestCRL.crl or http://crl.jcc.com.cy/crl/eSignature-G1/LatestCRL.crl
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location	https://pki.jcc.com.cy/repository/PDS/
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEsign	**0.4.0.1862.1.6.1**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	http://ocsp.jcc.com.cy or http://ocsp2.jcc.com.cy
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	https://pki.jcc.com.cy/certs/ca-esign.crt **or** https://pki.jcc.com.cy/certs/ca-esign-g1.crt
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*

7.1.2.9 Για τις Ηλεκτρονικές Υπογραφές Φυσικού Προσώπου που συνδέεται με Νομικό

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	

	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/cps
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.1**
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.1.0**
	Cert Policy ID	**0.4.0.194112.1.2**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://pki.jcc.com.cy/crl/eSignature/LatestCRL.crl or http://crl.jcc.com.cy/crl/eSignature-G1/LatestCRL.crl
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location	https://pki.jcc.com.cy/repository/PDS/
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEsign	**0.4.0.1862.1.6.1**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	http://ocsp.jcc.com.cy or http://ocsp2.jcc.com.cy
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	https://pki.jcc.com.cy/certs/ca-esign.crt **or** https://pki.jcc.com.cy/certs/ca-esign-g1.crt
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*

7.1.2.10 Για τις Ηλεκτρονικές Σφραγίδες Νομικού Προσώπου

Κανονική Επέκταση	***Πεδίο***	***Τιμή***
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/cps
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.1**
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.1.0**
	Cert Policy ID	**0.4.0.194112.1.3**
CRL Distribution Point	Distribution Point	**Full Name**

	Uniform Resource ID	http://pki.jcc.com.cy/crl/eSeal/LatestCRL.crl or http://pki.jcc.com.cy/crl/eSeal-G1/LatestCRL.crl
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**
	PDS Location	https://pki.jcc.com.cy/repository/PDS/
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEseal	**0.4.0.1862.1.6.2**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	http://ocsp.jcc.com.cy or http://ocsp2.jcc.com.cy
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	http://pki.jcc.com.cy/certs/ca-eseal.crt or http://pki.jcc.com.cy/certs/ca-eseal-g1.crt
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*

7.1.2.11 Για ηλεκτρονικές υπογραφές μέσω της Ηλεκτρονικής Ταυτότητας

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/cps
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.2**
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.2.1**
	Cert Policy ID	**0.4.0.194112.1.2**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://pki.jcc.com.cy/crl/eID/LatestCRL.crl or http://pki.jcc.com.cy/crl/eID-G1/LatestCRL.crl
Key Usage	Non-Repudiation	**Set**
	Digital Signature	**Set**
Qualified Certificate Statements	**etsiQcsCompliance**	**0.4.0.1862.1.1**
	etsiQcsQcSSCD	**0.4.0.1862.1.4**
	etsiQcPDS	**0.4.0.1862.1.5**

	PDS Location	https://pki.jcc.com.cy/repository/PDS/
	etsiQcType	**0.4.0.1862.1.6**
	etsiQcTypeEsign	**0.4.0.1862.1.6.1**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	http://ocsp.jcc.com.cy or http://ocsp2.jcc.com.cy
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	http://pki.jcc.com.cy/certs/ca-eid.crt or http://pki.jcc.com.cy/certs/ca-eid--g1.crt
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*

7.1.2.12 Για αυθεντικοποίηση μέσω της Ηλεκτρονικής Ταυτότητας

Κανονική Επέκταση	*Πεδίο*	*Τιμή*
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/cps
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.2**
	Cert Policy ID	**1.3.6.1.4.1.56511.1.1.2.2**
	Cert Policy ID	**0.4.0.2042.1.2**
CRL Distribution Point	Distribution Point	**Full Name**
	Uniform Resource ID	http://pki.jcc.com.cy/crl/eID/LatestCRL.crl or http://pki.jcc.com.cy/crl/eID-G1/LatestCRL.crl
Key Usage	Digital Signature	**Set**
Authority Information Access	Access Method	**1.3.6.1.5.5.7.48.1**
	Access Location	http://ocsp.jcc.com.cy or http://ocsp2.jcc.com.cy
	Access Method	**1.3.6.1.5.5.7.48.2**
	Access Location	http://pki.jcc.com.cy/certs/ca-eid.crt or http://pki.jcc.com.cy/certs/ca-eid--g1.crt
Subject Key Identifier	Key Identifier	*This field contains the ID of the Certificate Holder's key.*

7.1.3 Αναγνωριστικά Αντικειμένου Αλγορίθμου

Οι αλγόριθμοι υπογραφής ακολουθούν τις προδιαγραφές που περιγράφονται στις ενότητες 6.1.5 και 6.1.6. Όλοι οι αλγόριθμοι που χρησιμοποιούνται για τις ΑΠ και τον Συνδρομητή ακολουθούν τα ισχύοντα πρότυπα έρευνας και βιομηχανίας για την παροχή εύλογης ασφάλειας για τους επιδιωκόμενους σκοπούς που χρησιμοποιούνται.

7.1.4 Τύποι Ονομάτων

Κάθε πιστοποιητικό περιέχει έναν μοναδικό αύξοντα αριθμό που δεν επαναχρησιμοποιείται ποτέ.
Το περιεχόμενο του πεδίου Issuer Distinguished Name αντιστοιχεί στο Subject DN της Εκδότριας ΑΠ για την υποστήριξη της αλυσιδωτής ονοματοδοσίας όπως ορίζεται στο RFC 5280, ενότητα 4.1.2.4.

7.1.4.1 Για πιστοποιητικό υπογραφής φυσικού προσώπου

Πεδίο	***Τιμή***	
Issuer	*For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.*	
Subject DN	Common Name	*Space separated Person Given name and Surname.*
	givenName	*Person given name in UTF8 format according to RFC5280*
	sureName	*Person surename in UTF8 format according to RFC5280*
	serialNumber	*Random code as specified in clause 5.1.3 of ETSI EN 319 412-1*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.4.2 Για πιστοποιητικό υπογραφής φυσικού προσώπου που συνδέεται με νομικό

Πεδίο	***Τιμή***	
Issuer	*For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.*	
Subject DN	Common Name	*Space separated Person Given name and Surname.*
	givenName	*Person given name in UTF8 format according to RFC5280*
	sureName	*Person surename in UTF8 format according to RFC5280*
	serialNumber	*Random code as specified in clause 5.1.3 of ETSI EN 319 412-1*
	Organization	*Issuer organization name who made subscriber identification.*
	Organization Unit	*Issuer organization unit name (optional)*
	OrganizationIdentifier	*Legal Entity's Identification Number from a national trade register with the following semantics: "**NTR**CY-123456789".* *Legal Entity's Tax Identification Number with the following semantics:* *"**VAT**CY-123456789"*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.4.3 Για Ηλεκτρονικές Σφραγίδες Νομικού Προσώπου

Πεδίο	***Τιμή***	
Issuer	*For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.*	
Subject DN	Common Name	*Legal Person's name*
	Organization	*Issuer organization name who made subscriber identification.*
	Organization Unit	*Issuer organization unit name (optional)*
	OrganizationIdentifier	*Legal Entity's Identification Number from a national trade register with the following semantics: "**NTR**CY-123456789".*
		*Legal Entity's Tax Identification Number with the following semantics: "**VAT**CY-123456789"*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.4.4 Για πιστοποιητικό υπογραφής της Ηλεκτρονικής Ταυτότητας

Πεδίο	***Τιμή***	
Issuer	*For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.*	
Subject DN	Common Name	*Space separated Person Given name and Surname.*
	givenName	*Person given name in UTF8 format according to RFC5280*
	sureName	*Person surename in UTF8 format according to RFC5280*
	serialNumber	*Personal Identification Card with the following semantics: "IDCCY-0000123456787"*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	
Key Size	**2048**	
Validity Start	*First date of certificate validity*	
Validity End	*Last date of certificate validity*	
Signature Algorithm	**Sha256withRSAEncryption**	

7.1.4.5 Για πιστοποιητικό αυθεντικοποίησης της Ηλεκτρονικής Ταυτότητας

Πεδίο	***Τιμή***	
Issuer	*For Issuing CA certificates, the commonName attribute is present and the contents is an identifier that uniquely identifies the CA and distinguishes it from other CAs.*	
Subject DN	Common Name	*Space separated Person Given name and Surname.*
	givenName	*Person given name in UTF8 format according to RFC5280*
	sureName	*Person surename in UTF8 format according to RFC5280*
	serialNumber	*Personal Identification Card with the following semantics: "IDCCY-0000123456787"*
	Country	*2-character ISO 3166 country code*
Version	**3**	
Serial number	*Unique serial number of the certificate*	

Key Size	**2048**
Validity Start	*First date of certificate validity*
Validity End	*Last date of certificate validity*
Signature Algorithm	**Sha256withRSAEncryption**

7.1.5 Περιορισμοί Ονομάτων

Η JCC Payment Systems μπορεί να συμπεριλάβει περιορισμού ονομάτων στο πεδίο nameConstraints όταν αυτό κριθεί κατάλληλο.
Εάν μια Εκδότρια ΑΠ συμπεριλάβει την επεκτεινόμενη χρήση κλειδιού “id-kp-emailProtection” θα θεωρείται ως τεχνικά περιορισμένη και θα ελέγχεται όπως περιγράφεται στην ενότητα 8.

7.1.6 Αναγνωριστικά Αντικειμένου Πολιτικής Πιστοποιητικού

Σύμφωνα με τον κάθε τύπο πιστοποιητικού, τα παρακάτω αναγνωρισμένα OIDs μπορούν να προστεθούν στην επέκταση certificatePolicies:

- **QCP-n-qscd**: 0.4.0.194112.1.2 όπως περιγράφεται στο ETSI EN 319 411-2
- **QCP-l-qscd**: 0.4.0.194112.1.3 όπως περιγράφεται στο ETSI EN 319 411-2
- **NCP+**: 0.4.0.2042.1.2 όπως περιγράφεται στο ETSI EN 319 411-1

7.1.7 Χρήση Επέκτασης των Περιορισμών Πολιτικής

Δεν εφαρμόζεται.

7.1.8 Σύνταξη και σημασιολογία Προδιαγραφών Πολιτικής

Ο προσδιοριστής πολιτικής είναι η URL που παραπέμπει στη δημοσιευμένη ΔΠΠ της JCC Payment Systems.

7.1.9 Επεξεργασία Σημασιολογίας για την Επέκταση των Κρίσιμων Πολιτικών Πιστοποιητικού

Δεν προβλέπεται.

7.2 *Προφίλ ΚΑΠ*

Το προφίλ ΚΑΠ είναι σύμφωνα με την έκδοση 2 του X.509 και το RFC 5280 της Ομάδας Μελέτης του Internet (IETF).

7.2.1 Αριθμός Έκδοσης

Η JCC Payment Systems εκδίδει ΚΑΠ version 2 που περιέχουν τα παρακάτω πεδία:

Πεδίο	Τιμή
Issuer Signature Algorithm	sha-256WithRSAEncryption [1 2 840 113549 1 1 11]
Issuer Distinguished Name	JCC Issuing CA SubjectDN
thisUpdate	*CRL issue date in UTC format*
nextUpdate	Date when the next CRL will issue in UTC format.

Revoked Certificates List	List of revoked Certificates, including the serial number and revocation date
Signature	*The signature algorithm MUST follow the requirements described in sections 6.1.5 and 6.1.6*

7.2.2 Επεκτάσεις ΚΑΠ και Καταχωρίσεων ΚΑΠ

Οι ΚΑΠ έχουν τις παρακάτω επεκτάσεις:

Πεδίο	Τιμή
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the Certificate
Invalidity Date	Optional date in UTC format
Reason Code	Optional reason for revocation
ExpiredCertsOnCRL	This CRL extension field indicates that the CRL includes revocation notices for expired certificates

7.3 *Προφίλ OCSP*

7.3.1 Αριθμός Έκδοσης

Οι αποκριτές OCSP της JCC Payment Systems συμμορφώνονται με την έκδοση 1 του RFC 6960.

