



ATHEX
Χρηματιστήριο Αθηνών

ΥΠΗΡΕΣΙΕΣ ΨΗΦΙΑΚΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ

ΚΑΝΟΝΙΣΜΟΣ ΠΙΣΤΟΠΟΙΗΣΗΣ ΑΝΑΓΝΩΡΙΣΜΕΝΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΦΡΑΓΙΔΩΝ (CERTIFICATION PRACTICE STATEMENT FOR QUALIFIED ELECTRONIC SEAL)

Έκδοση 1.0 – 22/01/2018

OID: 1.3.6.1.4.1.29402.1.6.1.0

Εγκεκριμένος για τις ακόλουθες ‘Πολιτικές Πιστοποιητικών’ του Χ.Α.:
(Approved for the following ‘Certificate Policies’):

OID: 1.3.6.1.4.1.29402.1.6.1.0

{εσκεμμένα κενή}

- ΠΕΡΙΕΧΟΜΕΝΑ -

ΜΕΡΟΣ Ι: ΕΙΣΑΓΩΓΗ	7
1.1 ΓΕΝΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ.....	7
1.1.1 ΠΑΡΟΥΣΙΑΣΗ ΤΟΥ ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ Α.Ε. ΩΣ ΠΑΡΟΧΟΥ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ (Π.Υ.Π.).....	7
1.1.1.1 Τδρυση, σκοπός και δραστηριότητες του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ Α.Ε.	7
1.1.1.2 Οι ‘Υπηρεσίες Ψηφιακής Πιστοποίησης’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ	7
1.1.2 ΛΕΙΤΟΥΡΓΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΦΡΑΓΙΔΩΝ, ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ & ΕΦΑΡΜΟΓΕΣ.....	7
1.1.2.1 Ροή εργασίας της διαδικασίας ηλεκτρονικής σφράγισης.	7
1.1.2.2 Εφαρμογές των ηλεκτρονικών σφραγίδων.....	8
1.1.2.3 Θεσμικό πλαίσιο και κατηγορίες ηλεκτρονικών σφραγίδων	9
1.1.3 ΦΥΣΗ ΚΑΙ ΔΟΜΗ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ	10
1.1.3.1 Σκοπός της παρούσας τεκμηρίωσης	10
1.1.3.2 Δομή και περιεχόμενο	11
1.1.3.3 Αριθμός Έκδοσης και οι Αναθεωρήσεις μέρους ή του συνόλου του Κανονισμού.....	11
1.1.3.4 Χαρακτηριστικό Αναγνώρισης (OID) του παρόντος Κανονισμού	12
1.2 ΠΕΡΙΓΡΑΦΗ ΚΑΙ ΔΙΑΡΘΡΩΣΗ ΤΩΝ ‘ΥΠΗΡΕΣΙΩΝ ΨΗΦΙΑΚΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ’ ΤΟΥ ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ	13
1.2.1 ΛΕΙΤΟΥΡΓΙΚΗ ΔΙΑΚΡΙΣΗ ΤΩΝ ΠΡΟΣΦΕΡΟΜΕΝΩΝ ΥΠΗΡΕΣΙΩΝ.....	13
1.2.1.1 Υπηρεσία Εγγραφής	13
1.2.1.2 Υπηρεσία Έκδοσης Πιστοποιητικών.....	13
1.2.1.3 Υπηρεσία Προετοιμασίας Φορέα Συνδρομητών	13
1.2.1.4 Υπηρεσία Δημοσίευσης – ‘Ηλεκτρονικό Αποθετήριο’	13
1.2.1.5 Υπηρεσία Διαχείρισης Ανάκλησης	13
1.2.1.6 Υπηρεσία Χρονοσήμανσης Εγγράφων.....	14
1.2.1.7 Τοπικές Υπηρεσίες Υποβολής.....	14
1.2.2 ΟΙ ΕΠΙΤΡΟΠΕΣ ΤΟΥ ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ	14
1.2.2.1 ‘Επιτροπή Διαχείρισης Πολιτικής’ (Ε.Δ.Π.)	14
1.2.2.2 ‘Επιτροπή Διευθέτησης Παραπόνων και Επίλυσης Διαφορών’ (Ε.Δ.Π.Ε.Δ.)	14
1.2.3 ΚΟΙΝΟΤΗΤΑ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΚΑΙ ΣΥΜΒΑΛΛΟΜΕΝΑ ΜΕΡΗ	15
1.2.3.1 Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ ως ‘Πάροχος Υπηρεσιών Πιστοποίησης’	15
1.2.3.2 Οι ‘Τοπικές Υπηρεσίες Υποβολής’ (Τ.Υ.Υ.)	15
1.2.3.3 Οι Πιστοποιούμενοι Συνδρομητές - (‘Subscribers’)	16
1.2.3.4 Οι Χρήστες των Πιστοποιητικών (Τρίτα βασιζόμενα μέρη – ‘Relaying Parties’).	16
1.2.4 ΕΙΔΗ & ΕΦΑΡΜΟΓΕΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΠΟΥ ΕΚΔΙΔΟΝΤΑΙ ΑΠΟ ΤΟ ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ	16
1.2.4.1 Πιστοποιητικά για Νομικά Πρόσωπα.....	16
1.2.4.2 Πληροφορίες για τους τύπους Πιστοποιητικών	16
1.2.5 ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ	17
ΜΕΡΟΣ ΙΙ: ΓΕΝΙΚΟΙ ΟΡΟΙ ΚΑΙ ΠΟΛΙΤΙΚΕΣ	18
2.1 ΥΠΟΧΡΕΩΣΕΙΣ.....	18
2.1.1 ΥΠΟΧΡΕΩΣΕΙΣ ΤΟΥ ΠΑΡΟΧΟΥ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ	18
2.1.1.1 Υποχρεώσεις του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ ως ‘Θεμελιώδη Εκδότη Πιστοποιητικών’	18
2.1.1.2 Υποχρεώσεις της Υπηρεσίας Εγγραφής.....	18
2.1.1.3 Υποχρεώσεις της Υπηρεσίας Έκδοσης Πιστοποιητικών	18
2.1.1.4 Υποχρεώσεις της ‘Υπηρεσίας Προετοιμασίας Φορέα Συνδρομητών’	19
2.1.1.5 Υποχρεώσεις της Υπηρεσίας Δημοσίευσης - ‘Ηλεκτρονικού Αποθετηρίου’	19

2.1.1.6 Υποχρεώσεις της Υπηρεσίας Διαχείρισης Ανάκλησης	19
2.1.2 ΥΠΟΧΡΕΩΣΕΙΣ ΤΩΝ ΤΟΠΙΚΩΝ ΥΠΗΡΕΣΙΩΝ ΥΠΟΒΟΛΗΣ (Τ.Υ.Υ.)	20
2.1.3 ΥΠΟΧΡΕΩΣΕΙΣ ΤΟΥ ΣΥΝΔΡΟΜΗΤΗ	20
2.1.4 ΥΠΟΧΡΕΩΣΕΙΣ ΤΟΥ ΧΡΗΣΤΗ (ΒΑΣΙΖΟΜΕΝΟ ΜΕΡΟΣ)	21
2.2 ΕΓΓΥΗΣΕΙΣ, ΑΠΟΠΟΙΗΣΕΙΣ & ΟΡΙΑ ΕΥΘΥΝΗΣ	21
2.2.1 ΕΓΓΥΗΣΕΙΣ	21
2.2.2 ΑΠΟΠΟΙΗΣΕΙΣ ΕΥΘΥΝΗΣ	22
2.2.3 ΕΞΑΙΡΕΣΗ ΕΥΘΥΝΗΣ ΓΙΑ ΣΥΓΚΕΚΡΙΜΕΝΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ	22
2.2.4 ΑΝΩΤΑΤΑ ΟΡΙΑ ΕΥΘΥΝΗΣ ΤΟΥ ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ	23
2.2.5 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΙΣΗΣ	23
2.3 ΠΟΛΙΤΙΚΗ ΔΗΜΟΣΙΕΥΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ	23
2.3.1 ΗΛΕΚΤΡΟΝΙΚΟ ΑΠΟΘΕΤΗΡΙΟ (REPOSITORY) ΤΟΥ ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ	23
2.3.2 ΔΗΜΟΣΙΕΥΣΗ ΚΑΤΑΛΟΓΟΥ ΙΣΧΥΡΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ	23
2.3.3 ΔΗΜΟΣΙΕΥΣΗ 'ΛΙΣΤΩΝ ΑΝΑΚΛΗΘΕΝΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ' (ΛΑΠ)	23
2.3.4 ΔΗΜΟΣΙΕΥΣΗ ΚΑΝΟΝΙΣΜΟΥ ΠΙΣΤΟΠΟΙΗΣΗΣ & ΠΟΛΙΤΙΚΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ	24
2.3.5 ΑΣΦΑΛΗΣ ΔΙΑΝΟΜΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ	24
2.4 ΠΟΛΙΤΙΚΗ ΟΝΟΜΑΣΙΑΣ ΥΠΟΚΕΙΜΕΝΩΝ	24
2.5 ΠΟΛΙΤΙΚΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ	24
2.6 ΠΟΛΙΤΙΚΗ ΑΡΧΕΙΟΘΕΤΗΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ	25
2.7 ΠΟΛΙΤΙΚΗ ΕΠΙΛΥΣΗΣ ΔΙΑΦΟΡΩΝ	26
2.8 ΠΟΛΙΤΙΚΗ ΕΛΕΓΧΟΥ ΣΥΜΜΟΡΦΩΣΗΣ	26
2.8.1 ΕΘΕΛΟΝΤΙΚΗ ΔΙΑΠΙΣΤΕΥΣΗ ΚΑΙ ΔΙΑΠΙΣΤΩΣΗ	26
2.9 ΠΟΛΙΤΙΚΗ ΤΙΜΟΛΟΓΗΣΗΣ & ΕΠΙΣΤΡΟΦΗΣ ΧΡΗΜΑΤΩΝ	26
2.10 ΠΝΕΥΜΑΤΙΚΗ ΙΔΙΟΚΤΗΣΙΑ ΚΑΙ ΆΛΛΑ ΔΙΚΑΙΩΜΑΤΑ	26
2.11 ΕΡΜΗΝΕΙΑ ΚΑΙ ΕΚΤΕΛΕΣΤΟΤΗΤΑ	27
2.11.1 ΕΝΣΩΜΑΤΩΣΗ ΜΕ ΑΝΑΦΟΡΑ ΣΕ ΆΛΛΑ ΚΕΙΜΕΝΑ	27
2.11.2 ΣΥΓΚΡΟΥΣΗ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΕΙΡΑ ΙΣΧΥΟΣ	27
2.11.3 ΔΙΑΤΗΡΗΣΗ ΙΣΧΥΟΣ ΤΩΝ ΜΗ ΑΚΥΡΩΝ ΟΡΩΝ	27
2.11.4 ΕΦΑΡΜΟΣΤΕΟ ΔΙΚΑΙΟ – ΑΡΜΟΔΙΑ ΔΙΚΑΣΤΗΡΙΑ	27
ΜΕΡΟΣ III: ΛΕΙΤΟΥΡΓΙΚΟΙ ΟΡΟΙ	28
3.1 ΑΙΤΗΣΗ ΚΑΙ ΕΓΚΡΙΣΗ ΕΚΔΟΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ	28
3.1.1 ΠΟΙΟΙ ΚΑΙ ΠΩΣ ΜΠΟΡΟΥΝ ΝΑ ΑΙΤΗΘΟΥΝ ΤΗΝ ΕΚΔΟΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ	28
3.1.2 ΣΥΜΠΡΑΞΗ ΤΗΣ Τ.Υ.Υ. ΣΤΗΝ ΑΙΤΗΣΗ ΤΟΥ ΥΠΟΨΗΦΙΟΥ ΣΥΝΔΡΟΜΗΤΗ	28
3.1.3 ΕΓΚΡΙΣΗ ΑΠΟ ΤΗΝ ΥΠΗΡΕΣΙΑ ΕΓΓΡΑΦΗΣ	28
3.2 ΕΞΑΚΡΙΒΩΣΗ ΤΑΥΤΟΤΗΤΑΣ & ΓΝΗΣΙΟΤΗΤΑΣ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ	28
3.2.1 ΣΤΗΝ ΑΡΧΙΚΗ ΕΓΓΡΑΦΗ	28
3.2.2 ΣΤΗΝ ΑΙΤΗΣΗ ΑΝΑΚΛΗΣΗΣ & ΕΝΕΡΓΟΠΟΙΗΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ	29
3.2.3 ΣΤΗΝ ΑΝΑΝΕΩΣΗ ΤΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ	29
3.2.3.1 Φυσιολογική ανανέωση	29
3.2.3.2 Ανανέωση μετά από λήξη ή ανάκληση του πιστοποιητικού λόγω έκθεσης κλειδιών	29
3.2.3.3 Ανανέωση μετά από ανάκληση του πιστοποιητικού (όχι λόγω έκθεσης κλειδιών)	29