7.3.2 Επεκτάσεις OCSP

Κανονική Επέκταση	Πεδίο	Τιμή
Authority Key Identifier	Key Identifier	*This field contains the Subject Key Identifier of the issuer's Certificate.*
Basic Constraint	End Entity	**Yes**
	Maximum Path Length	**None**
Certificate Policies	**Cert Policy ID**	1.3.6.1.4.1.56511.1.1.1
	Cert Policy Qualifier ID	**1.3.6.1.5.5.7.2.1** (CPS Pointer)
	Cert Qualifier	https://pki.jcc.com.cy/cps
Key Usage	Digital Signature	**Set**
OCSP No Revocation Checking	ocsp-nocheck	**Set**
Enhanced Key Usage	OCSP Signing	**Set**
Subject Alternative Name	Directory Address	CN=OCSP2048-1-28 (eSignatures) CN=OCSP2048-1-29 (eSeals)
Subject Key Identifier	RFC822 Name	*This field contains the ID of the Certificate Holder's key.*

8 ΕΛΕΓΧΟΣ ΣΥΜΜΟΡΦΩΣΗΣ ΚΑΙ ΑΛΛΕΣ ΑΞΙΟΛΟΓΗΣΕΙΣ

Η συμμόρφωση του πληροφοριακού συστήματος, των πολιτικών και των πρακτικών, των εγκαταστάσεων, του προσωπικού και των περιουσιακών στοιχείων της JCC Payment Systems αξιολογείται από έναν φορέα αξιολόγησης συμμόρφωσης σύμφωνα με τον κανονισμό eIDAS, την αντίστοιχη νομοθεσία και πρότυπα ή όποτε συντελείται μια σημαντική αλλαγή στις λειτουργίες της Υπηρεσίας Εμπιστοσύνης, βάσει των προτύπων ETSI που αναφέρονται στην Ενότητα 9.15.

Πέρα από τους ελέγχους συμμόρφωσης, η JCC Payment Systems δικαιούται να διενεργεί και άλλες επιθεωρήσεις και έρευνες ώστε να διασφαλίσει την αξιοπιστία των Υπηρεσιών Πιστοποίησης της JCC

Payment Systems . Η JCC Payment Systems δικαιούται να αναθέσει την εκτέλεση των εν λόγω ελέγχων, επιθεωρήσεων και ερευνών σε μια εξωτερική ελεγκτική εταιρεία.

Η JCC Payment Systems δικαιούται να διενεργεί δεύτερο κύκλο ελέγχων σε αναδόχους που έχουν συνάψει σχέση με την JCC Payment Systems για να λειτουργούν ως Αρχές Εγγραφής (ΑΕ) ή Τοπικές Αρχές Εγγραφής (ΤΑΕ).

8.1 *Συχνότητα και συνθήκες αξιολόγησης*

Οι Έλεγχοι Συμμόρφωσης της JCC Payment Systems διενεργούνται τουλάχιστον σε ετήσια βάση. Οι έλεγχοι διενεργούνται στο πλαίσιο μιας συνεχούς ακολουθίας ελεγκτικών περιόδων όπου η καθεμία δεν ξεπερνά σε διάρκεια το ένα έτος.

8.2 *Ταυτότητα/τυπικά προσόντα του αξιολογητή*

Οι έλεγχοι συμμόρφωσης της ΑΠ της JCC Payment Systems πραγματοποιούνται από τους εξής:

- τους Εσωτερικούς Ελεγκτές,
- τον οργανισμό αξιολόγησης της συμμόρφωσης ο οποίος έχει διαπιστευθεί σύμφωνα με τον κανονισμό (ΕΚ) αριθ. 765/2008 και το πρότυπο EN 319 403, τα πρότυπα ETSI και τις Βασικές Απαιτήσεις (ενότητα 8.2).
- τον Εποπτικό Φορέα.

8.3 *Σχέση του αξιολογητή με την υπό αξιολόγηση οντότητα*

Ο ελεγκτής του οργανισμού αξιολόγησης της συμμόρφωσης πρέπει να είναι ανεξάρτητος από την JCC Payment Systems και από τα συστήματα της JCC Payment Systems που αξιολογούνται.

Ο εσωτερικός ελεγκτής δεν ελέγχει τους τομείς της αρμοδιότητάς του.

8.4 *Θέματα που καλύπτει η αξιολόγηση*

Η αξιολόγηση της συμμόρφωσης καλύπτει τη συμμόρφωση του πληροφοριακού συστήματος, των πολιτικών και των πρακτικών, των εγκαταστάσεων, του προσωπικού και των περιουσιακών στοιχείων της JCC Payment Systems με τον κανονισμό eIDAS, την αντίστοιχη νομοθεσία και πρότυπα. Ο οργανισμός αξιολόγησης της συμμόρφωσης ελέγχει τα μέρη του πληροφοριακού συστήματος που χρησιμοποιούνται για την παροχή των Υπηρεσιών Εμπιστοσύνης.

Οι τομείς δραστηριότητας που υπάγονται στον εσωτερικό έλεγχο είναι οι εξής:

- η ποιότητα της υπηρεσίας,
- η ασφάλεια της υπηρεσίας,
- η ασφάλεια των λειτουργιών και των διαδικασιών,
- η προστασία των δεδομένων των Συνδρομητών και η πολιτική ασφάλειας, η εκτέλεση των διαδικασιών εργασιών και των συμβατικών υποχρεώσεων, καθώς και η συμμόρφωση με την ΠΠ και τις δηλώσεις πολιτικών και πρακτικών βάσει υπηρεσιών.

Ο Οργανισμός Αξιολόγησης της Συμμόρφωσης και ο Εσωτερικός Ελεγκτής ελέγχουν επίσης τα τμήματα του πληροφοριακού συστήματος, των πολιτικών και των πρακτικών, των εγκαταστάσεων, του προσωπικού και των περιουσιακών στοιχείων των υπεργολάβων που σχετίζονται με την παροχή Υπηρεσιών Εμπιστοσύνης της JCC Payment Systems (π.χ. συμπεριλαμβανομένων των ΤΑΕ).

8.5 *Ανάληψη ενεργειών λόγω ανεπαρκειών*

Όσον αφορά τους ελέγχους συμμόρφωσης των λειτουργιών της JCC Payment Systems , σημαντικές εξαιρέσεις ή ανεπάρκειες που έχουν εντοπιστεί κατά τη διενέργεια του Ελέγχου Συμμόρφωσης θα οδηγήσουν στον προσδιορισμό των ενεργειών που πρέπει να ληφθούν. Ο συγκεκριμένος προσδιορισμός πραγματοποιείται από τη Διεύθυνση της JCC Payment Systems με δεδομένα που

προέρχονται από τον ελεγκτή. Η Διεύθυνση της JCC Payment Systems είναι υπεύθυνη για την ανάπτυξη και την υλοποίηση ενός σχεδίου λήψης διορθωτικών μέτρων. Σε περίπτωση που η JCC Payment Systems προσδιορίσει ότι οι εν λόγω εξαιρέσεις ή ανεπάρκειες απειλούν την ασφάλεια ή την ακεραιότητα των Υπηρεσιών Εμπιστοσύνης, θα αναπτυχθεί ένα σχέδιο ανάληψης διορθωτικών μέτρων εντός 30 ημερών και θα υλοποιηθεί εντός ενός ευλόγου από εμπορικής άποψης χρονικού διαστήματος. Για λιγότερο σημαντικές εξαιρέσεις ή ανεπάρκειες, η Διεύθυνση της JCC Payment Systems θα αξιολογεί τη σπουδαιότητα των σχετικών ζητημάτων και θα καθορίζει την ανάλογη πορεία δράσης.

Επιπλέον, σε περίπτωση που τα αποτελέσματα της αξιολόγησης του Οργανισμού Αξιολόγησης της Συμμόρφωσης καταδείξουν την ύπαρξη ανεπάρκειας, ο Εποπτικός Φορέας απαιτεί από την JCC Payment Systems να αποκαταστήσει τη μη τήρηση των απαιτήσεων εντός προθεσμίας (εάν ισχύει) που ορίζει ο Εποπτικός Φορέας. Η JCC Payment Systems καταβάλλει προσπάθειες να παραμένει συμμορφούμενη και να εκπληρώνει έγκαιρα όλες τις απαιτήσεις σχετικά με την ανεπάρκεια. Η Διεύθυνση της JCC Payment Systems είναι υπεύθυνη για την υλοποίηση ενός σχεδίου ανάληψης διορθωτικών μέτρων. Η JCC Payment Systems αξιολογεί τη σπουδαιότητα των ανεπαρκειών και θέτει σε προτεραιότητα τις ανάλογες ενέργειες που πρέπει να ληφθούν τουλάχιστον κατά το χρονικό περιθώριο που έχει ορίσει ο Εποπτικός Φορέας ή εντός εύλογου χρονικού διαστήματος.

Όταν υπάρχουν ενδείξεις ότι έχουν παραβιαστεί οι κανόνες προστασίας των προσωπικών δεδομένων, ο Εποπτικός Φορέας ενημερώνει τις αρχές προστασίας δεδομένων για τα αποτελέσματα των ελέγχων συμμόρφωσης.

8.6 *Κοινοποιήσεις των αποτελεσμάτων*

Τα συμπεράσματα των ελέγχων ή το(τα) πιστοποιητικό(ά) για την(τις) υπηρεσία(ες) εμπιστοσύνης, τα οποία βασίζονται σε αποτελέσματα ελέγχου του οργανισμού αξιολόγησης της συμμόρφωσης που διενεργείται σύμφωνα με τον κανονισμό eIDAS, την αντίστοιχη νομοθεσία και πρότυπα, δύνανται να δημοσιεύονται στον δικτυακό τόπο της JCC Payment Systems στη διεύθυνση: https://pki.jcc.com.cy/repository.

Επιπλέον, η JCC Payment Systems υποβάλει τη σχετική έκθεση για την αξιολόγηση της συμμόρφωσης στον Εποπτικό Φορέα εντός τριών (3) εργάσιμων ημερών μετά τη λήψη της. Η JCC Payment Systems υποβάλλει τα συμπεράσματα του ελέγχου ή το(τα) πιστοποιητικό(ά) για την(τις) υπηρεσία(ες) εμπιστοσύνης στους υπαλλήλους συντήρησης προγραμμάτων περιήγησης (Root Browser) στα οποία συμμετέχει η JCC Payment Systems και άλλα ενδιαφερόμενα μέρη.

Τα αποτελέσματα των εσωτερικών ελέγχων των λειτουργιών της JCC Payment Systems δύνανται να δημοσιευτούν κατά τη διακριτική ευχέρεια της Διεύθυνση της JCC Payment Systems.

8.7 *Εσωτερικοί Έλεγχοι*

Η JCC Payment Systems πραγματοποιεί τακτικού εσωτερικούς ελέγχους ώστε να επιβεβαιώνει τη συμμόρφωση κατά την ενότητα 8.4.

9 ΑΛΛΑ ΕΠΙΧΕΙΡΗΣΙΑΚΑ ΚΑΙ ΝΟΜΙΚΑ ΘΕΜΑΤΑ

9.1 *Τέλη*

9.1.1 Τέλη έκδοσης ή ανανέωσης Πιστοποιητικού

Η JCC Payment Systems χρεώνει τους Συνδρομητές για την έκδοση, τη διαχείριση και την επαναδημιουργία κλειδιών των Πιστοποιητικών.

9.1.2 Τέλη για την πρόσβαση σε Πιστοποιητικό

Η JCC Payment Systems δεν χρεώνει τέλη για τη διαθεσιμότητα ενός Πιστοποιητικού σε χώρο αποθήκευσης ή την κατ΄ άλλον τρόπο διαθεσιμότητα των Πιστοποιητικών προς τα Βασιζόμενα Μέρη.

9.1.3 Τέλη για την πρόσβαση σε πληροφορίες ανάκλησης ή κατάστασης

Η JCC Payment Systems δεν χρεώνει τέλη ως προϋπόθεση για τις υπηρεσίες OCSP και τη διαθεσιμότητα των ΚΑΠ όπως απαιτείται από την παρούσα ΠΠ και την σχετική ΔΠΠ σε χώρο αποθήκευσης ή την κατ΄ άλλον τρόπο διαθεσιμότητά τους προς τα Βασιζόμενα Μέρη. Η JCC Payment Systems δεν επιτρέπει την πρόσβαση σε πληροφορίες ανάκλησης ή πληροφορίες κατάστασης Πιστοποιητικού στους χώρους αποθήκευσής της σε τρίτους που παρέχουν προϊόντα ή υπηρεσίες που κάνουν χρήση των σχετικών πληροφοριών για την κατάσταση του Πιστοποιητικού χωρίς την πρότερη έγγραφη και ρητή συγκατάθεση της.