3.3 ΔΗΜΙΟΥΡΓΙΑ ΖΕΥΓΟΥΣ ΚΛΕΙΔΙΩΝ ΚΑΙ ΦΟΡΕΑΣ ‘Α.Δ.Δ.Υ.’	30
3.3.1 ΕΙΔΙΚΑ ΣΤΑ ΠΡΟΣΩΠΙΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ	30
3.3.1.1 Φορέας Έξυπνη Κάρτα	30
3.3.1.1.1 Δημιουργία και εναποθήκευση των κλειδιών σε φορέα ‘α.δ.δ.υ.’	30
3.3.1.1.2 Εξατομίκευση φορέα ‘α.δ.δ.υ.’ και καταγραφή ‘κωδικού ενεργοποίησής’ (PIN) του	30
3.3.1.1.3 Παράδοση του φορέα στον συνδρομητή	30
3.3.1.2 Συσκευή απομακρυσμένης υπογραφής	31
3.4 ΕΚΔΟΣΗ ΚΑΙ ΑΡΧΙΚΗ ΕΝΕΡΓΟΠΟΙΗΣΗ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ.....	31
3.4.1 ΕΚΔΟΣΗ ΑΠΟ ΤΟΝ ΚΑΤΑΛΛΗΛΟ ΛΕΙΤΟΥΡΓΙΚΟ ΕΚΔΟΤΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ	31
3.4.2 ΔΙΑΔΙΚΑΣΙΑ ΑΡΧΙΚΗΣ ΕΝΕΡΓΟΠΟΙΗΣΗΣ ΤΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ	31
3.5 ΔΙΑΡΚΕΙΑ ΚΑΙ ΛΗΞΗ ΙΣΧΥΟΣ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ	32
3.5.1 ΔΙΑΡΚΕΙΑ ΙΣΧΥΟΣ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ	32
3.5.2 ΑΥΤΟΜΑΤΗ ΛΗΞΗ ΤΗΣ ΙΣΧΥΟΣ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ	32
3.6 ΑΝΑΝΕΩΣΗ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ	32
3.6.1 ΠΕΡΙΠΤΩΣΕΙΣ ΑΝΑΝΕΩΣΗΣ	32
3.6.2 ΠΡΟΫΠΟΘΕΣΕΙΣ ΑΝΑΝΕΩΣΗΣ	33
3.6.3 ΤΡΟΠΟΣ ΑΝΑΝΕΩΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ	33
3.7 ΑΝΑΣΤΟΛΗ ΚΑΙ ΑΝΑΚΛΗΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ	33
3.7.1 ΕΝΝΟΙΑ ‘ΠΑΥΣΗΣ/ΑΝΑΣΤΟΛΗΣ’ ΚΑΙ ‘ΑΝΑΚΛΗΣΗΣ’ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ	33
3.7.2 ΛΟΓΟΙ ΑΝΑΣΤΟΛΗΣ’ Ή/ΚΑΙ ‘ΑΝΑΚΛΗΣΗΣ’ ΕΝΟΣ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ	34
3.7.2.1 Λόγοι ανάκλησης από τις Υπηρεσίες του Δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ ..	34
3.7.2.2 Λόγοι για υποβολή αίτησης ανάκλησης από τον Συνδρομητή	34
3.7.2.3 Άλλοι λόγοι Αναστολής ή Ανάκλησης	34
3.7.3 ΔΙΑΔΙΚΑΣΙΑ ΑΝΑΣΤΟΛΗΣ, ΑΝΑΚΛΗΣΗΣ ΚΑΙ (ΕΠΑΝ-)ΕΝΕΡΓΟΠΟΙΗΣΗΣ	35
3.7.4 ΥΠΟΧΡΕΩΤΙΚΗ (ΕΠΑΝ-)ΕΝΕΡΓΟΠΟΙΗΣΗ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ	35
3.7.5 ΣΥΧΝΟΤΗΤΑ ΕΚΔΟΣΗΣ ΛΙΣΤΑΣ ΑΝΑΚΛΗΘΕΝΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ (CRL)	35
3.8 ΑΛΛΑΓΗ ΚΛΕΙΔΙΩΝ ΚΑΙ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΤΗΣ ΥΠΟΔΟΜΗΣ ‘ΡΚΙ’	36
3.8.1 ΑΛΛΑΓΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΤΩΝ ‘ΥΠΟ-ΕΚΔΟΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ’	36
3.8.2 ΑΛΛΑΓΗ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΤΟΥ ‘Θ.Ε.Π.’ ΤΟΥ ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (ROOT CA)	36
3.9 ΠΑΥΣΗ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ ΑΠΟ ΤΟ ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ	36
ΜΕΡΟΣ IV: ΑΞΙΟΠΙΣΤΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΟΣ.....	38
4.1 ΤΕΧΝΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ	38
4.1.1 ΔΗΜΙΟΥΡΓΙΑ ΤΩΝ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΚΛΕΙΔΙΩΝ	38
4.1.1.1 Δημιουργία και αποθήκευση κλειδιών των Εκδοτών Πιστοποιητικών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ	38
4.1.1.2 Δημιουργία κλειδιών των συνδρομητών (τελικών οντοτήτων)	38
4.1.1.3 Μέγεθος και διάρκεια ισχύος των κλειδιών	39
4.1.1.4 Χρησιμοποιούμενοι Αλγόριθμοι από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ	39
4.1.2 ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΙΔΙΩΤΙΚΩΝ ΚΛΕΙΔΙΩΝ	39
4.1.2.1 Ασφαλής διαδικασία δημιουργίας και υποχρεωτική χρήση φορέα των ιδιωτικών κλειδιών	39
4.1.2.2 Αντιγραφή (back-up), εναποθήκευση και ανάκτηση των ιδιωτικών κλειδιών	40
4.1.2.3 Κωδικός ενεργοποίησης του φορέα των ιδιωτικών κλειδιών	40
4.1.2.4 Περιορισμένη χρήση των ιδιωτικών κλειδιών	40
4.1.2.5 Καταστροφή ιδιωτικών κλειδιών των Εκδοτών Πιστοποιητικών μετά την λήξη τους	41

4.1.3 ΆΛΛΑ ΜΕΤΡΑ ΤΕΧΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ	41
4.2 ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ	41
4.2.1 ΕΠΙΛΟΓΗ ΚΑΙ ΚΑΤΑΣΚΕΥΗ ΤΩΝ ΧΩΡΩΝ	41
4.2.2 ΦΥΣΙΚΗ ΠΡΟΣΒΑΣΗ	42
4.2.3 ΠΑΡΟΧΗ ΗΛΕΚΤΡΙΣΜΟΥ, ΚΛΙΜΑΤΙΣΜΟΣ, ΠΥΡΑΣΦΑΛΕΙΑ ΚΑΙ ΔΙΑΡΡΟΕΣ	42
4.2.4 ΕΝΑΠΟΘΗΚΕΥΣΗ ΦΟΡΕΩΝ ΔΕΔΟΜΕΝΩΝ (MEDIA).....	42
4.2.5 ΔΙΑΘΕΣΗ ΕΡΓΑΛΕΙΩΝ ΚΑΙ ΔΕΔΟΜΕΝΩΝ ΑΣΦΑΛΕΙΑΣ	42
4.2.6 ΑΠΟΜΑΚΡΥΣΜΕΝΟ ΕΝΑΛΛΑΚΤΙΚΟ ΣΥΣΤΗΜΑ ΚΑΙ ΑΝΤΙΓΡΑΦΑ ΑΣΦΑΛΕΙΑΣ	43
4.3 ΕΛΕΓΧΟΣ ΚΑΙ ΑΣΦΑΛΕΙΑ ΤΩΝ ΔΙΑΔΙΚΑΣΙΩΝ.....	43
4.3.1 ΕΜΠΙΣΤΟΙ ΡΟΛΟΙ.....	43
4.3.2 ΕΜΠΙΣΤΟΙ ΡΟΛΟΙ ΤΗΣ ΥΠΗΡΕΣΙΑΣ ΕΚΔΟΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ	43
4.3.3 ΕΜΠΙΣΤΟΙ ΡΟΛΟΙ ΤΗΣ ΥΠΗΡΕΣΙΑΣ ΕΓΓΡΑΦΗΣ & ΔΙΑΧΕΙΡΙΣΗΣ ΑΝΑΚΛΗΣΗΣ	43
4.3.4 ΑΡΙΘΜΟΣ ΑΠΑΙΤΟΥΜΕΝΩΝ ΠΡΟΣΩΠΩΝ ΓΙΑ ΤΗΝ ΕΚΤΕΛΕΣΗ ΜΙΑΣ ΕΡΓΑΣΙΑΣ	43
4.4 ΕΛΕΓΧΟΣ ΚΑΙ ΑΞΙΟΠΙΣΤΙΑ ΠΡΟΣΩΠΙΚΟΥ	44
4.4.1 ΑΠΑΙΤΗΣΕΙΣ ΕΜΠΕΙΡΙΑΣ, ΔΙΑΠΙΣΤΕΥΣΕΩΝ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗΣ	44
4.4.2 ΑΠΑΙΤΗΣΕΙΣ ΕΚΠΑΙΔΕΥΣΗΣ.....	44
4.4.3 ΔΙΕΝΕΡΓΕΙΑ ΕΛΕΓΧΩΝ ΚΑΙ ΚΥΡΩΣΕΙΣ	45
4.4.4 ΠΡΟΣΩΠΙΚΟ ΣΥΜΒΕΒΛΗΜΕΝΩΝ ΣΥΝΕΡΓΑΤΩΝ	45
4.4.5 ΠΑΡΟΧΗ ΟΔΗΓΙΩΝ ΚΑΙ ΤΕΚΜΗΡΙΩΣΗΣ	45
ΜΕΡΟΣ Β: ΠΕΡΙΓΡΑΦΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ & Λ.Α.Π.....	46
5.1 ΠΕΡΙΓΡΑΦΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ.....	46
5.1.1 ΤΥΠΟΣ ΚΑΙ ΑΡΙΘΜΟΣ ΕΚΔΟΣΗΣ	46
5.1.2 ΠΕΡΙΕΧΟΜΕΝΟ ΚΑΙ ΣΗΜΑΣΙΑ ΤΩΝ ΠΕΔΙΩΝ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ	46
5.1.3 ΤΥΠΟΣ ΚΑΙ ΠΕΡΙΕΧΟΜΕΝΟ ΤΩΝ ΔΙΑΚΕΚΡΙΜΕΝΩΝ ΟΝΟΜΑΤΩΝ (DN)	47
5.1.3.1 Διακεκριμένο όνομα (DN) του 'Θεμελιώδη Εκδότη Πιστοποιητικών' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ	47
5.1.3.2 Διακεκριμένο όνομα (DN) των 'Λειτουργικών Εκδοτών Πιστοποιητικών' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ	48
5.1.3.3 Διακεκριμένο όνομα (DN) των 'Θεμάτων' (Υποκείμενα-Συνδρομητές).....	49
5.1.4 ΧΑΡΑΚΤΗΡΙΣΜΟΣ ΚΡΙΣΙΜΟΤΗΤΑΣ ΤΩΝ ΕΚΤΕΤΑΜΕΝΩΝ ΠΕΔΙΩΝ ΤΟΥ	49
5.2 ΠΕΡΙΓΡΑΦΗ 'ΛΙΣΤΑΣ ΑΝΑΚΛΗΘΕΝΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ' (ΛΑΠ)	49
5.2.1 ΤΥΠΟΣ ΚΑΙ ΑΡΙΘΜΟΣ ΕΚΔΟΣΗΣ	49
5.2.2 ΠΕΡΙΕΧΟΜΕΝΟ ΚΑΙ ΣΗΜΑΣΙΑ ΤΩΝ ΠΕΔΙΩΝ ΜΙΑΣ ΛΑΠ	50
5.2.3 ΧΑΡΑΚΤΗΡΙΣΜΟΣ ΚΡΙΣΙΜΟΤΗΤΑΣ ΤΩΝ ΕΚΤΕΤΑΜΕΝΩΝ ΠΕΔΙΩΝ ΤΗΣ	50

ΜΕΡΟΣ Ι: ΕΙΣΑΓΩΓΗ

1.1 ΓΕΝΙΚΕΣ ΠΛΗΡΟΦΟΡΙΕΣ

1.1.1 ΠΑΡΟΥΣΙΑΣΗ ΤΟΥ ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ Α.Ε. ΩΣ ΠΑΡΟΧΟΥ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ (Π.Υ.Π.)

1.1.1.1 Έτοιμη στην χρήση για την παροχή υπηρεσιών πιστοποίησης

Παράλληλα με τις οικονομικού τύπου δραστηριότητες η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ αναπτύσσει και προϊόντα λογισμικού που βοηθούν στην καλύτερη οργάνωση, διαχείριση και πληροφοριακή υποστήριξη των άλλων συντελεστών της Κεφαλαιαγοράς, όπως τα μέλη της Αγοράς Αξιών και της Αγοράς Παραγώγων του ΧΑ, εισιγμένες εταιρίες, χρηματοπιστωτικούς οργανισμούς και επενδυτές.

Μερικά από τα χαρακτηριστικά έργα που η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ μελέτησε, ανάπτυξε ή διαχειρίζεται με επιτυχία είναι:

- το «Ολοκληρωμένο Αντόματο Σύστημα Ηλεκτρονικών Συναλλαγών (Ο.Α.Σ.Η.Σ.)» και το «Δίκτυο Χρηματιστηριακών Συναλλαγών (Δ.Χ.Σ.)» του ΧΑ, μέσω των οποίων διεξάγονται καθημερινά οι χρηματιστηριακές συναλλαγές στις αγορές Μετοχών, Ομολόγων και Παραγώγων της ελληνικής κεφαλαιαγοράς,
 - το «Σύστημα Στατιστικής και Πληροφόρησης» (Σ.Σ.Π.)» του ΧΑ, στο οποίο βασίζεται η λειτουργία των υπηρεσιών διάχυσης πληροφόρησης του ΧΑ,
 - η ιστοσελίδα της EXAE (www.athexgroup.gr),
- η σουίτα εφαρμογών MarketSuite του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ που απευθύνεται σε χρηματιστηριακές εταιρίες και επενδυτές.

1.1.1.2 Οι ‘Υπηρεσίες Ψηφιακής Πιστοποίησης’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ

Η διογκούμενη ανάγκη για ασφάλεια των ηλεκτρονικών επικοινωνιών, ειδικά σε χώρους όπως είναι αυτός της Κεφαλαιαγοράς, επέβαλε στο ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ την δημιουργία μιας λειτουργικά ανεξάρτητης επιχειρησιακής μονάδας, με την ονομασία «Υπηρεσίες Ψηφιακής Πιστοποίησης», η οποία ανέλαβε την ανάπτυξη, την εφαρμογή και την υποστήριξη ενός σύγχρονου και αξιόπιστου συστήματος ασφάλειας των ηλεκτρονικών συναλλαγών με την χρήση ‘προηγμένων ηλεκτρονικών υπογραφών’.

Στα πλαίσια του τμήματος αυτού, η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ,

- αξιοποιώντας την εμπειρία, την τεχνογνωσία και την αξιοπιστία του προσωπικού της,
- χρησιμοποιώντας τις πιο σύγχρονες -τόσο σε software όσο και hardware- τεχνολογικές εφαρμογές για τον συγκεκριμένο σκοπό,

ανέπτυξε μια σύγχρονη και αξιόπιστη ‘Υποδομή Δημοσίου Κλειδιού’ (Public Key Infrastructure – ‘P.K.I.’) για την παροχή «έμπιστων υπηρεσιών» προς το κοινό (ως ‘Εμπιστη Τρίτη Οντότητα’) που περιλαμβάνουν την έκδοση και διαχείριση ‘ηλεκτρονικών πιστοποιητικών’ για την δημιουργία ‘προηγμένων ηλεκτρονικών υπογραφών και ηλεκτρονικών σφραγίδων’.

1.1.2 ΛΕΙΤΟΥΡΓΙΑ ΗΛΕΚΤΡΟΝΙΚΩΝ ΣΦΡΑΓΙΔΩΝ, ΘΕΣΜΙΚΟ ΠΛΑΙΣΙΟ & ΕΦΑΡΜΟΓΕΣ

1.1.2.1 Ροή εργασίας της διαδικασίας ηλεκτρονικής σφράγισης.

Ένας κάτοχος σφραγίδας, για να δημιουργήσει μια σφραγίδα σε ένα έγγραφο, εργάζεται σε ένα συγκεκριμένο περιβάλλον (π.χ. φορητό υπολογιστή) για να αποκτήσει πρόσβαση σε λειτουργίες σφράγισης που είναι κατασκευασμένες από:

A. την εφαρμογή δημιουργίας σφραγίδας (π.χ. μια εφαρμογή pdf που παραμένει στον φορητό υπολογιστή) και

B. η συσκευή δημιουργίας σφραγίδας που

- i. διατηρεί τα δεδομένα δημιουργίας σφραγίδας (ιδιωτικό κλειδί).
- ii. πρέπει να είναι σε θέση να επικυρώνει τον δημιουργό της σφραγίδας (για να εγγυάται τον έλεγχό του στο ιδιωτικό κλειδί).
- iii. υπολογίζει τη σφράγιση (χρησιμοποιώντας τα δεδομένα δημιουργίας σφραγίδας).
- iv. μπορεί να κατέχει το πιστοποιητικό σφραγίσεως (ή να περιέχει αναμφισβήτητες αναφορές σε αυτό).

Συγκεκριμένα, πώς λειτουργεί;

1. Ο δημιουργός της σφραγίδας προετοιμάζει το έγγραφο που πρόκειται να σφραγιστεί (π.χ. ένα αρχείο PDF).
2. Η εφαρμογή προετοιμάζει τα δεδομένα που πρόκειται να σφραγιστούν (δηλ. Το PDF) σε ένα συμπύκνωμα (που ονομάζεται hash) και τα παρουσιάζει στη συσκευή δημιουργίας ασφαλούς σφραγίδας.
3. Η συσκευή δημιουργίας σφραγίδας ζητά την εξουσιοδότηση του δημιουργού της σφραγίδας να σφραγίσει τα δεδομένα, γενικά, μέσα από ένα παράθυρο που εμφανίζεται στην οθόνη. Ο δημιουργός της σφραγίδας πιστοποιεί τη συσκευή (π.χ. εισάγει έναν κωδικό PIN ή ένα δακτυλικό αποτύπωμα). Όπως εξηγείται αργότερα, τα δεδομένα δημιουργίας σφραγίδας μπορούν να διαχειρίζονται εξ αποστάσεως (π.χ. σε ασφαλές διακομιστή) και ενδέχεται να υπάρχουν περισσότερα από ένα άτομα εξουσιοδοτημένα να τα ενεργοποιούν για να δημιουργήσουν μια σφραγίδα για λογαριασμό ενός οργανισμού.
4. Η συσκευή δημιουργίας υπολογίζει τη σφραγίδα και στέλνει το αποτέλεσμα στην εφαρμογή που ενσωματώνει τη σφραγίδα στο έγγραφο. Σε αυτό το στάδιο, είναι σημαντικό να σημειωθεί ότι, γενικά, το πιστοποιητικό της σφραγίδας παρέχεται με τα σφραγισμένα δεδομένα. Αυτό επιτρέπει την ταυτοποίηση του κατόχου σφραγίδας και την επαλήθευση της σφραγίδας δεδομένου ότι το δημόσιο κλειδί είναι άμεσα διαθέσιμο από το πιστοποιητικό.

Προσθήκες για μεγαλύτερη ευεληξία

Προσθήκες στις σφραγίδες είναι η διαδικασία με την οποία ορισμένα υλικά (π.χ. χρονικά σήματα, δεδομένα επικύρωσης και ακόμη και αρχειακό υλικό) ενσωματώνονται στις σφραγίδες για να γίνουν πιο ανθεκτικές στις αλλαγές ή στη διεύρυνση της μακροζωίας τους. Η αύξηση μπορεί να γίνει είτε από τον δημιουργό της σφραγίδας, είτε από τον υπεύθυνο ή από ένα TSP που επικυρώνει ή διατηρεί τη σφραγίδα για λογαριασμό του δημιουργού της σφραγίδας ή του βασικού συμβαλλόμενου μέρους. Π.χ. αν κάποιος ζητήσει από μια εταιρεία να σφραγίσει ένα πιστωτικό σημείωμα, είναι πιθανό ότι το πρώτο πρόσωπο έχει κάποιο ενδιαφέρον για τη διατήρηση της σφραγίδας (κάτι που δεν είναι απαραίτητη η περίπτωση του δημιουργού της σφραγίδας). Αντίθετα, εάν η σφραγίδα δεν επαληθευθεί αμέσως από τον εμπλεκόμενο, ο δημιουργός της σφραγίδας μπορεί να έχει κάποιο ενδιαφέρον για την ολοκλήρωση της σφράγισης, π.χ. με μια αξιόπιστη σφραγίδα χρόνου, προκειμένου να παράσχει μια αξιόπιστη απόδειξη του χρόνου σφράγισης. Με τον τρόπο αυτό, θα είναι δύσκολο για τον εμπλεκόμενο να απορρίψει τη σφραγίδα σε περίπτωση επακόλουθου προβλήματος όσον αφορά τη σφράγιση (π.χ. λήξη του πιστοποιητικού σφράγισης).

1.1.2.2 Εφαρμογές των ηλεκτρονικών σφραγίδων

Επειδή εδώ και μερικά χρόνια είναι δυνατή η ηλεκτρονική υπογραφή δεδομένων και η επίτευξη των ίδιων αποτελεσμάτων με τη χρήση χειρόγραφης υπογραφής. Η ισοδυναμία με χειρόγραφες υπογραφές λειτουργεί πολύ καλά για τα ανθρώπινα όντα, αλλά ήταν δύσκολο να επεκταθεί σε νομικά πρόσωπα (που ουσιαστικά δεν μπορούν να υπογράψουν χειρόγραφα). Ωστόσο, για τα νομικά πρόσωπα (εταιρείες, οργανώσεις κλπ.) που τους ήταν απαραίτητο για την επίσημη δημοσίευση των ηλεκτρονικών εγγράφων που έχουν εκδώσει, προκειμένου να εξασφαλίσουν την προέλευση του εγγράφου.

Σήμερα ο κανονισμός eIDAS υποστηρίζει αυτή την ανάγκη χάρη στη νομική αναγνώριση των ηλεκτρονικών σφραγίδων, οι οποίες χρησιμεύουν ως απόδειξη ότι ένα ηλεκτρονικό έγγραφο εκδόθηκε από ένα νομικό πρόσωπο, εξασφαλίζοντας την βεβαιότητα της καταγωγής και της ακεραιότητας του εγγράφου. Εκτός από την επικύρωση του εγγράφου που εκδίδεται από το νομικό πρόσωπο, μπορούν να χρησιμοποιηθούν

ηλεκτρονικές σφραγίδες για τον έλεγχο ταυτότητας οποιουδήποτε ψηφιακού στοιχείου του νομικού προσώπου, όπως κώδικας λογισμικού ή διακομιστές (κανονισμός eIDAS).

Μια αναγνωρισμένη ηλεκτρονική σφραγίδα απολαμβάνει το τεκμήριο της ακεραιότητας των δεδομένων και της ορθότητας της προέλευσης των δεδομένων στα οποία συνδέεται η ειδική ηλεκτρονική σφραγίδα.

Εκτός από το νομικό πλαίσιο, το τεχνικό πλαίσιο είναι σήμερα πολύ ώριμο καθώς βασίζεται σε μεγάλο βαθμό στο τεχνικό πλαίσιο που αναπτύχθηκε με την πάροδο των ετών για την ηλεκτρονική υπογραφή.

Η χρήση εξειδικευμένων ηλεκτρονικών σφραγίδων θα βοηθήσει στην ανάπτυξη ηλεκτρονικών επιχειρήσεων και υπηρεσιών στην Ευρώπη, διασφαλίζοντας τις ηλεκτρονικές συναλλαγές και υπηρεσίες πέρα από πολλούς τομείς: ηλεκτρονικό εμπόριο, ηλεκτρονική διοίκηση, ηλεκτρονική τραπεζική, ηλεκτρονικές υπηρεσίες, ηλεκτρονική αρχειοθέτηση κ.λπ.

1.1.2.3 Θεσμικό πλαίσιο και κατηγορίες ηλεκτρονικών σφραγίδων

Ο κανονισμός (ΕΕ) αριθ. 910/2014 eIDAS ορίζει μια ηλεκτρονική σφραγίδα ως "δεδομένα σε ηλεκτρονική μορφή, τα οποία συνδέονται ή λογικά συνδέονται με άλλα δεδομένα σε ηλεκτρονική μορφή για να εξασφαλίζουν την προέλευση και την ακεραιότητα του τελευταίου". Μια αναγνωρισμένη ηλεκτρονική σφραγίδα απολαμβάνει το τεκμήριο της ακεραιότητας των δεδομένων και της ορθότητας της προέλευσης των δεδομένων στα οποία συνδέεται η ειδική ηλεκτρονική σφραγίδα.

Μια σφραγίδα "δημιουργείται" από έναν δημιουργό της σφραγίδας, ενδεχομένως "επαυξημένη" (δηλ. Συμπληρωμένη με σχετικές αποδείξεις ή ενδείξεις - βλ. Ενότητα 6), "επικυρωμένη" από τον παραλήπτη των σφραγισμένων δεδομένων (αποκαλούμενο ", και ενδεχομένως διατηρημένα, σε ορισμένες περιπτώσεις για μακρό χρονικό διάστημα.

Ο τρόπος με τον οποίο χρησιμοποιούνται αυτά τα χαρακτηριστικά καθορίζει το επίπεδο αντοχής, αξιοπιστίας και μακροζωίας των ειδικών σφραγίδων. Συγκεκριμένα, μπορούν να κληθούν οι TSPs, με τα κατάλληλα προσόντα ή όχι, για τη δημιουργία, την επικύρωση ή / και τη διατήρηση της κατάλληλης σφραγίδας.

Οι ηλεκτρονικές σφραγίδες δημιουργούνται από μια συσκευή δημιουργίας ηλεκτρονικής σφραγίδας, η οποία ορίζεται στον κανονισμό eIDAS ως «διαμορφωμένο λογισμικό ή υλικό που χρησιμοποιείται για τη δημιουργία ηλεκτρονικής σφραγίδας μέσω ενός« ηλεκτρονικού υλικού δημιουργίας σφραγίδας »(δηλαδή" ένα μοναδικό στοιχείο που χρησιμοποιείται από τον δημιουργό της σφραγίδας για να δημιουργήσει μια ηλεκτρονική σφραγίδα ")».

Στους ορισμούς αυτούς, τα "μοναδικά δεδομένα" πρέπει να θεωρούνται ως προσωπικό στοιχείο που ανήκει στον δημιουργό της σφραγίδας. Μπορεί να συγκριθεί με τους δακτυλίους με χαραγμένο σχέδιο που χρησιμοποιείται για τη σφράγιση σφράγισης σε κερί κατά την παλιά εποχή. Τα επίσημα μηνύματα, από ένα βασίλειο π.χ., αναγνωρίστηκαν εύκολα επειδή όλοι γνώριζαν την επίσημη χαραγμένη σχεδίαση. Το δαχτυλίδι ήταν ένα χειροποίητο τεχνούργημα, ένα a priori όχι (εύκολα) αναπαραγώγιμο, καθιστώντας τη βασιλική σφραγίδα δύσκολη να μιμηθεί και δύσκολο να κλέψει γιατί φορούσε το είδος. Με τον ίδιο τρόπο που ο δημιουργός της σφραγίδας διατηρεί τον δακτύλιο του ασφαλή στον κόσμο του χαρτιού, τα δεδομένα δημιουργίας ηλεκτρονικής σφραγίδας πρέπει επίσης να προστατεύονται στον ηλεκτρονικό κόσμο. Τυπικά, θα αποθηκεύεται με ασφάλεια σε μια συσκευή (π.χ. μια έξυπνη κάρτα όπως μια τραπεζική κάρτα) που μπορεί να ενεργοποιηθεί μόνο από τον κάτοχό της, π.χ. μέσω κωδικού PIN ή βιομετρίας (π.χ. δακτυλικό αποτύπωμα). Επειδή η σφραγίδα αντιπροσωπεύει έναν οργανισμό, σε ορισμένες περιπτώσεις μπορεί να υπάρχουν περισσότερα από ένα φυσικά πρόσωπα εξουσιοδοτημένα να δημιουργούν σφραγίδες για λογαριασμό της οργάνωσης. ενδέχεται να υπάρχουν περισσότεροι από ένας κωδικοί PIN ή ένα δακτυλικό αποτύπωμα που έχουν καταχωρηθεί για την ενεργοποίηση δεδομένων δημιουργίας σφραγίδας.