9.1.4 Τέλη για άλλες υπηρεσίες

Η JCC Payment Systems δεν χρεώνει τέλη για την πρόσβαση στην παρούσα ΔΠΠ. Οποιαδήποτε χρήση γίνεται για σκοπούς άλλους, πέραν της απλής προβολής των εγγράφων αυτών, όπως είναι η αναπαραγωγή, η αναδιανομή, η τροποποίηση ή η δημιουργία παράγωγων έργων, υπόκειται σε σύμβαση παραχώρηση σχετικής άδειας χρήσης με την JCC Payment Systems.

9.1.5 Πολιτική επιστροφής χρημάτων

9.1.5.1 Πωλήσεις εξ αποστάσεως

Σε περίπτωση που η πώληση του Πιστοποιητικού πραγματοποιηθεί μέσω διαδικτύου ή τηλεφώνου, ο Συνδρομητής έχει το δικαίωμα, σύμφωνα με το άρθρο 8 παρ. 1 του Ν. 133(Ι)/2013, όπως τροποποιήθηκε, να καταγγείλει τη σύμβαση πώλησης χωρίς να αναφέρει τους λόγους εντός του αποκλειστικού χρονικού ορίου των δεκατεσσάρων (14) ημερών από την ημερομηνία αγοράς. Η άσκηση του εν λόγω δικαιώματος μπορεί να γίνει γραπτώς από τον Συνδρομητή στην JCC Payment Systems μέσω της αποστολής μηνύματος ηλεκτρονικού ταχυδρομείου στη διεύθυνση: trust-sales@jcc.com.cy. Ακολούθως, και μετά την κοινοποίηση, η JCC Payment Systems υποχρεούται να επιστρέψει τα χρήματα που αντιστοιχούν στην αξία της σύμβασης πώλησης στον Συνδρομητή. Η πληρωμή της επιστροφής χρημάτων πραγματοποιείται με την ίδια μέθοδο όπως εκείνη της αρχικής πληρωμής και ο Συνδρομητής δεν έχει το δικαίωμα να χρησιμοποιήσει το Πιστοποιητικό. Μετά το πέρας της εν λόγω περιόδου, η ισχύς του δικαιώματος καταγγελίας λήγει και η JCC Payment Systems δεν έχει περαιτέρω υποχρέωση για την παραπάνω αιτία.

9.1.5.2 Άλλες περιπτώσεις

Με την επιφύλαξη της ενότητας 9.1.5.1, η JCC Payment Systems χειρίζεται ξεχωριστά κάθε περίπτωση επιστροφής χρημάτων.
Για την υποβολή αίτησης επιστροφής χρημάτων, ο Συνδρομητής θα πρέπει αποστείλει μια έγγραφη αίτηση στην JCC Payment Systems . Η παρούσα πολιτική επιστροφής χρημάτων δεν αποτελεί αποκλειστικό μέσο ικανοποίησης και δεν περιορίζει άλλα σχετικά μέσα που δύνανται να είναι διαθέσιμα στους συνδρομητές.

9.2 *Οικονομική Ευθύνη*

9.2.1 Ασφαλιστική κάλυψη

Η JCC Payment Systems διατηρεί ένα εμπορικώς εύλογο επίπεδο ασφαλιστικής κάλυψης αστικής ευθύνης έναντι σφαλμάτων και παραλείψεων, μέσω ενός σχετικού προγράμματος ασφάλισης αστικής ευθύνης.

9.2.2 Άλλα περιουσιακά στοιχεία

Η JCC Payment Systems διαθέτει επαρκείς οικονομικούς πόρους προκειμένου να διατηρεί τις λειτουργίες της και να εκτελεί τα καθήκοντα της ενώ παράλληλα μπορεί ευλόγως να αντιμετωπίσει τον κίνδυνο ευθύνης απέναντι στους Συνδρομητές και τα Βασιζόμενα Μέρη. Αποδεικτικά στοιχεία των οικονομικών πόρων δεν δημοσιοποιούνται.

9.2.3 Ασφαλιστική ή εγγυητική κάλυψη για τελικούς χρήστες (οντότητες)

Ανατρέξτε στην ενότητα 9.2.1 της παρούσας ΠΠ.

9.3 *Εμπιστευτικότητα επιχειρηματικών Πληροφοριών*

9.3.1 Πεδίο εφαρμογής εμπιστευτικών πληροφοριών

Όλες οι πληροφορίες που έχουν καταστεί γνωστές κατά την παροχή υπηρεσιών και δεν προορίζονται για δημοσίευση (πχ. πληροφορίες που ήταν γνωστές στην JCC Payment Systems λόγω λειτουργίας και παροχής Υπηρεσιών Εμπιστοσύνης) είναι εμπιστευτικές. Ο Συνδρομητής έχει το δικαίωμα να λαμβάνει πληροφορίες από την JCC Payment Systems σχετικά με εκείνον σύμφωνα με την ισχύουσα νομοθεσία.

9.3.2 Πληροφορίες που δεν εμπίπτουν στο πεδίο εφαρμογής των εμπιστευτικών πληροφοριών

Οποιαδήποτε πληροφορία που δεν αναφέρεται ως εμπιστευτική ή δεν προβλέπεται για εσωτερική χρήση, συνιστά δημόσια πληροφορία. Οι πληροφορίες που θεωρούνται δημόσιου χαρακτήρα στην JCC Payment Systems , αναφέρονται στην ενότητα 2.2. της παρούσας ΠΠ.

Επιπλέον, τα μη εξατομικευμένα στατιστικά στοιχεία για τις υπηρεσίες της JCC Payment Systems θεωρούνται επίσης δημόσιες πληροφορίες. Η JCC Payment Systems δύναται να δημοσιεύσει μη εξατομικευμένα στατιστικά στοιχεία σχετικά με τις υπηρεσίες της.

9.3.3 Ευθύνη προστασίας εμπιστευτικών πληροφοριών

Η JCC Payment Systems προστατεύει τις εμπιστευτικές πληροφορίες καθώς και τις πληροφορίες που προορίζονται για εσωτερική χρήση ώστε να μην εκτίθενται σε κίνδυνο και να μη γνωστοποιούνται σε τρίτα μέρη μέσω της εφαρμογής διαφορετικών ελέγχων ασφαλείας.

Η γνωστοποίηση ή προώθηση εμπιστευτικών πληροφοριών σε τρίτους επιτρέπεται μόνο με τη γραπτή συγκατάθεση του νομικού κατόχου των πληροφοριών βάσει δικαστικής εντολής ή άλλων περιπτώσεων που προβλέπονται από τον νόμο.

9.4 *Απόρρητο προσωπικών στοιχείων*

9.4.1 Σχέδιο απορρήτου

Η JCC Payment Systems εφαρμόζει πολιτική απορρήτου η οποία βρίσκεται στην εξής διεύθυνση: https://pki.jcc.com.cy/repository σε συμμόρφωση με την ισχύουσα νομοθεσία.

9.4.2 Πληροφορίες που αντιμετωπίζονται ως ιδιωτικές

Οποιαδήποτε πληροφορία σχετικά με τους Συνδρομητές δεν είναι δημόσια διαθέσιμη μέσω του περιεχομένου του εκδοθέντος πιστοποιητικού, η υπηρεσία καταλόγου του πιστοποιητικού και οι ΚΑΠ σε σύνδεση (online) αντιμετωπίζονται ως ιδιωτικοί.

9.4.3 Πληροφορίες που δεν θεωρούνται ιδιωτικές

Με την επιφύλαξη της ισχύουσας νομοθεσίας, κάθε πληροφορία που δημοσιοποιείται σε ένα πιστοποιητικό δεν θεωρείται απόρρητη.

9.4.4 Ευθύνη για την προστασία ιδιωτικών πληροφοριών

Η JCC Payment Systems διασφαλίζει τις ιδιωτικές πληροφορίες από την έκθεση σε κίνδυνο και τη γνωστοποίηση σε τρίτους και συμμορφώνεται με την ισχύουσα νομοθεσία περί απορρήτου.

9.4.5 Ειδοποίηση και συγκατάθεση για χρήση ιδιωτικών πληροφοριών

Εφόσον δεν ορίζεται διαφορετικά στην παρούσα ΔΠΠ, η εφαρμόσιμη πολιτική απορρήτου ή, βάσει σύμβασης, οι ιδιωτικές πληροφορίες δεν θα χρησιμοποιούνται χωρίς τη συναίνεση του μέρους στο οποίο εφαρμόζονται οι εν λόγω πληροφορίες, σε συμμόρφωση με την ισχύουσα νομοθεσία περί απορρήτου.

9.4.6 Γνωστοποίηση πληροφοριών σύμφωνα με δικαστική ή διοικητική διαδικασία

Η JCC Payment Systems δικαιούται να γνωστοποιεί Εμπιστευτικές Πληροφορίες εάν η JCC Payment Systems , καλή τη πίστει, θεωρεί ότι:

- η γνωστοποίηση είναι απαραίτητη αναφορικά με δικαστικές κλητεύσεις και εντάλματα έρευνας,
- η γνωστοποίηση είναι απαραίτητη αναφορικά με δικαστικές, διοικητικές ή άλλες νομικές διαδικασίες κατά τη διερευνητική φάση σε αστικού ή διοικητικού χαρακτήρα αγωγές, όπως κλητεύσεις, ανακρίσεις, αιτήματα παραδοχής και αιτήματα για προσκόμιση τεκμηρίων.

Η παρούσα ενότητα υπόκειται στην εφαρμοστέα νομοθεσία περί απορρήτου.

9.4.7 Γνωστοποίηση κατόπιν αιτήματος κατόχου

Η πολιτική απορρήτου της JCC Payment Systems περιλαμβάνει διατάξεις σχετικά με τη γνωστοποίηση των ιδιωτικών πληροφοριών στο άτομο που τις γνωστοποιεί προς την JCC Payment Systems . Η παρούσα ενότητα υπόκειται στην εφαρμοστέα νομοθεσία περί απορρήτου.

9.4.8 Λοιπές συνθήκες γνωστοποίησης πληροφοριών

Καμία διατύπωση.

9.5 *Δικαιώματα Πνευματικής Ιδιοκτησίας*

Η απονομή των Δικαιωμάτων Πνευματικής Ιδιοκτησία ανάμεσα στους Συμμετέχοντες στην JCC Payment Systems, εκτός των Συνδρομητών και των Βασιζόμενων Μερών, διέπεται από τις ισχύουσες συμβάσεις μεταξύ των σχετικών Συμμετεχόντων στον Υποτομέα της JCC Payment Systems. Οι ακόλουθες υποενότητες αφορούν τα Δικαιώματα Πνευματικής Ιδιοκτησίας σε σχέση με τους Συνδρομητές και τα Βασιζόμενα Μέρη.

9.5.1 Δικαιώματα ιδιοκτησίας επί των πιστοποιητικών και των πληροφοριών ανάκλησης

Οι ΑΠ διατηρούν όλα τα Δικαιώματα Πνευματικής Ιδιοκτησίας σε και επί των Πιστοποιητικών και των πληροφοριών ανάκλησης που εκδίδουν. Η JCC Payment Systems χορηγεί την άδεια αναπαραγωγής και διανομής Πιστοποιητικών σε μη αποκλειστική βάση και άνευ υποχρέωσης καταβολής δικαιωμάτων, εφόσον αυτά αναπαράγονται πλήρως και η χρήση τους υπόκειται στους Γενικούς Όρους και Προϋποθέσεις για τη χρήση των Εγκεκριμένων Πιστοποιητικών που αναφέρονται στο Πιστοποιητικό. Η JCC Payment Systems χορηγεί άδεια για τη χρήση των πληροφοριών ανάκλησης προκειμένου να εκτελέσει τις λειτουργίες των Βασιζόμενων Μερών με την επιφύλαξη των Γενικών Όρων και Προϋποθέσεων για τη χρήση των Εγκεκριμένων Πιστοποιητικών ή οποιωνδήποτε άλλων εφαρμοστέων συμβάσεων.

9.5.2 Δικαιώματα ιδιοκτησίας επί της ΠΠ

Οι Συνδρομητές αναγνωρίζουν ότι η JCC Payment Systems διατηρεί όλα τα Δικαιώματα Πνευματικής Ιδιοκτησίας σε και επί της παρούσας ΠΠ.

9.5.3 Δικαιώματα ιδιοκτησίας επί των ονομάτων

Ο Αιτών Πιστοποιητικό διατηρεί όλα τα δικαιώματα που κατέχει (εάν υπάρχουν) επί οποιουδήποτε εμπορικού σήματος, σήματος παροχής υπηρεσιών ή εμπορικής επωνυμίας που περιλαμβάνεται σε οποιαδήποτε Αίτηση για Πιστοποιητικό και επί οποιουδήποτε διακριτικού ονόματος εντός οποιουδήποτε Πιστοποιητικού που έχει εκδοθεί για τον εν λόγω Αιτούντα Πιστοποιητικό.