Οι ηλεκτρονικές σφραγίδες γενικά δεν θα στερούνται νομικής ισχύος και παραδεκτού ως αποδεικτικών στοιχείων σε δικαστικές διαδικασίες. Στο πλαίσιο της οικογένειας ηλεκτρονικών σφραγίδων, ο κανονισμός eIDAS ορίζει υποσύνολα ηλεκτρονικών σφραγίδων που παρέχουν αυξημένη νομική προβλεψιμότητα μέχρι

το επίπεδο, την κατάλληλη ηλεκτρονική σφραγίδα, η οποία επωφελείται από αυτόματο τεκμήριο ακεραιότητας των δεδομένων και από την ορθότητα της προέλευσης υπηρεσίας, επωφελείται από αυτόματη αναγνώριση):

- την ηλεκτρονική σφραγίδα (που παρουσιάζεται παραπάνω)
- η προηγμένη ηλεκτρονική σφραγίδα (AdESeal) - η οποία απαιτεί χαρακτηριστικά ασφαλείας που διασφαλίζουν ότι είναι μοναδικά συνδεδεμένη με τον υπογράφοντα, είναι ικανή να προσδιορίσει την υποκείμενη οντότητα και συνδέεται με τα δεδομένα με τέτοιο τρόπο ώστε οποιαδήποτε μεταγενέστερη αλλαγή των δεδομένων να είναι ανιχνεύσιμη.
- η αναγνωρισμένη ηλεκτρονική σφραγίδα (QESeal) - η οποία είναι μια προηγμένη ηλεκτρονική σφραγίδα που παρέχει πρόσθετο επίπεδο διαβεβαίωσης για την ταυτότητα του δημιουργού της σφραγίδας και μια ενισχυμένη προστασία και επίπεδο εξασφάλισης στη δημιουργία σφραγίδας. Απαιτείται ειδική συσκευή για τη δημιουργία του QESeal (ειδική συσκευή δημιουργίας σφραγίδας, QSealCD).

ΤΟ ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ, ΘΕΛΟΝΤΑΣ ΝΑ ΠΡΟΣΦΕΡΕΙ ΤΟ ΥΨΗΛΟΤΕΡΟ ΔΥΝΑΤΟ ΕΠΙΠΕΔΟ ΥΠΗΡΕΣΙΩΝ με την μεγαλύτερη δυνατή αξιοπιστία και ασφάλεια, ΠΑΡΕΧΕΙ ΣΤΟΥΣ ΣΥΝΔΡΟΜΗΤΕΣ ΤΗΣ ΕΝΑΝ ΣΥΝΔΥΑΣΜΟ ΠΡΟΪΟΝΤΩΝ ΚΑΙ ΥΠΗΡΕΣΙΩΝ ΠΟΥ ΔΙΕΥΚΟΛΥΝΟΥΝ ΤΙΣ ΑΣΦΑΛΕΙΣ ΣΥΝΑΛΛΑΓΕΣ ΤΟΥΣ, ΕΞΑΣΦΑΛΙΖΟΝΤΑΣ ΤΗΝ ΤΗΡΗΣΗ ΤΩΝ ΠΡΟΥΠΟΘΕΣΕΩΝ ΤΟΥ ΝΟΜΟΥ ΓΙΑ ΤΗΝ ΔΗΜΙΟΥΡΓΙΑ ‘ΑΝΑΓΝΩΡΙΣΜΕΝΩΝ ΗΛΕΚΤΡΟΝΙΚΩΝ ΥΠΟΓΡΑΦΩΝ’.

1.1.3 ΦΥΣΗ ΚΑΙ ΔΟΜΗ ΤΟΥ ΚΑΝΟΝΙΣΜΟΥ

1.1.3.1 Σκοπός της παρούσας τεκμηρίωσης

Η παρούσα τεκμηρίωση των «Υπηρεσιών Ψηφιακής Πιστοποίησης» της ΕΛΛΗΝΙΚΑ ΧΡΗΜΑΤΙΣΤΗΡΙΑ- ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ ΣΥΜΜΕΤΟΧΩΝ ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (στο εξής «ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ»), που φέρει τον τίτλο «Κανονισμός Πιστοποίησης των Αναγνωρισμένων Ηλεκτρονικών Σφραγίδων» ('*Certification Practice Statement of Qualified Electronic Seals*' ή '*CPS- QESeal*' στα αγγλικά) έχει ως σκοπό **να προσδιορίσει αναλυτικά και να καταγράψει, καθώς και να γνωστοποιήσει προς κάθε ενδιαφερόμενο μέρος (και συνεργάτες της, συνδρομητές και τρίτα -βασιζόμενα στις υπηρεσίες της- μέρη, αρχές και σχετικούς φορείς διαπίστωσης ή/και διαπίστευσης) τους όρους και τις συνθήκες και προϋποθέσεις καθώς και τις λειτουργικές και επιχειρηματικές πρακτικές που εφαρμόζονται ή διέπουν την παροχή των Υπηρεσιών Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, και πιο συγκεκριμένα την Πολιτική και τον Κανονισμό Πιστοποίησης για τα Αναγνωρισμένα Πιστοποιητικά.**

ΤΗ «Πολιτική Αναγνωρισμένων Πιστοποιητικών» που εκδίδεται από την ‘Επιτροπή Διαχείρισης Πολιτικής’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (δες παρακάτω -παράγραφο 1.2.5), καθορίζει και αναλύει τους όρους έκδοσης, διαχείρισης και χρήσης για τα Αναγνωρισμένα Πιστοποιητικά που εκδίδει το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ.

Το παρόν κείμενο (ο «Κανονισμός Πιστοποίησης») για τα Αναγνωρισμένα Πιστοποιητικά προσδιορίζει την οργάνωση των υπηρεσιών της, τις γενικές λειτουργικές αρχές και πρακτικές που εφαρμόζει καθώς και τα μέτρα ασφαλείας που λαμβάνονται κατά την παροχή των υπηρεσιών πιστοποίησης από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ για τα εν λόγω Αναγνωρισμένα Πιστοποιητικά. (Σημείωση: Όλες οι υποστηριζόμενες Πολιτικές των πιστοποιητικών και ο παρών Κανονισμός δημοσιεύονται από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ στο ‘ηλεκτρονικό αποθετήριό’ της, -δες παράγραφο 2.3.1.)

Έτσι, με την ανάγνωση του παρόντος «Κανονισμού Πιστοποίησης» και της σχετικής «Πολιτικής Πιστοποιητικού», ο κάθε ενδιαφερόμενος είναι σε θέση να εκτιμήσει και να αξιολογήσει τον βαθμό ασφαλείας και αξιοπιστίας που προσφέρει ένα συγκεκριμένο είδος ή ομάδα πιστοποιητικών που εκδίδονται από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ, ώστε να αποφασίσει ο ίδιος εάν θα βασισθεί στις πληροφορίες που του παρέχονται από αυτά ή/και για την καταλληλότητά τους σχετικά με τον σκοπό ή την εφαρμογή

που προτίθεται να τα χρησιμοποιήσει.

Τέλος, πρόθεση του κειμένου αυτού είναι να προσφέρει παράλληλα (με όσα δημοσιεύονται στο Ηλεκτρονικό Αποθετήριο του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ) μια γενική επιμόρφωση καθώς και μια στοιχειώδη βάση με πληροφορίες και παραπομπές σε σχετικές πηγές ή κείμενα για την έννοια, τον τρόπο χρήσης και τις νομικές συνέπειες των προηγμένων ηλεκτρονικών υπογραφών προς τον αναγνώστη του.

1.1.3.2 Δομή και περιεχόμενο

Ο παρών ‘Κανονισμός Πιστοποιήσεων των Αναγνωρισμένων Ηλεκτρονικών Σφραγίδων του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ’ (‘X.A. Certification Practice Statement for Qualified Electronic Seals’ or ‘X.A C.P.S. QESeal’) βασίζεται στον κανονισμό (ΕΕ) αριθ. 910/2014 eIDAS για την έκδοση, τη συντήρηση και τη διαχείριση του κύκλου ζωής των Πιστοποιητικών ΕΕ για ηλεκτρονικές σφραγίδες.

Η διάρθρωση του παρόντος Κανονισμού διαιρείται από την προτεινόμενη στο πρότυπο στο βαθμό που είναι απαραίτητο για να περιγράψει κατάλληλα και να απλοποιήσει την κατανόηση των λειτουργικών πρακτικών που ακολουθούνται στα πλαίσια των ‘Υπηρεσιών Ψηφιακής Πιστοποίησης’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

Το κείμενο του Κανονισμού διαιρείται σε **πέντε (5) Μέρη:**

ΜΕΡΟΣ Ι: ΕΙΣΑΓΩΓΗ	γενικές πληροφορίες για το ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, εισαγωγή στο PKI και το θεσμικό πλαίσιο, ταυτοποίηση της παρούσας τεκμηρίωσης, παρουσίαση της διάρθρωσης των υπηρεσιών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, περιγραφή και εφαρμογές των πιστοποιητικών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, στοιχεία επικοινωνίας.
ΜΕΡΟΣ ΙΙ: ΓΕΝΙΚΟΙ ΟΡΟΙ ΚΑΙ ΠΟΛΙΤΙΚΕΣ	Υποχρεώσεις και ευθύνες των συμμετεχόντων μερών, εγγυήσεις, αποποίησης και όρια ευθύνης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, καθώς και πολιτικές για την προστασία των προσωπικών δεδομένων, την επίλυση διαφορών, την παροχή πληροφοριών, την αρχειοθέτηση, την τιμολογιακή πολιτική κ.ά.
ΜΕΡΟΣ ΙΙΙ: ΔΕΙΤΟΥΡΓΙΚΟΙ ΟΡΟΙ	Αίτηση Πιστοποιητικού, ταυτοποίηση του αιτούντα, δημιουργία κλειδιών και εξαπομίκευση φορέα τους, έκδοση πιστοποιητικού, λήξη πιστοποιητικού, ανανέωση και δημιουργία νέων κλειδιών, πάση και ανάκληση πιστοποιητικών, αλλαγή κλειδιών, τερματισμός των υπηρεσιών
ΜΕΡΟΣ ΙV: ΑΞΙΟΠΙΣΤΙΑ & ΕΛΕΓΧΟΣ ΣΥΣΤΗΜΑΤΟΣ	Τεχνικές προδιαγραφές ασφαλείας, όπως δημιουργία και προστασία των κλειδιών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, ασφάλεια δικτύου, κ.λ.π., καθώς και προδιαγραφές φυσικής ασφάλειας, έλεγχος και ασφάλεια των διαδικασιών και στοιχεία για την αξιοπιστία και την εκπαίδευση του προσωπικού
ΜΕΡΟΣ V: ΠΕΡΙΓΡΑΦΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ & Λ.Α.Π.	Διάρθρωση και περιεχόμενα των X.509 v.3 πιστοποιητικών και της ‘Λίστας Ανακληθέντων Πιστοποιητικών’ (Λ.Α.Π.), κανόνες ονομασίας, χρησιμοποιόμενα πεδία και επεκτάσεις αντών, σημασία και ερμηνεία των περιεχομένων των πεδίων, κρισιμότητα των πεδίων κ.λ.π.

1.1.3.3 Αριθμός Έκδοσης και οι Αναθεωρήσεις μέρους ή του συνόλου του Κανονισμού

Ο Κανονισμός αυτός χαρακτηρίζεται από μία ‘ημερομηνία έκδοσης’ και από ένα ‘κωδικό αριθμό έκδοσης’ αποτελούμενο από δύο αριθμητικά ψηφία χωρισμένα με τελεία(.) τα οποία υποδεικνύουν το μεν πρώτο τον αριθμό σημαντικών αναθεωρήσεων που έχουν επέλθει στον Κανονισμό, το δε δεύτερο τις δευτερεύουσες ή/και επουσιώδεις τροποποιήσεις σε επιμέρους σημεία της τεκμηρίωσης. Η πρώτη εγκεκριμένη έκδοση αριθμείται με τον κωδικό ‘1.0’

Αναθεωρήσεις μέρους ή του συνόλου του Κανονισμού αυτού είναι δυνατόν να γίνονται περιοδικά ή οποτεδήποτε κριθεί αναγκαίο από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ. Οι αναθεωρήσεις αυτές δημοσιεύονται και τίθενται σε ισχύ σύμφωνα με τα οριζόμενα στην παράγραφο 2.3.4.

Κάθε νέα ή τροποποιημένη έκδοση του Κανονισμού λαμβάνει υέο ‘κωδικό αριθμό έκδοσης’ ανξάνοντας το πρώτο ή το δεύτερο ψηφίο του, ανάλογα με την κρισιμότητα των αλλαγών του.

(Σημείωση: Προσθήκες στο Μέρος VI του Κανονισμού αυτού (Παραρτήματα) που έχουν ως σκοπό την υποβοήθηση του αναγνώστη των στην κατανόηση της λειτουργίας και του θεσμικού πλαισίου των ηλεκτρονικών υπογραφών μπορούν να γίνονται οποτεδήποτε χωρίς την αλλαγή του ‘κωδικού αριθμού έκδοσης’ και χωρίς άλλες υποχρεώσεις δημοσιότητας.)

1.1.3.4 Χαρακτηριστικό Αναγνώρισης (OID) του παρόντος Κανονισμού

Αυτό το έγγραφο πρέπει να αναφέρεται σε σύντμηση ως «**Κ.Π.Α.Η.Σ. του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, έκδ. 1.0**» και στην αγγλική του έκδοση ως «**X.A. C.P.S. QESeal. ver. 1.0**»

Ο παγκοσμίως μοναδικός Αριθμός Αναγνώρισης (OID) αυτού του εγγράφου είναι:

1.3.6.1.4.1.29402.1.6.1.0

όπου:

1.3.6.1.4.1.29402	<i>Αριθμός Αναγνώρισης (OID) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, καταχωρημένος από τον IANA</i>
1	<i>Ανεξάρτητο τμήμα «Υπηρεσιών Δημοσίας Πιστοποίησης» του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ</i>
6	<i>Κανονισμός Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών</i>
1.0	<i>Πρώτο και δεύτερο ψηφίο του αριθμού έκδοσης του Κανονισμού</i>

1.2 ΠΕΡΙΓΡΑΦΗ ΚΑΙ ΔΙΑΡΩΡΩΣΗ ΤΩΝ ‘ΥΠΗΡΕΣΙΩΝ ΨΗΦΙΑΚΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ’ ΤΟΥ ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ

Σημείωση- Διευκρίνιση: Στα επόμενα, οποιαδήποτε αναφορά σε πιστοποιητικά και συναφείς υπηρεσίες αφορούν σε Αναγνωρισμένα Πιστοποιητικά και συναφείς υπηρεσίες, εκτός εάν ρητά δηλώνεται διαφορετικά. Επιπλέον οποιαδήποτε αναφορά σε Κανονισμό Πιστοποίησης και Πολιτική Πιστοποιητικών αφορά σε Κανονισμό Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών καθώς και Πολιτική Αναγνωρισμένων Πιστοποιητικών.

1.2.1 ΛΕΙΤΟΥΡΓΙΚΗ ΔΙΑΚΡΙΣΗ ΤΩΝ ΠΡΟΣΦΕΡΟΜΕΝΩΝ ΥΠΗΡΕΣΙΩΝ

Οι υπηρεσίες που παρέχονται από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ ως ‘Τρίτη Έμπιστη Οντότητα’ προς το κοινό στο πλαίσιο των ‘Υπηρεσίων Ψηφιακής Πιστοποίησής’ της, κατανέμονται λειτουργικά στις εξής διακριτές ‘λειτουργικές οντότητες’:

1.2.1.1 Υπηρεσία Εγγραφής

Η ‘Υπηρεσία Εγγραφής’ (*Registration Service*), καλούμενη και ‘Αρχή Εγγραφής’ (*Registration Authority* ή ‘RA’), δέχεται τις αιτήσεις των υποψήφιων συνδρομητών (υποκείμενα πιστοποίησης) από τις συνεργαζόμενές της ‘Τοπικές Υπηρεσίες Υποβολής’ (δες παραγράφους 1.2.1.7 και 1.2.3.2) και εφόσον επαληθεύσει την φυσική ταυτότητα και τα δημόσια κλειδιά του αιτούντα, εγκρίνει την έκδοση των πιστοποιητικών διαβιβάζοντας τα ακριβή στοιχεία του συνδρομητή στην ‘Υπηρεσία Έκδοσης Πιστοποιητικών’.

1.2.1.2 Υπηρεσία Έκδοσης Πιστοποιητικών

Η ‘Υπηρεσία Έκδοσης Πιστοποιητικών’ (*Certificate Generation Service*), διαθέτοντας επιμέρους ‘Λειτουργικούς Εκδότες Πιστοποιητικών’ (*Operational Certification Authorities* ή ‘*Operational CAs*’) ή Υπο-Εκδότες (Subordinate CA ή Sub-CA) για κάθε τύπο ή κλάση πιστοποιητικών, δημιουργεί, εκδίδει και υπογράφει πιστοποιητικά βασιζόμενη στα στοιχεία ταυτότητας και άλλες πληροφορίες που επαλήθευσε και της μεταβίβασε η ‘Υπηρεσία Εγγραφής’. Οι ‘Εκδότες Πιστοποιητικών’ της υπηρεσίας που υπογράφουν τα πιστοποιητικά των τελικών οντοτήτων, διαθέτουν για αυτόν το σκοπό διαφορετικά κρυπτογραφικά κλειδιά, πιστοποιημένα από τον Θεμελιώδη Εκδότη Πιστοποιητικών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ’ (X.A. Root CA). Επιπλέον ο Συνδρομητής έχει την δυνατότητα να χρησιμοποιήσει την ειδικά διαμορφωμένη διαδικτυακή εφαρμογή για την παραγωγή, ανανέωση ή και ανάκληση του Αναγνωρισμένου Πιστοποιητικού. Επίσης μέσω της εν λόγω εφαρμογής δημιουργεί με ασφαλή τρόπο ζεύγη ασύμμετρων κρυπτογραφικών κλειδιών. Συνεπώς, η παραγωγή του εν λόγω αναγνωρισμένου πιστοποιητικού και των ασύμμετρων κρυπτογραφικών κλειδιών μεταφέρεται πλήρως στην πλευρά του Συνδρομητή.

1.2.1.3 Υπηρεσία Προετοιμασίας Φορέα Συνδρομητών

Η Υπηρεσία αυτή (*Subscriber Device Provision Service*), εφόσον προβλέπεται από την Πολιτική του αιτηθέντος πιστοποιητικού, δημιουργεί με ασφαλή τρόπο ζεύγη ασύμμετρων κρυπτογραφικών κλειδιών για τους συνδρομητές, τα οποία μεταφέρει σε ‘εξατομικευμένες’ για αυτούς φορείς δημιουργίας υπογραφής (π.χ. smart-cards). Η Υπηρεσία προμηθεύει τους αιτηθέντες με τους φορείς αυτούς, ενημερώνοντας ταυτόχρονα την ‘Υπηρεσία Εγγραφής’ για τα δημιουργηθέντα δημόσια κλειδιά του συνδρομητή που πρέπει να πιστοποιηθούν.

1.2.1.4 Υπηρεσία Δημοσίευσης – ‘Ηλεκτρονικό Αποθετήριο’

Η ‘Υπηρεσία Δημοσίευσης’ (*Dissemination Service*), μέσω του ‘Ηλεκτρονικού Αποθετηρίου’ (*Repository*) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ - το οποίο συντηρεί και ενημερώνει (δες παράγραφο 2.3.1) -, δημοσιεύει και διανέμει προς κάθε ενδιαφερόμενο συνδρομητή ή τρίτο όλους τους όρους και τις προϋποθέσεις για την έκδοση, τη διαχείριση και την χρήση των πιστοποιητικών (π.χ. τον παρόντα ‘Κανονισμό Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών’, τις ‘Πολιτικές Αναγνωρισμένων Πιστοποιητικών’, κ.λ.π.) καθώς και τους καταλόγους με τα ισχύοντα και τα ανακληθέντα (ή πανθέντα) πιστοποιητικά.

1.2.1.5 Υπηρεσία Διαχείρισης Ανάκλησης

Η Υπηρεσία αυτή (*Revocation Management & Status Service*) διαχειρίζεται τις αιτήσεις και τις αναφορές για αναστολή ή ανάκληση πιστοποιητικών και αποφασίζει τις απαραίτητες ενέργειες που πρέπει να

γίνουν. Εκδίδει τακτικά ή και εκτάκτως ενημερωμένες ‘Λίστες Ανακληθέντων Πιστοποιητικών’ (Λ.Α.Π.) οι οποίες υπογράφονται από τον ίδιο τον ‘Λειτουργικό Εκδότη Πιστοποιητικών’ που τα εξέδωσε και τις οποίες δημοσιεύει σε συνεργασία με την ‘Υπηρεσία Δημοσίευσης’.

1.2.1.6 Υπηρεσία Χρονοσήμανσης Εγγράφων

Η ‘Υπηρεσία Χρονοσήμανσης Εγγράφων’ (*Time-stamping Service*) θα παρέχει πιστοποιητικά χρονοσήμανσης σε ηλεκτρονικά έγγραφα κατόπιν αίτησης του ‘κομιστή’ του εγγράφου. Η υπηρεσία αυτή συμβάλλει καθοριστικά στην μακροχρόνια επαλήθευση των ηλεκτρονικά υπογεγραμμένων εγγράφων.

1.2.1.7 Τοπικές Υπηρεσίες Υποβολής

Οι ‘Τοπικές Υπηρεσίες Υποβολής’ (Local RA Assistants), που συνεργάζονται με τις Υπηρεσίες Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, βοηθούν τους υποψήφιους συνδρομητές στην αίτησή τους για έκδοση πιστοποιητικών, προμηθεύοντάς τους με το απαραίτητο έντυπο υλικό (αιτήσεις, συμβάσεις, τεκμηρίωση κ.λπ.) και παρέχοντάς τους υπηρεσίες τιμολόγησης των υπηρεσιών. Οι T.Y.Y. συνυπογράφουν τις αιτήσεις των συνδρομητών -μετά από πρόχειρο έλεγχο των δικαιολογητικών τους- και τις στέλνουν στην αρμόδια ‘Υπηρεσία Εγγραφής’ για έγκριση. Ενίστε, και σε συνεργασία με την σχετική ‘Υπηρεσία Προμήθειας Φορέα Συνδρομητών’, παρέχουν προς τους υποψήφιους συνδρομητές και κατάλληλους φορείς ‘ασφαλούς διάταξης δημιουργίας υπογραφής’ ιδιοκτησίας τους.

1.2.2 ΟΙ ΕΠΙΤΡΟΠΕΣ ΤΟΥ ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ

Πέρα από τις παραπάνω λειτουργικές οντότητες που εκτελούν τις επιμέρους υπηρεσίες πιστοποίησης, στα πλαίσια των Υπηρεσιών Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ λειτουργούν επίσης οι εξής Επιτροπές:

1.2.2.1 ‘Επιτροπή Διαχείρισης Πολιτικής’ (Ε.Δ.Π.)

Η Ε.Δ.Π. συντίθεται από ανώτατα στελέχη του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ με την συμμετοχή έμπειρων/ εξειδικευμένων τεχνικών και νομικών συμβούλων και αποτελεί το αρμόδιο όργανο για την χάραξη της πολιτικής και τον σχεδιασμό των προσφερόμενων υπηρεσιών ψηφιακής πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

Η Ε.Δ.Π., αφού λάβει υπ’ όψιν της τις τεχνολογικές εξελίξεις, το κανονιστικό πλαίσιο, τις εμπορικές και συναλλακτικές ανάγκες (του ΧΑ ή και των συνδρομητών) και τους επιχειρηματικούς σχεδιασμούς του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, εκδίδει ή/και τροποποιεί τις ‘Πολιτικές Πιστοποιητικών’ (που ορίζονται από την άρση της έκδοσης, διαχείρισης και χρήσης για κάθε τύπο ηλεκτρονικών πιστοποιητικών που εκδίδεται από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ), και εγκρίνει τους ‘Κανονισμούς Πιστοποίησης Πιστοποιητικών’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (και πιθανώς και άλλων Παρόχων Υπηρεσιών Πιστοποίησης) ή τις αναθεωρήσεις του, διαπιστώνοντας την καταλληλότητά του στην υποστήριξη και στην εκτέλεση των παραπάνω Πολιτικών.

Η Ε.Δ.Π. συνεδριάζει κάθε τρείς μήνες εφόσον υπάρχει θέμα προς συζήτηση και λήψη αποφάσεως ή εκτάκτως όποτε συντρέχει περίπτωση, προκειμένου να εξετάσει τις τρέχουσες συνθήκες και την αναγκαιότητα για αναθεώρηση ή έκδοση νέων πολιτικών και κανονισμών.

Η επιτροπή δύναται να λάβει απόφαση ακόμη και εάν δεν έχει προηγηθεί συνεδριασή της εφόσον καταρτισθεί και υπογραφεί πρακτικό από όλα τα μέλη της με το περιεχόμενο της σχετικής απόφασής (δια περιφοράς συνεδρίαση)

1.2.2.2 ‘Επιτροπή Διευθέτησης Παραπόνων και Επίλυσης Διαφορών’ (Ε.Δ.Π.Ε.Δ.)

Η Ε.Δ.Π.Ε.Δ. συνεδριάζει κάθε τρείς μήνες εφόσον υπάρχει θέμα προς συζήτηση και λήψη αποφάσεως ή εκτάκτως όποτε συντρέχει περίπτωση, με αρμοδιότητα τον έλεγχο της τίτλησης του Κανονισμού Πιστοποίησης και την διευθέτηση πιθανών παραπόνων ή/και την επίλυση τυχόν διαφορών σχετικά με τις Υπηρεσίες Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

Αποτελείται από στελέχη του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ και εξειδικευμένους τεχνικούς και νομικούς οι οποίοι ενεργούν τις προβλεπόμενες στο Κεφάλαιο 2.7 (‘Πολιτική Επίλυσης Διαφορών’) διαδικασίες και διαβιβάζουν ερωτήματα προς την Ε.Δ.Π. του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ στην

περίπτωση αμφιβολίας.

Η επιτροπή δύναται να λάβει απόφαση ακόμη και εάν δεν έχει προηγηθει συνεδριασή της εφόσον καταρτισθεί και υπογραφεί πρακτικό από όλα τα μέλη της με το περιεχόμενο της σχετικής απόφασής (δια περιφοράς συνεδρίαση)

Η Ε.Δ.Π.Ε.Δ. έχει πλήρη πρόσβαση στα αρχεία και στις εγγραφές ελέγχου (logs) των Υπηρεσιών Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ και συντάσσει κάθε χρόνο ετήσια έκθεση απευθυνόμενη στην Ε.Δ.Π. με τα πεπραγμένα και τα συμπεράσματά της.

1.2.3 ΚΟΙΝΟΤΗΤΑ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΚΑΙ ΣΥΜΒΑΛΛΟΜΕΝΑ ΜΕΡΗ

1.2.3.1 Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ ως ‘Πάροχος Υπηρεσιών Πιστοποίησης’

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ, ως ‘Πάροχος Υπηρεσιών Πιστοποίησης’, **συμβάλλεται είτε άμεσα** (με την δική τους Τ.Υ.Υ.) **είτε έμμεσα** (μέσω των συνεργαζόμενων Τ.Υ.Υ. που λειτουργούν από εξουσιοδοτημένους τρίτους –βλ. παρακάτω) **με τους συνδρομητές της** με σκοπό να εκδώσει και να διαχειριστεί ηλεκτρονικά πιστοποιητικά για αυτούς και τις συσκευές τους.

Με βάση τους κανόνες υψηλής ασφάλειας που έχει ορίσει στον παρόντα Κανονισμό Πιστοποίησης, η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ, ως ‘Θεμελιώδης Εκδότης Πιστοποιητικών’ (Root CA), δημιουργεί το βασικό ζεύγος κρυπτογραφικών κλειδιών με το οποίο εκδίδει και υπογράφει το πιστοποιητικό της (self-signing) και τα πιστοποιητικά όλων των ‘**Υπο-Εκδοτών Πιστοποιητικών**’ της (Subordinate CAs) που εκδίδουν τα πιστοποιητικά προς τις τελικές οντότητες, εγκαθιδρύοντας έτσι μια ολοκληρωμένη ‘υποδομή δημοσίων κλειδιών’ (PKI) που στηρίζει τις παρεχόμενες υπηρεσίες της.

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ μπορεί να αναθέτει μέρος ή και το σύνολο των αναφερόμενων στην παράγραφο 1.2.1 υπηρεσών σε συνεργαζόμενους τρίτους φορείς (φυσικά ή νομικά πρόσωπα) δημιουργώντας έτσι ένα ‘**Δίκτυο Υπηρεσιών Δημοσίας Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ**’ (στο εξής «**Δίκτυο**»), διατηρεί ούμως η ίδια **την συνολική ευθύνη** απέναντι στους συνδρομητές της και στους χρήστες των πιστοποιητικών της. Τα μέλη του ‘**Δικτύου**’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ αναλαμβάνουν να παρέχουν προς τους συνδρομητές και τους τρίτους τις ανατεθειμένες σ’ αυτούς υπηρεσίες (π.χ. Υπηρεσία Εγγραφής, Υπηρεσία Έκδοσης, Υπηρεσία Δημοσίευσης κ.λ.π.) σύμφωνα με τους όρους του παρόντος Κανονισμού, **ευθυνόμενα σύμφωνα με τις υπάρχουσες συμβάσεις συνεργασίας απέναντι στο ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ και ευρισκόμενα υπό τον άμεσο έλεγχό της** για την συμμόρφωσή τους με τους παραπάνω όρους.