9.5.4 Δικαιώματα ιδιοκτησίας επί των κλειδιών και του υλικού κλειδιών

Τα ζεύγη κλειδιών που αντιστοιχούν σε Πιστοποιητικά των ΑΠ και των Συνδρομητών αποτελούν ιδιοκτησία των ΑΠ και των Συνδρομητών οι οποίοι είναι τα αντίστοιχα Υποκείμενα των Πιστοποιητικών αυτών ανεξάρτητα από το φυσικό μέσο στο οποίο έχουν αποθηκευθεί και προστατεύονται και τα πρόσωπα αυτά διατηρούν όλα τα Δικαιώματα Πνευματικής Ιδιοκτησίας σε και επί των συγκεκριμένων ζευγών κλειδιών. Με την επιφύλαξη της γενικότητας των όσων ορίζονται προηγουμένως, τα δημόσια κλειδιά Βάσης (Root public Keys) της JCC Payment Systems και τα Πιστοποιητικά Βάσης (Root Certificates) που τα περιλαμβάνουν, αποτελούν ιδιοκτησία της JCC Payment Systems.
Τέλος, τα Μερίδια Απορρήτου του ιδιωτικού κλειδιού μιας ΑΠ αποτελούν ιδιοκτησία της ΑΠ, η οποία διατηρεί όλα τα Δικαιώματα Πνευματικής Ιδιοκτησίας επί αυτών των Μεριδίων Απορρήτου, ακόμη και αν δεν μπορούν να αποκτήσουν φυσική κατοχή των μεριδίων αυτών ή της ΑΠ από την JCC Payment Systems.

9.5.5 Παραβίαση δικαιωμάτων Πνευματικής Ιδιοκτησίας

Η JCC Payment Systems δεν παραβιάζει εν γνώσει της τα δικαιώματα πνευματικής ιδιοκτησίας οποιουδήποτε τρίτου μέρους.

9.6 *Δηλώσεις και Εγγυήσεις*

9.6.1 Δηλώσεις και Εγγυήσεις της ΑΠ

Η ΑΠ της JCC Payment Systems εγγυάται ότι:

- παρέχει τις υπηρεσίες της σύμφωνα με τις απαιτήσεις και τις διαδικασίες που ορίζονται στην παρούσα ΠΠ, την εφαρμοστέα ΔΠΠ και τα σχετικά έγγραφα·
- συμμορφώνεται με τον κανονισμό eIDAS και τις σχετικές νομικές πράξεις που ορίζονται στην παρούσα ΠΠ και τα σχετικά έγγραφα·
- δημοσιεύει τη ΠΠ, την ΔΠΠ και τα σχετικά έγγραφα και εγγυάται τη διαθεσιμότητά τους σε δημόσιο δίκτυο επικοινωνίας δεδομένων·
- δημοσιεύει και πληροί τις απαιτήσεις της σε ό,τι αφορά τους όρους και τις προϋποθέσεις για τους συνδρομητές και εγγυάται τη διαθεσιμότητα και πρόσβασή τους σε δημόσιο δίκτυο επικοινωνίας δεδομένων·
- διατηρεί την εμπιστευτικότητα των πληροφοριών για τις οποίες έχουν λάβει γνώση κατά τη διάρκεια της παροχής της υπηρεσίας και δεν υπόκεινται σε δημοσίευση·
- τηρεί λογαριασμό των εκδοθέντων από εκείνη Διακριτικών Υπηρεσιών Εμπιστοσύνης και της εγκυρότητάς τους και διασφαλίζει τη δυνατότητα ελέγχου της εγκυρότητας των πιστοποιητικών·
- εγγυάται την πρόσβαση σε ιδιωτικά κλειδιά σε εξ αποστάσεως ΕΔΔΥ, στο εξουσιοδοτημένο Υποκείμενο των κλειδιών
- Εγγυάται την κατάλληλη διαχείριση και συμμόρφωση της εξ αποστάσεως ΕΔΔΥ
- ενημερώνει τον Εποπτικό Φορέα για τυχόν αλλαγές σε ένα δημόσιο κλειδί που χρησιμοποιείται για την παροχή των Υπηρεσιών Εμπιστοσύνης·
- χωρίς αδικαιολόγητη καθυστέρηση αλλά, σε κάθε περίπτωση, εντός 24 ωρών αφού έχουν λάβουν γνώση αυτής, ειδοποιεί τον Εποπτικό Φορέα και, κατά περίπτωση, άλλους σχετικούς φορείς, όπως η εθνική αρχή αντιμετώπισης ηλεκτρονικών επιθέσεων (Εθνικό CERT) ή επιθεώρηση δεδομένων για την απώλεια ασφάλειας ή ακεραιότητας που έχει σημαντικό αντίκτυπο στην παρεχόμενη Υπηρεσία Εμπιστοσύνης ή στα προσωπικά δεδομένα που διατηρούνται σε αυτή·
- όπου η παραβίαση της ασφάλειας ή η απώλεια της ακεραιότητας είναι πιθανόν να επηρεάσει δυσμενώς φυσικό ή νομικό πρόσωπο στο οποίο έχει παρασχεθεί η Υπηρεσία Εμπιστοσύνης, ειδοποιεί το φυσικό ή νομικό πρόσωπο για την παραβίαση της ασφάλειας ή την απώλεια της ακεραιότητας χωρίς αδικαιολόγητη καθυστέρηση·
- διατηρεί όλη την τεκμηρίωση, τις εγγραφές και τα αρχεία καταγραφής που σχετίζονται με τις Υπηρεσίες Εμπιστοσύνης σύμφωνα με τις ενότητες 5.4 και 5.5·
- εξασφαλίζει την αξιολόγηση της συμμόρφωσης σύμφωνα με τις απαιτήσεις και προσκομίζει τα συμπεράσματα του οργανισμού αξιολόγησης της συμμόρφωσης στον Εποπτικό Φορέα προκειμένου να διασφαλιστεί η συνεχή κατάσταση των Υπηρεσιών Εμπιστοσύνης στον Κατάλογο Εμπιστοσύνης·
- διαθέτει την απαιτούμενη οικονομική σταθερότητα, καθώς και τους απαιτούμενους οικονομικούς πόρους για να λειτουργεί σύμφωνα με την παρούσα ΠΠ·
- δημοσιεύει τους όρους του υποχρεωτικού ασφαλιστηρίου συμβολαίου και τα συμπεράσματα του οργανισμού αξιολόγησης της συμμόρφωσης σε δημόσιο δίκτυο επικοινωνίας δεδομένων·
- δεν περιορίζει τη προσβασιμότητα στις υπηρεσίες της για άτομα με αναπηρίες·
- δεν υπάρχει καμία ψευδής δήλωση στοιχείων στο Πιστοποιητικό η οποία να είναι γνωστή ή να οφείλεται σε υπαιτιότητα των οντοτήτων που εγκρίνουν την Αίτηση για Πιστοποιητικό ή που εκδίδουν το Πιστοποιητικό·
- δεν υπάρχουν λάθη στα στοιχεία του Πιστοποιητικού τα οποία εισήχθηκαν από τις οντότητες που ενέκριναν την Αίτηση για Πιστοποιητικό ή που εξέδωσαν το Πιστοποιητικό ως αποτέλεσμα αποτυχίας να επιδείξουν εύλογη μέριμνα κατά τον χειρισμό της Αίτησης για Πιστοποιητικό ή τη δημιουργία του Πιστοποιητικού·
- Οι υπηρεσίες ανάκλησης και η χρήση του χώρου αποθήκευσης είναι σύμφωνες με την ισχύουσα ΠΠ σε κάθε ουσιώδη πτυχή.

Οι Γενικοί Όροι και Προϋποθέσεις της JCC Payment Systems για τη χρήση των Πιστοποιητικών δύνανται να περιλαμβάνουν πρόσθετες δηλώσεις και εγγυήσεις.

9.6.2 Δηλώσεις και Εγγυήσεις της ΑΕ

Η ΑΕ της JCC Payment Systems εγγυάται ότι:

- δεν υπάρχει καμία ψευδής δήλωση στοιχείων στο Πιστοποιητικό η οποία να είναι γνωστή ή να οφείλεται σε υπαιτιότητα των οντοτήτων που εγκρίνουν την Αίτηση για Πιστοποιητικό ή που εκδίδουν το Πιστοποιητικό·
- δεν υπάρχουν λάθη στα στοιχεία του Πιστοποιητικού τα οποία εισήχθηκαν από τις οντότητες που ενέκριναν την Αίτηση για Πιστοποιητικό ως αποτέλεσμα αποτυχίας να επιδείξουν εύλογη μέριμνα κατά τον χειρισμό της Αίτησης για Πιστοποιητικό·
- τα Πιστοποιητικά τους πληρούν όλες τις ουσιώδεις απαιτήσεις της παρούσας ΠΠ και
- οι υπηρεσίες ανάκλησης (κατά περίπτωση) και η χρήση του χώρου αποθήκευσης είναι σύμφωνες με την ισχύουσα ΠΠ σε κάθε ουσιώδη πτυχή.

Οι Γενικοί Όροι και Προϋποθέσεις της JCC Payment Systems για τη χρήση των Πιστοποιητικών δύνανται να περιλαμβάνουν πρόσθετες δηλώσεις και εγγυήσεις.

9.6.3 Δηλώσεις και εγγυήσεις του Συνδρομητή

Οι Συνδρομητές εγγυώνται ότι:

- κάθε Εγκεκριμένη Ηλεκτρονική Υπογραφή ή Ηλεκτρονική Σφραγίδα που έχει δημιουργηθεί με τη χρήση ιδιωτικού κλειδιού που αντιστοιχεί στο δημόσιο κλειδί που αναφέρεται στο Εγκεκριμένο Πιστοποιητικό, είναι η Εγκεκριμένη Ηλεκτρονική Υπογραφή ή Ηλεκτρονική Σφραγίδα του Συνδρομητή και το Εγκεκριμένο Πιστοποιητικό έχει εγκριθεί και είναι σε ισχύ (δεν έχει λήξει ή ανακληθεί) κατά τον χρόνο που δημιουργείται η Εγκεκριμένη Ηλεκτρονική Υπογραφή ή Ηλεκτρονική Σφραγίδα
- Κάθε αυθεντικοποίηση που πραγματοποιείται χρησιμοποιώντας το ιδιωτικό κλειδί που αντιστοιχεί σε δημόσιο κλειδί που αναφέρεται στο Πιστοποιητικό Αυθεντικοποίησης, είναι η επαλήθευση ταυτότητας του συνδρομητή και το Πιστοποιητικό Αυθεντικοποίησης έχει εγκριθεί και είναι σε ισχύ (δεν έχει λήξει ή ανακληθεί) κατά τον χρόνο που δημιουργείται η αυθεντικοποίηση
- Τα διαπιστευτήρια πρόσβασης (PIN, όνομα χρήστη, κωδικό πρόσβασης και εξουσιοδότηση μέσω εφαρμογής στο κινητό χρησιμοποιώντας κωδικό ή βιομετρικά) στο ιδιωτικό τους κλειδί προστατεύονται και ότι κανένα μη εξουσιοδοτημένο άτομο δεν έχει ποτέ πρόσβαση.
- η Εγκεκριμένη Ηλεκτρονική Υπογραφή ή Ηλεκτρονική Σφραγίδα ή Αυθεντικοποίηση δημιουργείται μόνο από τη ΕΔΔΥ
- όλες οι δηλώσεις που πραγματοποιούνται από τον Συνδρομητή ο οποίος τις έχει υποβάλλει στην Αίτηση για Πιστοποιητικό, είναι αληθείς και ο Συνδρομητής είναι ενήμερος για το γεγονός ότι η JCC Payment Systems δύναται να αρνηθεί να παράσχει την υπηρεσία εάν ο Συνδρομητής έχει σκόπιμα παρουσιάσει ψευδείς, ανακριβείς ή ελλιπείς πληροφορίες στην αίτηση για την υπηρεσία·
- ο Συνδρομητής τηρεί της απαιτήσεις που προβλέπονται από την JCC Payment Systems στην παρούσα ΠΠ, την εφαρμοστέα ΔΠΠ και τα σχετικά έγγραφα
- όλες οι πληροφορίες που παρέχονται από τον Συνδρομητή και περιλαμβάνονται στο Πιστοποιητικό είναι αληθείς και, σε περίπτωση αλλαγής στα δεδομένα που υποβλήθηκαν, ο Συνδρομητής κοινοποιεί τα ορθά δεδομένα σύμφωνα με τους κανόνες που έχουν οριστεί από την παρούσα ΠΠ, την εφαρμοστέα ΔΠΠ και τα σχετικά έγγραφα
- το Πιστοποιητικό που χρησιμοποιείται αποκλειστικά για εξουσιοδοτημένους και νόμιμους σκοπούς, συμβατούς με την παρούσα ΠΠ
- Ο Συνδρομητής δεν είναι ΑΠ και δεν χρησιμοποιεί το ιδιωτικό κλειδί που αντιστοιχεί σε οποιοδήποτε δημόσιο κλειδί που αναφέρεται στο Πιστοποιητικό, για σκοπούς ψηφιακής υπογραφής οποιουδήποτε Πιστοποιητικού (ή άλλης μορφής πιστοποιημένου δημοσίου κλειδιού) ή ΚΑΠ, όπως μια ΑΠ ή άλλως
- ο Συνδρομητής ειδοποιεί την JCC Payment Systems χωρίς καμία αδικαιολόγητη καθυστέρηση εάν το ιδιωτικό κλειδί του υποκειμένου ή ο έλεγχός του έχει απολεσθεί, κλαπεί και δυνητικά εκτεθεί σε κίνδυνο.