1.2.3.2 Οι ‘Τοπικές Υπηρεσίες Υποβολής’ (Τ.Υ.Υ.)

Οι Τ.Υ.Υ. είναι συνήθως **ανεξάρτητοι οργανισμοί ή εταιρίες** που συμβάλλονται με το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ (ή με κάποιο εξουσιοδοτημένο μέλος του ‘**Δικτύου**’ της που παρέχει ‘**Υπηρεσίες Εγγραφής**’), ώστε να συνεισφέρουν στην παροχή των υπηρεσιών του ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ προς τα συνδεόμενα με αυτές (ως εργαζόμενοι, πελάτες ή συνεργάτες) πρόσωπα ή οντότητες (π.χ. servers), πιθανώς για την κοινή χρήση των πιστοποιητικών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ σε κάποια συγκεκριμένη εφαρμογή τους. Παρόλο που οι Τ.Υ.Υ. δεν παρέχουν ‘**Υπηρεσίες Εγγραφής**’, αποτελούν την **αποκλειστική δίοδο** για έναν συνδρομητή να ζητήσει την εγγραφή του και να αποκτήσει πιστοποιητικά από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ.

Έτσι οι Τ.Υ.Υ. **αναλαμβάνουν** την ενημέρωση, την προμήθεια του κατάλληλου έντυπου υλικού και την τιμολόγηση των υπηρεσιών πιστοποίησης προς το κοινό, στο οποίο απευθύνονται. Οι Τ.Υ.Υ. μπορούν επίσης να παρέχουν (είτε υποχρεωτικά είτε προαιρετικά και κατά την κρίση τους) και ‘**ασφαλή διάταξη δημιουργίας υπογραφών**’ (π.χ. έξυπνη κάρτα) ιδιοκτησίας τους, προς τους συνδρομητές που συμβάλλονται με το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ μέσω αυτών, η οποία εξαπομικεύεται (με την αναγραφή προσωπικών στοιχείων) για τους συνδρομητές από την ‘**Υπηρεσία Προετοιμασίας Φορέα Συνδρομητών**’ του δικτύου.

Οι Τ.Υ.Υ., μέσω εξουσιοδοτημένων υπαλλήλων τους που ορίζονται από αυτήν ως ‘**Διαχειριστές της Τ.Υ.Υ.**’, **συνυπογράφουν** υποχρεωτικά την ‘**Αίτηση Πιστοποίησης και Σύμβασης Συνδρομητή**’ των υποψήφιων συνδρομητών, την οποία και αποστέλλουν (μαζί και με τα υπόλοιπα απαραίτητα δικαιολογητικά) στην αρμόδια Υπηρεσία Εγγραφής του δικτύου. Τέλος, οι Τ.Υ.Υ. **χρεώνουν** τους αιτηθέντες με όλα τα τέλη

και το κόστος σχετικά με τις παρεχόμενες υπηρεσίες από το δίκτυο του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, έχοντας ανεξάρτητη ‘Τιμολογιακή Πολιτική’.

Τοπική Υπηρεσία Υποβολής μπορεί να λειτουργεί και από το ίδιο το νομικό πρόσωπο του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ για τις ανάγκες πιστοποίησης των υφιστάμενων τεχνολογικών υποδομών της.

1.2.3.3 Οι Πιστοποιούμενοι Συνδρομητές - ('Subscribers')

Συνδρομητές ή πιστοποιούμενοι του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ είναι τα νομικά πρόσωπα για τα οποία έχει εκδοθεί πιστοποιητικό για κάποιο αντικείμενο ή συσκευή (π.χ. server) της κυριότητάς τους από το Δίκτυο Υπηρεσιών Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

Για να γίνει κάποιος ‘συνδρομητής’ πρέπει να απευθυνθεί σε κάποια ‘Τοπική Υπηρεσία Υποβολής’ (ΤΥΥ) του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ ώστε να συμπληρώσει την σχετική Αίτηση - προσκομίζοντας παράλληλα και τα απαραίτητα σχετικά δικαιολογητικά, καθώς και να υπογράψει την ‘Σύμβαση συνδρομητή’. Εάν **εγκριθεί** η αίτησή του από την αρμόδια Υπηρεσία Εγγραφής (YE) του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, τότε αυτή δίνει την εντολή στον σχετικό Λειτουργικό Εκδότη Πιστοποιητικών του δικτύου ο οποίος προχωρεί στην έκδοση του πιστοποιητικού.

1.2.3.4 Οι Χρήστες των Πιστοποιητικών (Τρίτα βασιζόμενα μέρη – ‘Relaying Parties’)

Χρήστες ή τρίτα βασιζόμενα μέρη των πιστοποιητικών είναι τα νομικά πρόσωπα που, αφού ενημερωθούν και συμφωνήσουν με τους όρους και τις προϋποθέσεις χρήσης του πιστοποιητικού που περιέχονται στον παρόντα Κανονισμό, στη σχετική ‘Πολιτική Αναγνωρισμένου Πιστοποιητικού’ και στη ‘Σύμβαση Χρήστη/Αποδέκτη’, και αφού ελέγξουν και επαληθεύσουν την εγκυρότητα ενός αναγνωρισμένου πιστοποιητικού που έχει εκδοθεί από το δίκτυο του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ σύμφωνα με τα παραπάνω (είτε διά τις εποπτικής μεθόδου είτε με την χρήση αυτόματων εφαρμογών τους), **αποφασίζουν οι ίδιοι** αν θα βασισθούν ή όχι στα περιεχόμενα του πιστοποιητικού ώστε να προβούν σε μία συγκεκριμένη πράξη, ενέργεια ή παράλειψη, ή να αποκτήσουν την δικαιολογημένη πεποίθηση για ένα γεγονός.

‘Χρήστης Πιστοποιητικού’ μπορεί κάλλιστα να είναι ένας συνδρομητής ή ακόμη και ένα μέλος του ίδιου του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, που ακολουθώντας την παραπάνω διαδικασία, βασίζεται ή όχι στο πιστοποιητικό κάποιου τρίτου που έχει εκδοθεί από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ.

1.2.4 ΕΙΔΗ & ΕΦΑΡΜΟΓΕΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΠΟΥ ΕΚΔΙΔΟΝΤΑΙ ΑΠΟ ΤΟ ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ

1.2.4.1 Πιστοποιητικά για Νομικά Πρόσωπα

Για τις νομικές οντότητες ή τους νόμιμους εκπροσώπους των νομικών προσώπων, το Χ.Α. εκδίδει πιστοποιητικά για ηλεκτρονικές σφραγίδες, δηλαδή εγκεκριμένη ηλεκτρονική σφραγίδα (QESeal) - η οποία είναι προηγμένη ηλεκτρονική σφραγίδα και παρέχει πρόσθετο επίπεδο διαβεβαίωσης για την ταυτότητα του δημιουργού της σφραγίδας και ενισχυμένη προστασία του επίπεδου εξασφάλισης της δημιουργίας σφραγίδας. Απαιτείται ειδική συσκευή για τη δημιουργία του QESeal (ειδική συσκευή δημιουργίας σφραγίδας, QSealCD).

Τα Πιστοποιητικά συμμορφώνονται με τα NCP + και QCP-lqscd. Τα πιστοποιητικά που εκδίδονται βάσει αυτών των απαιτήσεων αποσκοπούν στη στήριξη ειδικευμένων ηλεκτρονικών σφραγίδων με τη χρήση συσκευής ειδικής δημιουργίας υπογραφής (QSCD) όπως ορίζεται στο άρθρο 3 (27) του κανονισμού (ΕΕ) αριθ. 910/2014 [i.1].

1.2.4.2 Πληροφορίες για τους τύπους Πιστοποιητικών

Για περισσότερες πληροφορίες σχετικά με το βοηθητικό πρόγραμμα, τον προορισμό, το περιεχόμενο, τους ειδικούς όρους και προϋποθέσεις χρήσης κάθε πιστοποιητικού, ανατρέξτε στις αντίστοιχες «Πολιτικές Πιστοποιητικών» που είναι διαθέσιμες στο διαδίκτυο (εκτός από την πολιτική «Πιστοποιητικά ΑΠ») στο «Καταθετήριο» του Χ.Α. στον ιστότοπο <http://www.athexgroup.gr/web/guest/digital-certificates>) ή

επικοινωνήστε με το Χ.Α. (Ανατρέξτε στις πληροφορίες επικοινωνίας που ακολουθούν) ή έναν τοπικό βοηθό RA για περισσότερες πληροφορίες και έντυπες εκδόσεις των κειμένων.

1.2.5 ΣΤΟΙΧΕΙΑ ΕΠΙΚΟΙΝΩΝΙΑΣ

Η επικοινωνία και οι τυχόν κοινοποιήσεις προς τις Υ.Ψ.Π.. του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, τις υπηρεσίες του Δικτύου της, ή τις παραπάνω Επιτροπές της, πρέπει να γίνονται στην διεύθυνση:

Χρηματιστήριο Αθηνών

ΥΠΗΡΕΣΙΕΣ ΨΗΦΙΑΚΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ

Λεωφ. Αθηνών 110 , 10442

Αθήνα

Τηλ.: +30 210 336 6300

Fax: +30 210 336 6301

e-mail: PKICA-Services@athexgroup.gr

web: <http://www.athexgroup.gr/web/guest/digital-certificates>

ΜΕΡΟΣ ΙΙ: ΓΕΝΙΚΟΙ ΟΡΟΙ ΚΑΙ ΠΟΛΙΤΙΚΕΣ

2.1 ΥΠΟΧΡΕΩΣΕΙΣ

2.1.1 ΥΠΟΧΡΕΩΣΕΙΣ ΤΟΥ ΠΑΡΟΧΟΥ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ

2.1.1.1 Υποχρεώσεις του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ ως ‘Θεμελιώδη Εκδότη Πιστοποιητικών’

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ, ως ‘Θεμελιώδης Εκδότης Πιστοποιητικών’ (‘ΘΕΠ’ ή ‘Root CA’) και ιδρύτρια της ‘υποδομής δημοσίων κλειδιών’ (PKI) της, έχει τις ακόλουθες υποχρεώσεις:

1) Να υποστηρίζει την λειτουργία της ‘υποδομής δημοσίου κλειδιού’ (PKI) της και να καταβάλλει κάθε εύλογη προσπάθεια για τη διατήρηση ενός αξιόπιστου συστήματος, σύμφωνα με τις προβλέψεις του παρόντος Κανονισμού.

3) Να δημοσιεύει και να διαθέτει το ‘αυτο-ϋπογραφόμενο πιστοποιητικό’ της, και τα ‘Πιστοποιητικά CA’ των ‘Λειτουργικών Εκδοτών Πιστοποιητικών’ (*Operational CAs*) που έχει εκδώσει.

3) Να εκδίδει και να εγκρίνει, διαμέσου των Επιτροπών της, τον Κανονισμό Πιστοποίησης, τις Πολιτικές για κάθε τύπο, είδος ή κλάση πιστοποιητικού που εκδίδεται από το δίκτυο της και, γενικά, όλους του όρους που διέπουν την παροχή των ‘υπηρεσιών ψηφιακής πιστοποίησης’ της.

4) Να επιβλέπει, να διενεργεί τακτικούς ελέγχους και να υποστηρίζει όλες τις λειτουργικές οντότητες κάτω από το δίκτυο της (YE, ΥΕΠ, ΥΔΑ, ΤYY, κ.λ.π.) ώστε αυτές να συμμορφώνονται με τους όρους και τις προϋποθέσεις που τίθενται από τον παρόντα Κανονισμό Πιστοποίησης.

2.1.1.2 Υποχρεώσεις της Υπηρεσίας Εγγραφής

Η ‘Υπηρεσία Εγγραφής’ (YE) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, αλλά και κάθε συμβεβλημένη YE του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, υπόκειται στις εξής υποχρεώσεις:

1) Να ελέγχει τις αιτήσεις των συνδρομητών που παραλαμβάνει από τις συνεργαζόμενες ‘Τοπικές Υπηρεσίες Υποβολής’ και να προχωρεί στην έγκρισή τους εντός το πολύ πέντε (5) εργάσιμων ημερών από την παραλαβή τους εφόσον αυτές πληρούν τους όρους και τις προϋποθέσεις που προβλέπονται στον Κανονισμό και στην Πολιτική του σχετικού πιστοποιητικού.

2) Να επιβεβαιώνει ή να εξασφαλίζει - με την συνεργασία της ‘Υπηρεσίας Προετοιμασίας Φορέα Συνδρομητών’ - την κατοχή των ‘δεδομένων δημιουργίας υπογραφής’ (ιδιωτικών κλειδιών) από τον πιστοποιούμενο συνδρομητή (*Proof of Possession*).

3) Να δίνει την σχετική εντολή στην ‘Υπηρεσία Εκδοσης Πιστοποιητικών’ για έκδοση του σχετικού πιστοποιητικού παρέχοντάς της, πλήρεις και ακριβείς πληροφορίες για τα στοιχεία που θα περιλαμβάνονται στο πιστοποιητικό.

4) Να συνεργάζεται με την ‘Υπηρεσία Διαχείρισης Ανάκλησης’ για την απαιτούμενη εξακρίβωση της ταυτότητας του συνδρομητή κατά τις αιτήσεις του για παύση, ανάκληση ή ενεργοποίηση των πιστοποιητικών του.

5) Να διατηρεί αρχείο με τις αιτήσεις, τις συμβάσεις και τα δικαιολογητικά έγγραφα των συνδρομητών των οποίων ενέκρινε την έκδοση πιστοποιητικών για το χρονικό διάστημα που ορίζεται στον Κανονισμό και στην Πολιτική του κάθε πιστοποιητικού (δες Κεφάλαιο 2.6 ‘Πολιτική Αρχειοθέτησης Πληροφοριών’).

2.1.1.3 Υποχρεώσεις της Υπηρεσίας Έκδοσης Πιστοποιητικών

Στο πλαίσιο της ‘Υπηρεσίας Έκδοσης Πιστοποιητικών’ (ΥΕΠ) της, η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ, αλλά και κάθε ΥΕΠ του δικτύου της, εκδίδονται πιστοποιητικά ‘τελικών οντοτήτων’, αναλαμβάνει τις εξής υποχρεώσεις:

1) Να εκδίδει τα πιστοποιητικά συμμορφούμενη με τον παρόντα Κανονισμό Πιστοποιήσεων και την σχετική Πολιτική των πιστοποιητικών, και να περιλαμβάνει στα πιστοποιητικά ακριβώς τα στοιχεία που ελέχθησαν και εγκρίθηκαν από τις συνεργαζόμενες ‘Υπηρεσίες Εγγραφής’.

2) Να δημοσιεύει στο ‘ηλεκτρονικό αποθετήριο’ (*repository*) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (μέσω της συνεργαζόμενης ‘Υπηρεσίας Δημοσίευσης’) κατάλογο με τα εκδοθέντα πιστοποιητικά, και να συνεργάζεται με την σχετική ‘Υπηρεσία Προετοιμασίας Φορέα Συνδρομητών’ για την εγγραφή των πιστοποιητικών αυτών στον τυχόν απαιτούμενο φορέα ‘α.δ.δ.ν.’ του συνδρομητή.

3) Να υπογράφει τις δημοσιευόμενες ‘Λίστες Ανακληθέντων Πιστοποιητικών’ (‘ΛΑΠ’ ή ‘CRL’) που αφορούν τα πιστοποιητικά που εξέδωσε, όπως αυτές διαμορφώνονται από την σχετική ‘Υπηρεσία Διαχείρισης Ανακλήσεων’.

4) Να ελέγχει τα αρχεία της για τυχόν προηγούμενη έκδοση πιστοποιητικού με τα ίδια δεδομένα επαλήθευσης υπογραφής (προς την ίδια ή άλλη οντότητα) και να αποτρέπει έτσι διπλή πιστοποίηση πιθανών ίδιων κλειδιών στο περιβάλλον της.

5) Να καταγράφει και να αρχειοθετεί, με ηλεκτρονικά μέσα, ακριβές ημερολόγιο με όλες τις σημαντικές κινήσεις που αφορούν κάθε εκδοθέν από αυτήν πιστοποιητικό (έκδοση, παύση, επαναφορά, ανάκληση κ.λ.π.) για το χρονικό διάστημα που ορίζεται στον Κανονισμό και στην Πολιτική του κάθε πιστοποιητικού (δες Κεφάλαιο 2.6 ‘Πολιτική Αρχειοθέτησης Πληροφοριών’).

2.1.1.4 Υποχρεώσεις της ‘Υπηρεσίας Προετοιμασίας Φορέα Συνδρομητών’

Η ‘Υπηρεσία Προετοιμασίας Φορέα Συνδρομητών’ (ΥΠΦΣ) του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, έχει τις εξής υποχρεώσεις:

1) Να δημιουργεί δεδομένα δημιουργίας και επαλήθευσης ηλεκτρονικής υπογραφής (ζεύγη ιδιωτικών και δημοσίων κλειδιών) και να τα αποθηκεύει σε εξατομικευμένους φορείς για τους συνδρομητές με ‘ασφαλή διάταξη δημιουργίας υπογραφής’ (‘α.δ.δ.ν.’), σύμφωνα με τα αναγνωρισμένα νομικοτεχνικά και επιχειρηματικά πρότυπα, συνεργαζόμενη στην προμήθεια των φορέων αυτών με τις σχετικές ‘Τοπικές Υπηρεσίες Υποβολής’.

2) Να αποστέλλει στην ‘Υπηρεσία Εγγραφής’ το δημιουργηθέν δημόσιο κλειδί που θα πιστοποιηθεί για τον συνδρομητή και να αποθηκεύουν στον εξατομικευμένο φορέα το σχετικό ηλεκτρονικό πιστοποιητικό που παραλαμβάνουν από την ‘Υπηρεσία Έκδοσης Πιστοποιητικών’, εφόσον αυτό εκδοθεί.

3) να τηρούν κάθε προβλεπόμενη από τον Κανονισμό και τις σχετικές Πολιτικές Πιστοποιητικών διαδικασία για την μη έκθεση και την μη αντιγραφή του ιδιωτικού κλειδιού του συνδρομητή καθώς και για την ασφαλή μεταφορά του φορέα και του κωδικού ενεργοποίησής του σ’ αυτόν.

2.1.1.5 Υποχρεώσεις της Υπηρεσίας Δημοσίευσης - ‘Ηλεκτρονικού Αποθετηρίου’

Η ‘Υπηρεσία Δημοσίευσης’ (ΥΔ) του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, μέσω του ‘Ηλεκτρονικού Αποθετηρίου’ (*Repository*) που παρέχει και συντηρεί (δες σχετικά παράγραφο 2.3.1), έχει τις εξής υποχρεώσεις:

1) Να δημοσιεύει εγκαίρως στο ‘Ηλεκτρονικό Αποθετήριο’ όλη την ισχύουσα τεκμηρίωση των ‘Υπηρεσιών Ψηφιακής Πιστοποίησης’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (όπως Κανονισμός Πιστοποίησης, Πολιτικές Πιστοποιητικών, Συμβάσεις κ.λ.π.), καθώς και τις τυχόν προηγούμενες σημαντικές εκδόσεις των κειμένων αυτών.

2) Να δημοσιεύει και παρέχει προς μεταφόρτωση (*download*) από οποιονδήποτε όλα τα ‘πιστοποιητικά CA’ του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (το βασικό πιστοποιητικό του ΘΕΠ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ και τα πιστοποιητικά όλων των ‘Λειτουργικών Εκδοτών Πιστοποιητικών’ του δικτύου) που είναι απαραίτητα για την σύνθεση της ‘Αλυσίδας Εμπιστοσύνης’ (*Trusted Path*) που επιβεβαιώνει την γνησιότητα των πιστοποιητικών των τελικών οντοτήτων (συνδρομητών) του δικτύου.

3) Να παρέχει, μέσα από τις σελίδες του ‘Ηλεκτρονικού Αποθετηρίου’ της, συνδέσμους (*links*) προς τους δημόσιους καταλόγους (*Directories*) των εκδοθέντων πιστοποιητικών του δικτύου και τις ‘Λίστες Ανακληθέντων Πιστοποιητικών’ (‘ΛΑΠ’ ή ‘CRLs’) που αφορούν τα πιστοποιητικά αυτά.

2.1.1.6 Υποχρεώσεις της Υπηρεσίας Διαχείρισης Ανάκλησης

Η ‘Υπηρεσία Διαχείρισης Ανάκλησης’ (ΥΔΑ) που λειτουργεί στα πλαίσια του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, υποχρεούται τα εξής:

1) Να διατηρεί σε συνεχή λειτουργία ηλεκτρονικούς καταλόγους (*Directories*) με ενημερωμένες ‘Λίστες Ανακληθέντων Πιστοποιητικών’ (‘ΛΑΠ’ ή *Certificate Revocation Lists - ‘CRLs’*) της συνεργαζόμενης ΥΕΠ που εξέδωσε τα αναφερόμενα σ’ αυτές ανακληθέντα (ή παυθέντα) πιστοποιητικά.

2) Να συνεργάζεται με την ‘*Υπηρεσία Εγγραφής*’ για την απαιτούμενη εξακρίβωση της ταυτότητας του συνδρομητή κατά τις αιτήσεις του για παύση, ανάκληση ή ενεργοποίηση των πιστοποιητικών του.

3) Να ενημερώνουν άμεσα τη σχετική ΥΕΠ και τον συνδρομητή (στην περίπτωση που το αγνοεί) για οποιαδήποτε περίπτωση (π.χ. υποψία για έκθεση ιδιωτικών κλειδιών ή εξακριβωμένη αίτηση) που επιβάλλει την παύση ή την ανάκληση κάποιου πιστοποιητικού σύμφωνα με τον παρόντα Κανονισμό.

4) Να ικανοποιεί τις αιτήσεις για ανάκληση, παύση ή ενεργοποίηση πιστοποιητικών **άμεσα μετά** από την παραλαβή και εξακρίβωση της σχετικής αίτησης, σύμφωνα με τους ιδιαίτερους όρους του παρόντος Κανονισμού και της Πολιτικής του συγκεκριμένου πιστοποιητικού. Σε περίπτωση άμεσης ανάγκης η διαδικασία γίνεται μέσω της τηλεφωνικής γραμμής επείγουσας ανάκλησης πιστοποιητικών +30 6951007878.

2.1.2 ΥΠΟΧΡΕΩΣΕΙΣ ΤΩΝ ΤΟΠΙΚΩΝ ΥΠΗΡΕΣΙΩΝ ΥΠΟΒΟΛΗΣ (Τ.Υ.Υ.)

Οι Τοπικές Υπηρεσίες Υποβολής (Τ.Υ.Υ), ως ανεξάρτητοι φορείς που αναλαμβάνουν τον συγκεκριμένο ρόλο συμβαλλόμενες με το δίκτυο του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, αποδέχονται τις παρακάτω υποχρεώσεις:

1) Να συμβάλλουν στην ενημέρωση και την εγγραφή των συνδρομητών τους, παρέχοντάς τους πληροφόρηση και το απαραίτητο έντυπο υλικό που διανέμεται από τις ‘*Υπηρεσίες Ψηφιακής Πιστοποίησης*’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

2) Να συγκεντρώνουν και να συνυπογράφουν τις συμπληρωμένες φόρμες ‘*Αίτησης & Σύμβασης Συνδρομητή*’ του περιβάλλοντός τους και να τις στέλνουν (εντός εύλογου χρόνου) στην συνεργαζόμενη ‘*Υπηρεσία Εγγραφής*’ προς έγκριση, σύμφωνα με τους όρους του παρόντος Κανονισμού.

3) Να προμηθεύουν την ‘*Υπηρεσία Προετοιμασίας Φορέα Συνδρομητών*’ (ή να έχουν ορίσει στην σύμβασή τους το τρόπο προμήθειάς της) με τους τυχών απαιτούμενους φορείς ‘ασφαλούς διάταξης δημιουργίας υπογραφής’ (π.χ. έξυπνες κάρτες) για τους προτεινόμενους συνδρομητές τους.

4) Να ενημερώνουν αμέσως την ‘*Υπηρεσία Διαχείρισης Ανάκλησης*’ για κάθε (προσδιοριζόμενη στον παρόντα Κανονισμό και την σχετική Πολιτική Πιστοποιητικού) περίπτωση ή αίτηση που έχει υποπέσει στην αντίληψή τους και απαιτεί την αναστολή, ενεργοποίηση ή ανάκληση ενός πιστοποιητικού.

2.1.3 ΥΠΟΧΡΕΩΣΕΙΣ ΤΟΥ ΣΥΝΔΡΟΜΗΤΗ

Ο συνδρομητής (κάτοχος πιστοποιητικού) των ‘*Υπηρεσιών Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ*’, είτε ως το ίδιο το υποκείμενο της πιστοποίησης (στα προσωπικά πιστοποιητικά), είτε ως κύριος ενός πιστοποιούμενου αντικειμένου (π.χ. στα πιστοποιητικά ‘*Trust-ServerTM*’), έχει τις εξής υποχρεώσεις:

1) Να είναι ενημερωμένος και να γνωρίζει καλά πώς χρησιμοποιούνται τα δεδομένα δημιουργίας υπογραφής, τα ηλεκτρονικά πιστοποιητικά και οι φορείς αυτών, και γενικότερα να κατανοεί την λειτουργία της ‘*υποδομής δημοσίων κλειδιών*’ (PKI) πριν προβεί σε οποιαδήποτε σχετική ενέργεια ή χρήση του πιστοποιητικού του.

2) Να έχει διαβάσει, κατανοήσει και συμφωνήσει με όλους τους όρους και τις προϋποθέσεις που περιλαμβάνονται στον παρόντα Κανονισμό Πιστοποιήσεων του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ και στην σχετική Πολιτική του πιστοποιητικού που χρησιμοποιεί.

3) Να παράσχει ακριβείς πληροφορίες για τα στοιχεία που του ζητούνται τόσο για την έκδοση όσο και την ανανέωση ή την ανάκληση του πιστοποιητικού και να ελέγξει την ορθότητά τους στο εκδιδόμενο πιστοποιητικό πριν την χρήση του ή την χρήση των δεδομένων δημιουργίας υπογραφής που αντιστοιχούν σ’ αυτό.

4) Να ενημερώνει άμεσα την ‘*Υπηρεσία Διαχείρισης Ανάκλησης*’ ή την σχετική ‘*Τοπική Υπηρεσία Υποβολής*’ για κάθε μεταβολή των στοιχείων που έχει δηλώσει στην αίτησή του για την έκδοση

πιστοποιητικού καθώς και να ζητά άμεσα την αναστολή ή την ανάκληση του πιστοποιητικού του σε κάθε περίπτωση που υποψιάζεται ή γνωρίζει ότι κάποιος τρίτος απέκτησε πρόσβαση ή με οποιοδήποτε τρόπο εκτέθηκαν τα δεδομένα δημιουργίας της υπογραφής του.

5) Να χρησιμοποιεί για την δημιουργία υπογραφής αποκλειστικά τον εξατομικευμένο ‘φορέα ασφαλούς δημιουργίας υπογραφής’ (π.χ. smart card) που πιθανώς του έχει χορηγηθεί με τρόπο κατάλληλο και σύμφωνο με τις σχετικές οδηγίες και να μην προσπαθήσει να εξαγάγει τα δεδομένα δημιουργίας υπογραφής του σε άλλον φορέα.

6) Να προστατεύει τα ‘δεδομένα δημιουργίας υπογραφής’ (ιδιωτικά κλειδιά) του, τον φορέα τους και τον ‘κωδικό ενεργοποίησης’ (PIN) τους από απώλεια, αποκάλυψη ή έκθεσή τους σε τρίτους και γενικά από οποιαδήποτε μη εξουσιοδοτημένη ή μη νόμιμη χρήση τους.