Οι Γενικοί Όροι και Προϋποθέσεις της JCC Payment Systems για τη χρήση των Πιστοποιητικών δύνανται να περιλαμβάνουν πρόσθετες δηλώσεις και εγγυήσεις.

9.6.4 Δηλώσεις και εγγυήσεις Βασιζόμενου Μέρους

Οι Γενικοί Όροι και Προϋποθέσεις της JCC Payment Systems για τη χρήση των Πιστοποιητικών απαιτούν τα Βασιζόμενα Μέρη να αναγνωρίσουν ότι διαθέτουν επαρκείς πληροφορίες προκειμένου να λάβουν μια τεκμηριωμένη απόφαση ως προς τον βαθμό στον οποίο επιθυμούν να βασίζονται όσον αφορά τις πληροφορίες σε ένα Πιστοποιητικό, ότι μόνο αυτά είναι αρμόδια να αποφασίσουν κατά πόσο πρόκειται να βασιστούν ή όχι στις εν λόγω πληροφορίες και ότι αναλαμβάνουν τις νομικές συνέπειες της μη τήρησης των υποχρεώσεών τους ως Βασιζόμενα Μέρη σύμφωνα με την παρούσα ΠΠ.

Οι Γενικοί Όροι και Προϋποθέσεις της JCC Payment Systems για τη χρήση των Πιστοποιητικών δύνανται να περιλαμβάνουν πρόσθετες δηλώσεις και εγγυήσεις των Βασιζόμενων Μερών.

9.6.5 Δηλώσεις και εγγυήσεις άλλων συμμετεχόντων

Καμία διατύπωση.

9.7 *Δηλώσεις αποποίησης ευθύνης εγγυήσεων*

Στον βαθμό που επιτρέπεται από την ισχύουσα νομοθεσία, οι Γενικοί Όροι και Προϋποθέσεις για τη Χρήση Πιστοποιητικών, η JCC Payment Systems αποποιείται πιθανές εγγυήσεις, συμπεριλαμβανομένης οποιασδήποτε εγγύησης ως προς την εμπορευσιμότητα ή την καταλληλότητα για έναν συγκεκριμένο σκοπό.

JCC Payment Systems δεν φέρει ευθύνη για τα εξής:

- το απόρρητο των διαπιστευτηρίων πρόσβασης (PIN, όνομα χρήστη, κωδικός πρόσβασης και εξουσιοδότηση μέσω εφαρμογής στο κινητό χρησιμοποιώντας κωδικό ή βιομετρικά) στα ιδιωτικά κλειδιά των Συνδρομητών, την πιθανή εσφαλμένη χρήση των πιστοποιητικών ή των ανεπαρκών ελέγχων των πιστοποιητικών ή για τις εσφαλμένες αποφάσεις ενός Βασιζόμενου Μέρους ή οποιαδήποτε συνέπεια λόγω σφαλμάτων ή παραλείψεων στους ελέγχους επικύρωσης της Υπηρεσίας Εμπιστοσύνης·
- τη μη τήρηση των υποχρεώσεών της, εάν η εν λόγω μη τήρηση οφείλεται σε σφάλματα ή προβλήματα ασφαλείας του Εποπτικού Φορέα, την εποπτική αρχή προστασίας δεδομένων, τον Κατάλογο Εμπιστοσύνης ή οποιαδήποτε άλλη δημόσια αρχή·
- τη μη τήρηση των υποχρεώσεων που απορρέουν από την παρούσα ΠΠ, την εφαρμοστέα ΔΠΠ και τα σχετικά έγγραφα, εάν η εν λόγω μη τήρηση προκύπτει λόγω Ανωτέρας Βίας.

9.8 *Περιορισμοί Ευθύνης*

Οι Γενικοί Όροι και Προϋποθέσεις της JCC Payment Systems για τη Χρήση Πιστοποιητικών περιορίζουν την ευθύνη της JCC Payment Systems. Οι περιορισμοί ευθύνης περιλαμβάνουν τον αποκλεισμό έμμεσων, εξαιρετικών, τυχαίων και συνεπαγόμενων ζημιών. Περιλαμβάνουν επίσης ανώτατο όριο ευθύνης ύψους χιλίων ευρώ (1.000,00 €), το οποίο περιορίζει την αποζημίωση της JCC Payment Systems αναφορικά με ένα Πιστοποιητικό .

Η ευθύνη (και/ή ο περιορισμός αυτής) των Συνδρομητών και των Βασιζόμενων Μερών είναι όπως ορίζεται στους ισχύοντες Γενικούς Όρους και Προϋποθέσεις για τη χρήση των Πιστοποιητικών .

9.9 *Αποζημιώσεις*

9.9.1 Αποζημίωση από πλευράς Συνδρομητών

Στον βαθμό που το επιτρέπει η ισχύουσα νομοθεσία, οι Συνδρομητές υποχρεούνται να αποζημιώσουν την JCC Payment Systems για τα εξής:

- ανακρίβειες ή ψευδείς δηλώσεις στοιχείων από τον Συνδρομητή στην Αίτηση του για Πιστοποιητικό·
- αποτυχία του Συνδρομητή να γνωστοποιήσει κάποιο ουσιώδες στοιχείο στην Αίτηση για Πιστοποιητικό, εφόσον η ψευδής δήλωση ή η παράλειψη έγινε από αμέλεια ή με πρόθεση να εξαπατήσει οποιοδήποτε μέρος·
- αποτυχία του Συνδρομητή να προστατεύσει το ιδιωτικό του κλειδί, να χρησιμοποιήσει ένα Αξιόπιστο Σύστημα ή άλλως να λάβει απαραίτητα προληπτικά μέτρα προκειμένου να αποτραπεί η έκθεση σε κίνδυνο, η απώλεια, η αποκάλυψη, η τροποποίηση ή η μη εξουσιοδοτημένη χρήση του ιδιωτικού κλειδιού του Συνδρομητή ή για
- χρήση ονόματος από τον Συνδρομητή (συμπεριλαμβανομένων ενδεικτικά του κοινού ονόματος, ονόματος τομέα ή διεύθυνσης ηλεκτρονικού ταχυδρομείου) που παραβιάζει τα Δικαιώματα περί Πνευματικής Ιδιοκτησίας οποιουδήποτε τρίτου μέρους.

Οι Γενικοί Όροι και Προϋποθέσεις της για τη χρήση των Πιστοποιητικών δύνανται να περιλαμβάνουν πρόσθετες υποχρεώσεις σχετικά με την αποζημίωση.

9.9.2 Αποζημίωση από πλευράς βασιζόμενων μερών

Στον βαθμό που το επιτρέπει η ισχύουσα νομοθεσία, οι Γενικοί Όροι και Προϋποθέσεις της JCC Payment Systems για τη χρήση εγκεκριμένων πιστοποιητικών υποχρεώνουν τα Βασιζόμενα Μέρη να αποζημιώνουν την JCC Payment Systems για τα εξής:

- αποτυχία του Βασιζόμενου Μέρους να εκτελεί τις υποχρεώσεις του ως Βασιζόμενο Μέρος·
- στήριξη του Βασιζόμενου Μέρους σε Πιστοποιητικό που δεν είναι εύλογο σύμφωνα με τις περιστάσεις ή
- αποτυχία του Βασιζόμενου Μέρους να ελέγξει την κατάσταση του σχετικού Πιστοποιητικού ώστε να προσδιορίσει εάν το Πιστοποιητικό έχει λήξει ή ανακληθεί.

Οι Γενικοί Όροι και Προϋποθέσεις της για τη χρήση των Πιστοποιητικών δύνανται να περιλαμβάνουν πρόσθετες υποχρεώσεις σχετικά με την αποζημίωση.

9.10 *Διάρκεια και λήξη ισχύος*

9.10.1 Διάρκεια ισχύος

Η ΠΠ τίθεται σε ισχύ τουλάχιστον 30 ημέρες μετά τη δημοσίευσή της στον χώρο αποθήκευσης της JCC Payment Systems.

9.10.2 Λήξη ισχύος

Η παρούσα ΠΠ, όπως, κατά διαστήματα, έχει τροποποιηθεί, παραμένει σε ισχύ έως ότου αντικατασταθεί με μια νέα έκδοση.

9.10.3 Συνέπειες Λήξης και Διατήρηση ισχύος όρων

Με τη λήξη ισχύος της παρούσας ΠΠ, οι Συμμετέχοντες στον Υποτομέα της JCC Payment Systems εξακολουθούν εντούτοις να δεσμεύονται από τους όρους της όσον αφορά όλα τα πιστοποιητικά που εκδόθηκαν για το υπόλοιπο των περιόδων ισχύος των σχετικών πιστοποιητικών.

9.11 *Ατομικές ειδοποιήσεις και κοινοποιήσεις με συμμετέχοντες*

Έκτος αν η συμφωνία μεταξύ των μερών ορίζει διαφορετικά, οι Συμμετέχοντες στον Υποτομέα της JCC Payment Systems οφείλουν να χρησιμοποιούν εμπορικά εύλογες μεθόδους για την μεταξύ τους επικοινωνία, λαμβάνοντας υπόψη την κρισιμότητα και το αντικείμενο της επικοινωνίας.

Η παράγραφος 1.5.1 παρέχει όλους τους διαθέσιμους τρόπους επικοινωνίας.

9.12 *Τροποποιήσεις*

9.12.1 Διαδικασία τροποποίησης

Τροποποιήσεις της παρούσας ΔΠΠ πραγματοποιούνται από τον Υπεύθυνο Πολιτικής ΥΔΚ της JCC Payment Systems. Οι τροποποιήσεις είναι είτε υπό μορφή εγγράφου που περιέχει την τροποποιημένη μορφή της ΠΠ είτε με τη μορφή ενημέρωσης. Οι τροποποιημένες εκδόσεις ή ενημερώσεις είναι συνδεδεμένες με τον Χώρο Αποθήκευσης της JCC Payment Systems στη διεύθυνση: https://pki.jcc.com.cy/repository. Οι νέες ενημερωμένες εκδόσεις υπερισχύουν έναντι οποιωνδήποτε καθορισμένων ή συγκρουόμενων διατάξεων της αναφερόμενης έκδοσης της ΠΠ. Ο Υπεύθυνος Πολιτικής ΥΔΚ προσδιορίζει εάν οι αλλαγές στην ΠΠ απαιτούν ή όχι αλλαγές στα αναγνωριστικά αντικειμένου των πολιτικών Πιστοποιητικού.

9.12.2 Μηχανισμός και χρονική περίοδος ειδοποίησης

Ο Υπεύθυνος Πολιτικής ΥΔΚ της JCC Payment Systems διατηρεί το δικαίωμα να τροποποιήσει την παρούσα ΠΠ χωρίς ειδοποίηση, για επουσιώδεις αλλαγές, συμπεριλαμβανομένων, ενδεικτικά, των διορθώσεων τυπογραφικών λαθών και των αλλαγών των δικτυακών κόμβων (URL) ή των αλλαγών στα στοιχεία επικοινωνίας. Ο χαρακτηρισμός των τροποποιήσεων ως ουσιωδών ή επουσιωδών εναπόκειται στην αποκλειστική διακριτική ευχέρεια του Υπεύθυνου Πολιτικής ΥΔΚ της JCC Payment Systems.

Οι προτεινόμενες τροποποιήσεις στην ΠΠ είναι συνδεδεμένες με τον Χώρο Αποθήκευσης της JCC Payment Systems στη διεύθυνση: https://pki.jcc.com.cy/repository.

Έκτος αν ορίζεται διαφορετικά στην παρούσα ΠΠ, εάν ο Υπεύθυνος Πολιτικής ΥΔΚ της JCC Payment Systems θεωρεί ότι ουσιώδεις τροποποιήσεις στην παρούσα ΠΠ είναι άμεσα απαραίτητες, προκειμένου να διακοπεί ή να προληφθεί μία παραβίαση της ασφάλειας του ΠΥΕ ή οποιουδήποτε τμήματός του, η Διεύθυνση της JCC Payment Systems δικαιούται να προχωρήσει στις συγκεκριμένες τροποποιήσεις προβαίνοντας στη δημοσίευσή τους στον Αποθηκευτικό χώρο της JCC Payment Systems. Οι εν λόγω τροποποιήσεις θα τεθούν αμέσως σε ισχύ με τη δημοσίευσή τους. Μέσα σε εύλογο χρονικό διάστημα μετά τη δημοσίευση, η JCC Payment Systems ειδοποιεί σχετικά με τις εν λόγω τροποποιήσεις στους Συμμετέχοντες στον Υποτομέα της JCC Payment Systems.
Τουλάχιστον, η Διεύθυνση της JCC Payment Systems και ο Υπεύθυνος Πολιτικής ΥΔΚ θα ενημερώνουν την παρούσα ΠΠ σε ετήσια βάση σύμφωνα με τις κατευθυντήριες οδηγίες της ΑΠ/ του Φόρουμ Φυλλομετρητών.

Οι τροποποιήσεις που δεν αλλάζουν τη σημασία της παρούσας ΠΠ, όπως τυπογραφικές διορθώσεις, μεταφραστικές ενέργειες και ενημερώσεις των στοιχείων επικοινωνίας, τεκμηριώνονται στην ενότητα «Εκδόσεις και Αλλαγές» του παρόντος εγγράφου. Στην περίπτωση αυτή, το διαχωρισμένο τμήμα του εγγράφου, ο αριθμός έκδοσης μεγεθύνεται.

Σε περίπτωση σημαντικών αλλαγών, η νέα έκδοση της ΠΠ είναι σαφώς διακριτή από τις προηγούμενες και ο αριθμός σειράς μεγεθύνεται κατά ένα.

9.12.3 Συνθήκες υπό τις οποίες επιβάλλεται τροποποίηση του αναγνωριστικού αντικειμένου (OID)

Εάν ο Υπεύθυνος Πολιτικής ΥΔΚ, αποφασίσει ότι είναι απαραίτητη κάποια αλλαγή στο αναγνωριστικό αντικειμένου που αντιστοιχεί στην Πολιτική Πιστοποιητικού, η αλλαγή αυτή θα περιλαμβάνει νέα αναγνωριστικά αντικειμένου για τις Πολιτικές Πιστοποιητικών. Διαφορετικά, οι τροποποιήσεις δεν θα πρέπει να απαιτούν αλλαγή στο αναγνωριστικό αντικειμένου της Πολιτικής Πιστοποιητικού.

9.13 *Διατάξεις περί επίλυσης διαφορών*

9.13.1 Διαφορές μεταξύ της JCC, των συνδεδεμένων εταιρειών και των πελατών

Οι διαφορές ανάμεσα στους Συμμετέχοντες στον Υποτομέα της JCC Payment Systems επιλύονται σύμφωνα με τους διατάξεις των εφαρμοστέων συμβάσεων που έχουν συναφθεί μεταξύ των μερών.

9.13.2 Διαφορές με Συνδρομητές ή Βασιζόμενα Μέρη

Οι Γενικοί Όροι και Προϋποθέσεις της JCC Payment Systems για τη Χρήση Πιστοποιητικών περιλαμβάνουν ρήτρα για την επίλυση διαφορών. Οι διαφορές που αφορούν την JCC Payment Systems απαιτούν αρχική περίοδο διαπραγμάτευσης εξήντα (60) ημερών που θα ακολουθείται από δικαστική διαδικασία στα δικαστήρια της Κύπρου.

9.14 *Εφαρμοστέο δίκαιο*

Η εκτελεστότητα, η δομή, η ερμηνεία και η εγκυρότητα της παρούσας ΠΠ διέπεται από το κυπριακό δίκαιο, χωρίς να λαμβάνονται υπόψη συμβάσεις ή άλλες επιλογές διατάξεων δικαίου και χωρίς την απαίτηση θεμελίωσης εμπορικού δεσμού με την Κύπρο. Η ανωτέρω επιλογή του εφαρμοστέου δικαίου στοχεύει στη διασφάλιση ομοιόμορφων διαδικασιών και ερμηνείας για το σύνολο των Συμμετεχόντων στον Υποτομέα της JCC Payment Systems, ανεξάρτητα από την εγκατάστασή τους.

Η παρούσα διάταξη περί εφαρμοστέου δικαίου ισχύει μόνο για την παρούσα ΠΠ. Οι Συμβάσεις που ενσωματώνουν τη ΠΠ με παραπομπή, δύνανται να περιέχουν διαφορετικές διατάξεις περί εφαρμοστέου δικαίου, υπό την προϋπόθεση ότι η παρούσα διάταξη της ενότητας 9.14 διέπει την εκτελεστότητα, δομή, ερμηνεία και την εγκυρότητα των όρων της ΠΠ, ανεξάρτητα από τις λοιπές διατάξεις οποιωνδήποτε σχετικών συμβάσεων που υπόκεινται σε οποιονδήποτε περιορισμό προβλεπόμενο από την ισχύουσα νομοθεσία.

9.15 *Συμμόρφωση με την ισχύουσα νομοθεσία*

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

- του eIDAS - Κανονισμού (ΕΕ) 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ·
- Νομοθεσία και Διατάγματα για την Εθνική Ηλεκτρονική Ταυτότητα της Κύπρου
- των Κανονισμών της ΕΕ και νόμων περί προσωπικών δεδομένων, όπως η Νομοθεσία (ΕΕ) 2016/679 (GDPR)·
- των σχετικών Ευρωπαϊκών Προτύπων:
    a. ETSI EN 319 401 Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) – Απαιτήσεις γενικής πολιτικής για παρόχους υπηρεσιών εμπιστοσύνης·
    b. ETSI EN 319 411-1 Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) – Απαιτήσεις πολιτικής και ασφάλειας για παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν πιστοποιητικά, Μέρος 1: Γενικές Απαιτήσεις·
    c. ETSI EN 319 411-2 Ηλεκτρονικές Υπογραφές και Υποδομές (ESI) – Απαιτήσεις πολιτικής και ασφάλειας για παρόχους υπηρεσιών εμπιστοσύνης που εκδίδουν πιστοποιητικά, Μέρος 2: Απαιτήσεις πολιτικής για αρχές πιστοποίησης που εκδίδουν εγκεκριμένα πιστοποιητικά·

9.16 *Λοιπές διατάξεις*

9.16.1 Σύνολο σύμβασης

Δεν εφαρμόζεται.

9.16.2 Εκχώρηση

Οποιαδήποτε οντότητα που δραστηριοποιείται δυνάμει της παρούσας ΠΠ δεν δύνανται να εκχωρήσει τα δικαιώματα ή τις υποχρεώσεις της χωρίς την πρότερη έγγραφη συγκατάθεση της JCC Payment Systems. Εκτός εάν άλλως ορίζεται σε σύμβαση με ένα μέρος, η JCC Payment Systems δεν κοινοποιεί την εκχώρηση.

9.16.3 Διαιρετότητα

Σε περίπτωση που ένα άρθρο ή μια διάταξη της παρούσας ΠΠ κριθεί μη εκτελεστέο από δικαστήριο ή άλλη δικαστική αρχή, το υπόλοιπο της ΠΠ παραμένει σε ισχύ.

9.16.4 Εφαρμογή (Αμοιβές δικηγόρων και Παραίτηση από δικαιώματα)

Η JCC Payment Systems δύναται να απαιτήσει αποζημίωση και αμοιβές δικηγόρων από ένα μέρος για ζημίες, απώλειες και έξοδα που σχετίζονται με τη συμπεριφορά του εν λόγω μέρους. Η αδυναμία της JCC Payment Systems να εφαρμόσει μια διάταξη της παρούσας ΠΠ δεν αποτελεί παραίτηση της JCC Payment Systems από το δικαίωμά της να εφαρμόσει την ίδια διάταξη αργότερα ή το δικαίωμά της να εφαρμόσει μια οποιαδήποτε άλλη διάταξη της παρούσας ΠΠ. Για να τεθεί σε ισχύ, η παραίτηση από δικαίωμα πρέπει να πραγματοποιείται εγγράφως και να υπογράφεται από την JCC Payment Systems.

9.16.5 Ανωτέρα βία

Η μη τήρηση των υποχρεώσεων που απορρέουν από την παρούσα ΠΠ και/ή τα σχετικά έγγραφα δεν θεωρείται παράβαση, εάν η εν λόγω μη τήρηση προκύπτει λόγω Ανωτέρας Βίας. Κανένα από τα μέρη εγείρει απαιτήσεις έναντι ζημίας ή οποιαδήποτε άλλης αποζημίωσης από τα έτερα μέρη για καθυστερήσεις και/ή τη μη τήρηση της παρούσας ΠΠ και/ή των σχετικών εγγράφων λόγω Ανωτέρας Βίας.

9.17 *Άλλες διατάξεις*

Η JCC Payment Systems ενσωματώνουν με παραπομπή, μέσω των Πιστοποιητικών της ΑΠ, την αντίστοιχη ΔΠΠ και τους Γενικούς Όρους και Προϋποθέσεις που ισχύουν για κάθε Πιστοποιητικό που εκδίδουν. Αυτή η ενσωμάτωση μέσω αναφοράς περιγράφεται περαιτέρω στο σχετικό προφίλ πιστοποιητικού της ΑΠ.

Παράρτημα Α. Πίνακας ακρωνυμίων και ορισμών

Πίνακας ακρωνυμίων

Διάρκεια ισχύος	Ορισμός
ΑΕ	Αρχή Εγγραφής
ΑΠ	Αρχή Πιστοποίησης
ΠΠ	Πολιτική Πιστοποιητικού
ΔΠΠ	Δήλωση Πρακτικών Πιστοποίησης
ΚΑΠ	Κατάλογοι Ανακληθέντων Πιστοποιητικών
ΑΥΠ	Αίτημα Υπογραφής Πιστοποιητικού
FIPS	Ομοσπονδιακά Πρότυπα Επεξεργασίας Πληροφοριών των Ηνωμένων Πολιτειών
ΤΑΕ	Τοπική Αρχή Εγγραφής
NCP	Κανονικοποιημένη Πολιτική Πιστοποιητικού
NCP+	Εκτεταμένη Κανονικοποιημένη Πολιτική Πιστοποιητικού
OCSP	Πρωτόκολλο κατάστασης πιστοποιητικού μέσω σύνδεσης
OID	Αναγνωριστικό αντικειμένου, μοναδικός κωδικός αναγνώρισης αντικειμένου
ΠΑΠ	Πρωτεύουσα Αρχή Πιστοποίησης
PDS	Γνωστοποίηση ΥΔΚ
PIN	Προσωπικός αναγνωριστικός αριθμός
PKCS	Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού
ΥΔΚ	Υποδομή Δημόσιου Κλειδιού
ΕΔΔΥ	Εγκεκριμένες Διατάξεις Δημιουργίας Ηλεκτρονικής Υπογραφής/ Σφραγίδας
ΑΕ	Αρχή Εγγραφής
RFC	Αίτηση για σχολιασμό
SSL	Επίπεδο Ασφαλών Συνδέσεων
ΠΥΕ	Πάροχος Υπηρεσίας Εμπιστοσύνης

Ορισμοί

Διάρκεια ισχύος	Ορισμός
Αποθηκευτικός χώρος της JCC Payment Systems	Η βάση δεδομένων της JCC Payment Systems όσον αφορά τα Πιστοποιητικά και άλλες σχετικές πληροφορίες της JCC Payment Systems που είναι προσβάσιμες διαδικτυακά (online).
Διαχειριστής	Πρόκειται για ένα Έμπιστο Πρόσωπο εντός του οργανισμού που πραγματοποιεί την επικύρωση και άλλες λειτουργίες της ΑΠ ή της ΑΕ.
Πιστοποιητικό Διαχειριστή	Πρόκειται για ένα Πιστοποιητικό που εκδίδεται σε έναν Διαχειριστή το οποίο μπορεί να χρησιμοποιηθεί μόνο για την εκτέλεση των λειτουργιών της ΑΠ ή της ΑΕ.
Προηγμένη ηλεκτρονική σφραγίδα	Μια προηγμένη ηλεκτρονική σφραγίδα πληροί τις ακόλουθες απαιτήσεις: • συνδέεται κατά τρόπο μοναδικό με τον δημιουργό της σφραγίδας· • είναι ικανή να ταυτοποιεί τον δημιουργό της σφραγίδας· • δημιουργείται χρησιμοποιώντας δεδομένα δημιουργίας ηλεκτρονικής σφραγίδας που ο δημιουργός της σφραγίδας μπορεί, με υψηλό επίπεδο εμπιστοσύνης υπό τον έλεγχό του, να χρησιμοποιήσει για τη δημιουργία της ηλεκτρονικής σφραγίδας· και • συνδέεται με τα δεδομένα στα οποία αναφέρεται με τέτοιο τρόπο ώστε οποιαδήποτε επακόλουθη αλλαγή στα δεδομένα να είναι ανιχνεύσιμη.
Προηγμένη ηλεκτρονική υπογραφή	Μια προηγμένη ηλεκτρονική υπογραφή πληροί τις ακόλουθες απαιτήσεις: • συνδέεται κατά τρόπο μοναδικό με τον υπογράφοντα· • είναι ικανή να ταυτοποιεί τον υπογράφοντα· • δημιουργείται με δεδομένα δημιουργίας ηλεκτρονικής υπογραφής τα οποία ο υπογράφων μπορεί, με υψηλό βαθμό εμπιστοσύνης, να χρησιμοποιεί υπό τον αποκλειστικό του έλεγχο, και

Διάρκεια ισχύος	Ορισμός
	• συνδέεται με τα δεδομένα που έχουν υπογραφεί σε σχέση με αυτήν κατά τρόπο ώστε να μπορεί να ανιχνευθεί οποιαδήποτε επακόλουθη τροποποίηση των εν λόγω δεδομένων.
Επαλήθευση Ταυτότητας/Αυθεντικοποίηση	Μοναδική ταυτοποίηση ενός φυσικού προσώπου με έλεγχο της ισχυριζόμενης ταυτότητάς του
Πιστοποιητικό Αυθεντικοποίησης	Ένα πιστοποιητικό που έχει σκοπό να χρησιμοποιηθεί για αυθεντικοποίηση
Πιστοποιητικό	Πρόκειται για το δημόσιο κλειδί ενός χρήστη μαζί με ορισμένες άλλες πληροφορίες οι οποίες παραδίδονται μη παραποιημένες βάσει κρυπτογράφησης με το ιδιωτικό κλειδί της αρχής πιστοποίησης που το εξέδωσε.
Αιτών Πιστοποιητικό	Το φυσικό πρόσωπο ή ένας οργανισμός που ζητά την έκδοση Πιστοποιητικού από μια ΑΠ.
Αίτηση για Πιστοποιητικό	Το αίτημα από τον Αιτούντα για Πιστοποιητικό προς μια ΑΠ για την έκδοση ενός Πιστοποιητικού.
Αλυσίδα πιστοποιητικού	Ο κατάλογος κατά σειρά κατάταξης των Πιστοποιητικών που περιλαμβάνει ένα Πιστοποιητικό Συνδρομητή, Πιστοποιητικά της ΑΠ και καταλήγει σε ένα Πιστοποιητικό Βάσης (Root).
Πολιτική Πιστοποιητικού (ΠΠ)	Κατονομαζόμενο σύνολο κανόνων που υποδεικνύει την εφαρμοσιμότητα ενός πιστοποιητικού σε μια συγκεκριμένη κοινότητα και/ή κατηγορία εφαρμογής με κοινές απαιτήσεις για την ασφάλεια.
Κατάλογοι Ανακληθέντων Πιστοποιητικών (ΚΑΠ)	Ο υπογεγραμμένος κατάλογος που αναφέρει ένα σύνολο πιστοποιητικών που δεν θεωρούνται πλέον έγκυρα από τον εκδότη πιστοποιητικών.
Αίτημα Υπογραφής Πιστοποιητικού (ΑΥΠ)	Μήνυμα που μεταφέρει αίτημα για έκδοση Πιστοποιητικού.
Αρχή Πιστοποίησης (ΑΠ)	Ο οντότητα που έχει εξουσιοδοτηθεί να δημιουργήσει και να αναθέτει πιστοποιητικά.
Δήλωση Πρακτικών Πιστοποίησης (ΔΠΠ)	Δήλωση των πρακτικών τις οποίες εφαρμόζει μια Αρχή Πιστοποίησης κατά την έκδοση, τη διαχείριση, την ανάκληση, την ανανέωση ή την επαναδημιουργία κλειδιών πιστοποιητικών.
Συνθηματική φράση	Η μυστική φράση που επιλέγει ο Αιτών Πιστοποιητικό κατά την εγγραφή για ένα Πιστοποιητικό. Κατά την έκδοση του Πιστοποιητικού, ο Αιτών Πιστοποιητικό καθίσταται Συνδρομητής και η ΑΠ ή η ΑΕ μπορεί να χρησιμοποιήσει τη Συνθηματική Φράση για την επαλήθευση της ταυτότητας του Συνδρομητή όταν αυτός ζητά την ανάκληση ή την ανανέωση του Πιστοποιητικού του.
Έλεγχος συμμόρφωσης	Ο περιοδικός έλεγχος στον οποίο υποβάλλεται ένα Κέντρο Επεξεργασίας, το Κέντρο Υπηρεσιών ή Πελάτης της υπηρεσίας Managed PKI ώστε να προσδιοριστεί η συμμόρφωσή του με τα Πρότυπα που ισχύουν αντίστοιχα για τα ανωτέρω.
Έκθεση σε κίνδυνο	Η παραβίαση (ή υποτιθέμενη παραβίαση) μιας πολιτικής ασφαλείας, κατά την οποία μπορεί να έχει συμβεί μη εξουσιοδοτημένη αποκάλυψη ή απώλεια του ελέγχου επί διαβαθμισμένων πληροφοριών. Όσον αφορά τα ιδιωτικά κλειδιά, η Έκθεση σε Κίνδυνο αποτελεί η απώλεια, η κλοπή, η γνωστοποίηση, η τροποποίηση, η μη εξουσιοδοτημένη χρήση ή κάθε άλλη έκθεση της ασφάλειας του ιδιωτικού αυτού κλειδιού σε κίνδυνο.
Όνομα Τομέα	Η ετικέτα που αποδίδεται σε έναν κόμβο στο Σύστημα Ονομάτων Τομέα (Domain Name System - DNS).
Κανονισμός eIDAS	Κανονισμός (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές στην εσωτερική αγορά και την κατάργηση της οδηγίας 1999/93/ΕΚ.
Ηλεκτρονική υπογραφή	Δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε ή συσχετίζονται λογικά με άλλα ηλεκτρονικά δεδομένα και τα οποία χρησιμοποιούνται από τον υπογράφοντα για να υπογράφει.
Ηλεκτρονική σφραγίδα	Δεδομένα σε ηλεκτρονική μορφή τα οποία είναι συνημμένα σε ή συσχετίζονται λογικά με άλλα δεδομένα σε ηλεκτρονική μορφή, με σκοπό τη διασφάλιση της προέλευσης και της ακεραιότητάς τους.

Διάρκεια ισχύος	Ορισμός
Δικαιώματα Πνευματικής Ιδιοκτησίας	Δικαιώματα επί ενός ή περισσοτέρων από τα ακόλουθα: οποιοδήποτε δικαίωμα δημιουργού, δίπλωμα ευρεσιτεχνίας, εμπορικό μυστικό, εμπορικό σήμα, καθώς και κάθε άλλο δικαίωμα πνευματικής ιδιοκτησίας.
Ενδιάμεση Αρχή Πιστοποίησης (Ενδιάμεση ΑΠ)	Η Αρχή Πιστοποίησης της οποίας το Πιστοποιητικό βρίσκεται εντός της Αλυσίδας Πιστοποιητικών μεταξύ του Πιστοποιητικού της ΑΠ Βάσης (Root) και του Πιστοποιητικού της Αρχής Πιστοποίησης που εξέδωσε το Πιστοποιητικό Συνδρομητή τελικού χρήστη.
Διαδικασία Παραγωγής Κλειδιών	Μια διαδικασία δια της οποίας παράγεται το ζεύγος κλειδιών μιας ΑΠ ή μιας ΑΕ, το ιδιωτικό κλειδί της μεταφέρεται σε μια κρυπτογραφική μονάδα, παράγεται εφεδρικό αντίγραφο του ιδιωτικού της κλειδιού και/ή πιστοποιείται το δημόσιο κλειδί της.
Τοπική ΕΔΔΥ	Εγκεκριμένη διάταξη τύπου USB (token) ή έξυπνης κάρτας
Μη αυτόματη επαλήθευση ταυτότητας	Διαδικασία με την οποία οι Αιτήσεις για Πιστοποιητικό ελέγχονται και εγκρίνονται με μη αυτόματο τρόπο (manually), μία προς μία, από έναν Διαχειριστή που χρησιμοποιεί διεπαφή που βασίζεται στο Web.
Μη αποκήρυξη	Το χαρακτηριστικό μιας επικοινωνίας που παρέχει προστασία έναντι ενός μέρους που συμμετέχει στην επικοινωνία και το οποίο αρνείται ψευδώς για την προέλευσή της, αρνείται ότι υποβλήθηκε ή επιδόθηκε. Η άρνηση της προέλευσης περιλαμβάνει την άρνηση ότι η επικοινωνία προερχόταν από την ίδια πηγή στα πλαίσια μιας σειράς ενός ή περισσοτέρων προγενέστερων μηνυμάτων, ακόμα και αν η ταυτότητα που σχετίζεται με τον αποστολέα είναι άγνωστη. Σημείωση: μόνο η απόφαση δικαστηρίου, οργάνου διαιτησίας ή άλλου δικαστικού σώματος μπορεί να αποτρέψει τελικώς την αποκήρυξη. Για παράδειγμα, μια ψηφιακή υπογραφή που επαληθεύεται κατ' αναφορά σε ένα Πιστοποιητικό του STN μπορεί να αποτελεί αποδεικτικό στοιχείο προς υποστήριξη δικαστικής απόφασης περί μη αποκήρυξης, ενώ η ίδια δεν συνιστά από μόνη της μη αποκήρυξη.
ΑΠ εκτός σύνδεσης (offline)	Οι εκδότριες ΑΠ Βάσης ΠΑΠ της Symantec και άλλες καθορισμένης ενδιάμεσες ΑΠ διατηρούνται εκτός σύνδεσης για λόγους ασφάλειας προκειμένου να προστατευθούν έναντι πιθανών επιθέσεων από εισβολείς μέσω του δικτύου. Οι εν λόγω ΑΠ δεν υπογράφουν απευθείας τα Πιστοποιητικά Συνδρομητών τελικού χρήστη.
ΑΠ σε σύνδεση (online)	Οι ΑΠ που υπογράφουν Πιστοποιητικά Συνδρομητών τελικού χρήστη διατηρούνται σε σύνδεση προκειμένου να παρέχουν συνέχεια υπηρεσίες υπογραφής.
Πρωτόκολλο κατάστασης πιστοποιητικού μέσω σύνδεσης (OCSP)	Το πρωτόκολλο που χρησιμοποιείται για να παρέχει στα Βασιζόμενα Μέρη πληροφορίες σε πραγματικό χρόνο σχετικά με την κατάσταση των Πιστοποιητικών.
OTP	Κωδικός μιας χρήσης
Λειτουργική περίοδος	Το χρονικό διάστημα το οποίο ξεκινά την ημερομηνία και τον χρόνο έκδοσης ενός Πιστοποιητικού (ή σε μεταγενέστερη καθορισμένη ημερομηνία και χρόνο εάν δηλώνεται στο Πιστοποιητικό) και τερματίζει με την ημερομηνία και τον χρόνο κατά τον οποίο λήγει ή πρόωρα ανακαλείται το Πιστοποιητικό.
PKCS #10	Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού (Public−Key Cryptography Standard) #10 που έχει αναπτυχθεί από την RSA Security Inc. και το οποίο καθορίζει τη δομή του Αιτήματος Υπογραφής Πιστοποιητικού.
PKCS #12	Πρότυπο Κρυπτογραφίας Δημόσιου Κλειδιού (Public−Key Cryptography Standard) #12 που έχει αναπτυχθεί από την RSA Security Inc. και το οποίο καθορίζει το ασφαλές μέσο για τη μεταβίβαση των ιδιωτικών κλειδιών.
Ιδιωτικό Κλειδί	Το κλειδί ενός ζεύγους κλειδιών το οποίο διατηρείται κρυφό από τον κάτοχο του ζεύγους κλειδιών και το οποίο χρησιμοποιείται για τη εγκεκριμένων πιστοποιητικών ή για την αποκρυπτογράφηση ηλεκτρονικών αρχείων ή φακέλων που έχουν κρυπτογραφηθεί με το αντίστοιχο δημόσιο κλειδί.
Πρωτεύουσα Αρχή Πιστοποίησης ΠΑΠ)	Μια ΑΠ που ενεργεί ως ΑΠ Βάσης (Root) και εκδίδει Πιστοποιητικά σε ΑΠ που είναι ιεραρχικά υφιστάμενές της.
Κέντρο Επεξεργασίας	Η χώρος της JCC Payment Systems που δημιουργεί μια ασφαλή εγκατάσταση που στεγάζει, μεταξύ άλλων, τις κρυπτογραφικές μονάδες που χρησιμοποιούνται για την έκδοση των Πιστοποιητικών.
Δημόσιο Κλειδί	Το κλειδί ενός ζεύγους κλειδιών που μπορεί να δημοσιοποιηθεί από τον κάτοχο του αντίστοιχου ιδιωτικού κλειδιού και το οποίο χρησιμοποιείται από

Διάρκεια ισχύος	Ορισμός
	Βασιζόμενο Μέρος για την επαλήθευση ενός εγκεκριμένου πιστοποιητικού που έχει δημιουργηθεί με το αντίστοιχο ιδιωτικό κλειδί του κατόχου και/ή για την κρυπτογράφηση μηνυμάτων ώστε να μπορούν να αποκρυπτογραφηθούν μόνο με το αντίστοιχο ιδιωτικό κλειδί του κατόχου.
Υποδομή Δημόσιου Κλειδιού (ΥΔΚ)	Η αρχιτεκτονική, η οργανωτική δομή, οι τεχνικές, οι κανονισμοί, και οι διαδικασίες που στο σύνολό τους υποστηρίζουν την εφαρμογή και τη λειτουργία του κρυπτογραφικού συστήματος δημοσίου κλειδιού που βασίζεται σε Πιστοποιητικό. Η ΥΔΚ της JCC Payment Systems αποτελείται από συστήματα που συνεργάζονται για την παροχή και την υλοποίηση της ΥΔΚ της JCC Payment Systems.
Υπεύθυνος Πολιτικής (ΥΔΚ)	Ο οργανισμός εντός της JCC Payment Systems που είναι υπεύθυνος για την έκδοση της παρούσας πολιτικής.
Εγκεκριμένη ηλεκτρονική σφραγίδα	Πρόκειται για μια προηγμένη ηλεκτρονική σφραγίδα που δημιουργείται από εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής σφραγίδας και βασίζεται σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής σφραγίδας.
Εγκεκριμένη ηλεκτρονική υπογραφή	Πρόκειται για μια προηγμένη ηλεκτρονική υπογραφή που δημιουργείται από εγκεκριμένη διάταξη δημιουργίας ηλεκτρονικής υπογραφής και βασίζεται σε εγκεκριμένο πιστοποιητικό ηλεκτρονικής υπογραφής.
Εγκεκριμένο Πιστοποιητικό	Το Εγκεκριμένο Πιστοποιητικό είναι ένα Πιστοποιητικό που εκδίδεται από μια ΑΠ και το οποίο έχει διαπιστευτεί και εποπτεύεται από αρχές που ορίζονται από κράτος μέλος της ΕΕ και πληροί τις απαιτήσεις του κανονισμού eIDAS.
Εγκεκριμένη διάταξη δημιουργίας υπογραφής (ΕΔΔΥ)	Διάταξη που είναι υπεύθυνη για την έγκριση ψηφιακών υπογραφών με τη χρήση ειδικού υλικού και λογισμικού που διασφαλίζει ότι μόνο ο υπογράφων έχει τον έλεγχο του ιδιωτικού του κλειδιού. Οι εγκεκριμένες διατάξεις δημιουργίας ηλεκτρονικής υπογραφής ή σφραγίδας πληρούν τις απαιτήσεις του κανονισμού eIDAS.
Εγκεκριμένος πάροχος υπηρεσιών εμπιστοσύνης	Ο πάροχος υπηρεσιών εμπιστοσύνης ο οποίος παρέχει μία ή περισσότερες εγκεκριμένες υπηρεσίες εμπιστοσύνης και έχει αναγνωριστεί ως τέτοιος από τον Εποπτικό Φορέα.
Αρχή Εγγραφής (ΑΕ)	Πρόκειται για μια οντότητα που έχει εγκριθεί από μια ΑΠ και είναι υπεύθυνη για την ταυτοποίηση και την επαλήθευση της ταυτότητας των υποκειμένων των πιστοποιητικών. Επιπλέον, μια ΑΕ μπορεί να συνδράμει στη διαδικασία υποβολής αιτήσεων για πιστοποιητικό ή στη διαδικασία ανάκλησης ή και στις δύο διαδικασίες.
Βασιζόμενο Μέρος	Ένα φυσικό πρόσωπο ή οργανισμός που ενεργεί βασιζόμενος σε ένα πιστοποιητικό.
Εξ αποστάσεως ΕΔΔΥ	Εγκεκριμένη Διάταξη Δημιουργίας Υπογραφής Εξ αποστάσεως που πληροί τις απαιτήσεις του Παραρτήματος II του Κανονισμού eIDAS
Ανάκληση	Οριστική ανάκληση της ισχύος του πιστοποιητικού πριν από την ημερομηνία λήξης που αναγράφεται στο πιστοποιητικό.
ΑΠ βάσης	Η αρχή πιστοποίησης η οποία βρίσκεται στο υψηλότερο επίπεδο εντός του τομέα του ΠΥΕ και η οποία χρησιμοποιείται για να υπογράψει ιεραρχικά υφιστάμενες ΑΠ.
RSA	Κρυπτογραφικό σύστημα δημοσίου κλειδιού που επινοήθηκε από τους Rivest, Shamir και Adelman.
Μερίδιο Απορρήτου	Ένα τμήμα του ιδιωτικού κλειδιού μιας ΑΠ ή ένα τμήμα των δεδομένων ενεργοποίησης που είναι απαραίτητα για τη λειτουργία ενός ιδιωτικού κλειδιού της ΑΠ σύμφωνα με το σχέδιο του Διαμοιρασμού Απορρήτου.
Διαμοιρασμός Απορρήτου	Η πρακτική του διαχωρισμού ενός ιδιωτικού κλειδιού της ΑΠ ή των δεδομένων ενεργοποίησής του προκειμένου να λειτουργήσει το ιδιωτικό κλειδί της ΑΠ ώστε να ενισχύσει τον έλεγχο πολλαπλών ατόμων επί των λειτουργιών του ιδιωτικού κλειδιού της ΑΠ.
Επίπεδο Ασφαλών Συνδέσεων (SSL)	Η πρότυπη μέθοδος του κλάδου για την προστασία των Διαδικτυακών επικοινωνιών η οποία αναπτύχθηκε από τη Netscape Communications Corporation. Το πρωτόκολλο ασφαλείας SSL παρέχει κρυπτογράφηση των δεδομένων, επαλήθευση ταυτότητας διακομιστή (server), ακεραιότητα μηνύματος, και προαιρετικά επαλήθευση ταυτότητας χρήστη (client) για σύνδεση Transmission Control Protocol/Internet Protocol (Πρωτοκόλλου Ελέγχου Μετάδοσης/ Πρωτοκόλλου Διαδικτύου).

Διάρκεια ισχύος	Ορισμός
Υφιστάμενη ΑΠ	Η αρχή πιστοποίησης της οποίας το Πιστοποιητικό υπογράφεται από την ΑΠ Βάσης ή άλλης ιεραρχικά υφιστάμενης ΑΠ. Μια ιεραρχικά υφιστάμενη ΑΠ συνήθως εκδίδει είτε πιστοποιητικά τελικού χρήστη είτε άλλα πιστοποιητικά της ιεραρχικά υφιστάμενης ΑΠ.
Υποκείμενο	Το Υποκείμενο μπορεί να είναι: α) ένα φυσικό πρόσωπο· β) ένα φυσικό πρόσωπο που προσδιορίζεται σε σχέση με ένα νομικό πρόσωπο· γ) ένα νομικό πρόσωπο (που μπορεί να είναι ένας Οργανισμός ή μια μονάδα ή τμήμα που προσδιορίζεται σε σχέση με έναν Οργανισμό)·
Συνδρομητής	Μια οντότητα που είναι εγγεγραμμένη στον Πάροχο Υπηρεσιών Εμπιστοσύνης, η οποία δεσμεύεται νομικά από τυχόν υποχρεώσεις του Συνδρομητή.
Εποπτικός φορέας	Η αρχή που ορίζεται από κράτος μέλος για να διενεργεί τις εποπτικές δραστηριότητες σχετικά με τις Υπηρεσίες Εμπιστοσύνης και τους Παρόχους Υπηρεσιών Εμπιστοσύνης δυνάμει του κανονισμού eIDAS εντός της επικράτειας του εν λόγω κράτους μέλους.
Υπηρεσία Εμπιστοσύνης	Πρόκειται για την ηλεκτρονική υπηρεσία για τα ακόλουθα: • τη δημιουργία, την εξακρίβωση και την επικύρωση ψηφιακών υπογραφών, αυθεντικοποίησης και σχετικών πιστοποιητικών· • τη δημιουργία, την εξακρίβωση και την επικύρωση χρονοσφραγίδων και σχετικών πιστοποιητικών· • τη συστημένη παράδοση και τα πιστοποιητικά που σχετίζονται με την υπηρεσία αυτή· • τη δημιουργία, την εξακρίβωση και την επικύρωση πιστοποιητικών για επαλήθευση της ταυτότητας ιστότοπων, ή • τη διαφύλαξη ψηφιακών υπογραφών, αυθεντικοποίησης ή πιστοποιητικών που σχετίζονται με τις υπηρεσίες αυτές.
Πάροχος Υπηρεσίας Εμπιστοσύνης	Οντότητα που παρέχει μία ή περισσότερες Υπηρεσίες Εμπιστοσύνης.
Έμπιστο πρόσωπο	Ένας υπάλληλος, ανάδοχος ή σύμβουλος μιας οντότητας, ο οποίος είναι υπεύθυνος για τη διαχείριση της αξιοπιστίας της υποδομής της οντότητας, των προϊόντων, των υπηρεσιών, των εγκαταστάσεων και/ή των πρακτικών της.
Θέση Εμπιστοσύνης	Οι θέσεις εντός της JCC Payment Systems τις οποίες πρέπει να κατέχει Έμπιστο Πρόσωπο.
Αξιόπιστο Σύστημα	Το υλικό υπολογιστή, το λογισμικό και οι διαδικασίες, τα οποία είναι ασφαλή σε λογικά πλαίσια από εισβολές και κακή χρήση. Παρέχει ένα επίπεδο διαθεσιμότητας, αξιοπιστίας και ορθής λειτουργίας σε λογικά πλαίσια. Είναι κατά το δυνατόν κατάλληλο για την εκτέλεση των προβλεπόμενων λειτουργιών του και υλοποιεί την ισχύουσα πολιτική ασφάλειας. Ένα αξιόπιστο σύστημα δεν αποτελεί απαραίτητα ένα «σύστημα εμπιστοσύνης», όπως αναγνωρίζεται στην ταξινομημένη κρατική ονοματολογία.
Γενικοί Όροι και Προϋποθέσεις για τη χρήση πιστοποιητικών	Δεσμευτικό έγγραφο που καθορίζει του όρους και τις προϋποθέσεις βάσει των οποίων ένα φυσικό ή νομικό πρόσωπο ενεργεί ως Συνδρομητής ή ως Βασιζόμενο Μέρος και η JCC Payment Systems παρέχει τις αντίστοιχες Υπηρεσίες Εμπιστοσύνης.
Έγκυρο Πιστοποιητικό	Πιστοποιητικό που πέρασε με επιτυχία τη διαδικασία επικύρωσης η οποία προσδιορίζεται στο RFC 5280.
Περίοδος ισχύος	Η χρονική περίοδος που υπολογίζεται από την ημερομηνία έκδοσης του Πιστοποιητικού έως την ημερομηνία λήξης ισχύος.