7) Να αποτρέπει, με ποινή αποζημίωσης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ ή και οποιουδήποτε άλλου ζημιωθέντος τρίτου, πράξεις αλλοιώσης, τροποποίησης, παράνομης αντιγραφής ή/και κακόβουλης χρήσης των δεδομένων δημιουργίας υπογραφής, του πιστοποιητικού που του διέθεσε το δίκτυο υπηρεσιών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ και των πληροφοριών (καταλόγων, λίστες ανάκλησης, κείμενα κανονισμών και πολιτικών κ.λ.π.) που δημοσιεύει η ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ στο ηλεκτρονικό αποθετήριο της (*repository*), τα οποία στοιχειοθετούν επιχείρηση απάτης ή/και απειλούν την αρτιότητα και την αξιοπιστία των υπηρεσιών πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

2.1.4 ΥΠΟΧΡΕΩΣΕΙΣ ΤΟΥ ΧΡΗΣΤΗ (ΒΑΣΙΖΟΜΕΝΟ ΜΕΡΟΣ)

Ο χρήστης (βασιζόμενο μέρος) ενός πιστοποιητικού του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, πριν να αποφασίσει αν θα βασισθεί ή όχι στα περιεχόμενα του πιστοποιητικού ώστε να προβεί σε μία συγκεκριμένη πράξη, ενέργεια ή παράλειψη, ή να αποκτήσει δικαιολογημένη πεποίθηση για την γνησιότητα του υπογράφοντος και του υπογεγραμμένου εγγράφου (με την ευρεία έννοια), έχει τις εξής υποχρεώσεις:

1) Να ελέγξει την γνησιότητα και την τυχόν παύση ή ανάκληση του συγκεκριμένου πιστοποιητικού ανατρέχοντας στα ‘πιστοποιητικά CA’ και στις σχετικές ‘Λίστες Ανακληθέντων Πιστοποιητικών’ (ΛΑΠ) που δημοσιεύονται στο ‘ηλεκτρονικό αποθετήριο’ (*Repository*) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

2) Να ελέγξει αν η συγκεκριμένη χρήση του πιστοποιητικού που προτίθεται να προβεί, επιτρέπεται ή όχι από την σχετική Πολιτική του πιστοποιητικού, σύμφωνα με την οποία αυτό εκδόθηκε.

3) Να έχει λάβει γνώση για τα όρια ευθύνης, τις αποποίησεις και τον περιορισμό των εγγυήσεων που έχει δηλώσει ο εκδότης του πιστοποιητικού καθώς και για το χρονικό διάστημα αρχειοθέτησης των αποδεικτικών στοιχείων, όπως αυτά αναφέρονται στην πολιτική του συγκεκριμένου πιστοποιητικού και στη ‘Σύμβαση Χρήστη/Αποδέκτη’ που δημοσιεύει η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ και την οποία πρέπει να αποδεχθεί πριν από την οποιαδήποτε χρήση των υπηρεσιών της ο χρήστης.

ΠΡΟΣΟΧΗ! Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ και οι εξουσιοδοτημένοι συνεργάτες της στην παροχή των υπηρεσιών πιστοποίησης δεν αναλαμβάνουν καμιά ευθύνη απέναντι σε οποιουδήποτε χρήστη των πιστοποιητικών της, αν αυτός δεν συμμορφώθηκε με τις παραπάνω υποχρεώσεις του και η παράλειψή του αυτή είχε ως συνέπεια να ζημιωθεί με οποιοδήποτε τρόπο.

2.2 ΕΓΓΥΗΣΕΙΣ, ΑΠΟΠΟΙΗΣΕΙΣ & ΟΡΙΑ ΕΥΘΥΝΗΣ

2.2.1 ΕΓΓΥΗΣΕΙΣ

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ, ως πάροχος υπηρεσιών πιστοποίησης, **εγγυάται την ακρίβεια και την εγκυρότητα των πιστοποιητικών της** (σύμφωνα με τις προϋποθέσεις που ορίζονται στον παρόντα Κανονισμό Πιστοποιήσεων και στην Πολιτική του σχετικού πιστοποιητικού) έναντι οποιουδήποτε τρίτου που εύλογα βασίζεται σ' αυτά.

Συγκεκριμένα η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ, ανεξάρτητα από την διάρθρωση των υπηρεσιών της, **εγγυάται:**

- την ακρίβεια, κατά τη στιγμή της αρχικής ενεργοποίησής του, όλων των πληροφοριών που περιέχονται στο πιστοποιητικό, καθώς και την ύπαρξη όλων των στοιχείων που απαιτούνται για την έκδοσή του,

σύμφωνα με τα οριζόμενα στον παρόντα Κανονισμό Πιστοποίησης (Κ.Π.) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ και στην σχετική Πολιτική του Πιστοποιητικού (Π.Π.).

- ότι ο υπογράφων, η ταυτότητα του οποίου βεβαιώνεται στο πιστοποιητικό, κατά τη στιγμή της αρχικής ενεργοποίησής του πιστοποιητικού, κατείχε τα ‘δεδομένα δημιουργίας υπογραφής’ (ιδιωτικό κλειδί), που αντιστοιχούν στα αναφερόμενα ή καθοριζόμενα στο πιστοποιητικό ‘δεδομένα επαλήθευσης της υπογραφής’ (δημόσιο κλειδί).
- ότι αμφότερα τα δεδομένα δημιουργίας υπογραφής και επαλήθευσης υπογραφής (ιδιωτικό και δημόσιο κλειδί) που παρέχει η ίδια στους συνδρομητές/πιστοποιούμενούς της, μπορούν να χρησιμοποιηθούν συμπληρωματικά.
- ότι καταβάλλει κάθε εύλογη προσπάθεια ώστε να δημοσιεύονται οι ανακλήσεις των πιστοποιητικών της σύμφωνα με τους όρους και την διαδικασία που περιγράφεται στον παρόντα Κανονισμό Πιστοποίησης και την σχετική Πολιτική του κάθε πιστοποιητικού.

2.2.2 ΑΠΟΠΟΙΗΣΕΙΣ ΕΥΘΥΝΗΣ

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ, **δεν ευθύνεται** προς οποιονδήποτε ζημιωθέντα τρίτο, εφόσον δεν βαρύνεται με πταίσμα για την δυσλειτουργία ή την αστοχία που προκάλεσε την ζημιά στον τρίτο ή εάν οι πράξεις της ήταν σύμφωνες με τα οριζόμενα στον Κανονισμό Πιστοποίησεων (Κ.Π.) και τις Πολιτικές Πιστοποιητικών της (Π.Π.), ή εάν ο ίδιος ο ζημιωθείς ή άλλος - εκτός του δικτύου παροχής υπηρεσιών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ -, προκάλεσε την ζημιά παραβιάζοντας τους όρους και τις προϋποθέσεις των Κ.Π. και των σχετικών Π.Π. ή προξένησε με οποιαδήποτε λανθασμένη, απρόσφορη ή παράνομη πράξη του την ζημιά αυτή.

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ **δεν ευθύνεται** (και κατ' επέκταση ούτε και οι συνεργαζόμενοι μαζί της στην παροχή υπηρεσιών πιστοποίησης τρίτοι φορείς), και για τυχόν δυσλειτουργία των υπηρεσιών της σε περιπτώσεις **ανωτέρας βίας**, όπως ενδεικτικά σεισμοί, πλημμύρες, πυρκαγιές κ.λ.π., συμπεριλαμβανόμενων των περιπτώσεων διακοπής της παροχής ηλεκτρικού ρεύματος (black-out), προβλημάτων στα τηλεπικοινωνιακά δίκτυα και γενικότερα όλων των εξωτερικών εμποδίων που μπορεί να εμποδίσουν την ομαλή παροχή των υπηρεσιών της και δεν οφείλονται σε υπαιτιότητά της ούτε μπορούσαν να προβλεφθούν ή να περιοριστούν οι συνέπειές τους.

Επίσης η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ, εκτός αν διαφορετικά ορίζεται στον παρόντα Κανονισμό Πιστοποίησεων (Κ.Π.) ή στην Πολιτική του Πιστοποιητικού (Π.Π.), **δεν εγγυάται και ούτε ευθύνεται** για την προσφορότητα, την ποιότητα, την έλλειψη λάθους ή και την καταλληλότητα για συγκεκριμένο σκοπό για όλες τις παρεχόμενες ή προσφερόμενες από αυτήν υπηρεσίες, προϊόντα και τεκμηριώσεις. Οι προσφερόμενες υπηρεσίες και προϊόντα προς τους συνδρομητές της και τους τρίτους, παρέχονται από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ και το δίκτυο της ‘**ως έχουν**’, και η ευθύνη για το αν αυτά είναι κατάλληλα για τον σκοπό που επιθυμούν ή αν θα πρέπει να βασισθούν ή όχι σ' αυτά, **βαρύνοντας αποκλειστικά** τον συνδρομητή του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ ή τον τρίτο (αποδέκτη) που αποφασίζει να βασισθεί σ' αυτά.

Τέλος η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ **δεν ευθύνεται** για οποιαδήποτε έμμεση ή αποθετική ζημιά, ποινική ή πειθαρχική δίωξη ή τιμωρία, διαφυγόντα κέρδη ή οποιεσδήποτε άλλες έμμεσες συνέπειες προκληθούν σε οποιονδήποτε με αφορμή την χρήση ή την στήριξή του σε κάποιο πιστοποιητικό της.

2.2.3 ΕΞΑΙΡΕΣΗ ΕΥΘΥΝΗΣ ΓΙΑ ΣΥΓΚΕΚΡΙΜΕΝΕΣ ΔΡΑΣΤΗΡΙΟΤΗΤΕΣ

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ δεν συνιστά και δεν εγγυάται την χρήση των ηλεκτρονικών υπογραφών και των πιστοποιητικών που εκδίδει σε δραστηριότητες ιδιαίτερα επικίνδυνες ή που απαιτούν υψηλότατα επίπεδα ασφάλειας, όπως ενδεικτικά έλεγχος εναέριας κυκλοφορίας, διαχείριση κρίσιμων πληροφοριών και υποδομών για την ζωή και την περιθάλψη ασθενών, έλεγχος πυρηνικών συστημάτων, διαχείριση μονάδων παραγωγής ηλεκτρικής ενέργειας και γενικά τη λειτουργία συστημάτων των οποίων η πιθανή δυσλειτουργία τους θα επέφερε δυσανάλογα μεγάλες ζημιές σε σχέση με τις συνήθεις δραστηριότητες για τις οποίες προορίζεται η χρήση των εκδιδόμενων πιστοποιητικών σύμφωνα με τον παρόντα Κανονισμό.

2.2.4 ΑΝΩΤΑΤΑ ΟΡΙΑ ΕΥΘΥΝΗΣ ΤΟΥ ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ

Αν, παρά τις παραπάνω αποποιήσεις ευθύνης και τους περιορισμούς στις εγγυήσεις που προσφέρει η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ, προκύψει ευθύνη της για αποζημίωση σε οποιονδήποτε τρίτο ή συνδρομητή της, για πραγματικό σφάλμα ή παράλειψη, παραβίαση όρου, δυσλειτουργία ή ανακρίβεια στις παρεχόμενες υπηρεσίες της, το ανώτατο όριο ευθύνης που αναλαμβάνει η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ και όλο το δίκτυο των υπηρεσιών της, για κάθε ένα πιστοποιητικό και για ολόκληρη την διάρκεια ισχύος αυτού, δεν μπορεί να είναι αθροιστικά μεγαλύτερο από το ποσό που αναφέρεται ως «**Ανώτατο Όριο Ευθύνης του Π.Υ.Π.**» στην σχετική Πολιτική του ‘ζημιογόνου’ Πιστοποιητικού (Π.Π.), και το οποίο είναι ανάλογο με την ‘Κλάση’ και τις επιτρεπόμενες από αυτήν χρήσεις του συγκεκριμένου πιστοποιητικού.

2.2.5 ΠΟΛΙΤΙΚΗ ΑΣΦΑΛΙΣΗΣ

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ διατηρεί το δικαίωμα να ασφαλίζει ή όχι την αστική της ευθύνη που σχετίζεται με την έκδοση των πιστοποιητικών της και για ποσό ίσο (ή και μεγαλύτερο) με το «**Ανώτατο Όριο Ευθύνης**» του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ το οποίο αντιστοιχεί για κάθε είδος και κλάση εκδιδόμενου πιστοποιητικού της (και το οποίο αναφέρεται στην σχετική Πολιτική Πιστοποιητικού').

2.3 ΠΟΛΙΤΙΚΗ ΔΗΜΟΣΙΕΥΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

2.3.1 ΗΛΕΚΤΡΟΝΙΚΟ ΑΠΟΘΕΤΗΡΙΟ (REPOSITORY) ΤΟΥ ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ

Το ‘Ηλεκτρονικό Αποθετήριο’ (*repository*) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ είναι μια ελευθέρως προσβάσιμη ηλεκτρονική τοποθεσία, όπου η Υπηρεσία Δημοσίευσης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ συγκεντρώνει και δημοσιεύει σε ηλεκτρονική μορφή (μέσω σχετικών ‘συνδέσμων’ – ‘links’) **όλες τις κρίσιμες πληροφορίες** που αφορούν την παροχή των υπηρεσιών πιστοποίησης, όπως τα πιστοποιητικά του Θεμελιώδη Εκδότη (Root CA) και των Λειτουργικών Εκδοτών (Operational CAs) πιστοποιητικών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, ο Κατάλογος (*Directory*) των εκδόθεντων πιστοποιητικών των συνδρομητών, οι Λίστες με τα παυθέντα ή/και ανακληθέντα πιστοποιητικά (*CRLs*), η Συνοπτική Διακήρυξη των Υπηρεσιών (PDS), οι τρέχουσες και οι προηγούμενες εκδόσεις του Κανονισμού Πιστοποίησης και των υποστηριζόμενων Πολιτικών των Πιστοποιητικών, οι χρησιμοποιούμενες Συμβάσεις για τον συνδρομητή και τον αποδέκτη και άλλες χρήσιμες πληροφορίες.

Η ηλεκτρονική σελίδα που φιλοξενεί το ‘ηλεκτρονικό αποθετήριο’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ βρίσκεται στην διεύθυνση <http://www.athexgroup.gr/web/guest/digital-certificates> και είναι ελευθέρως προσβάσιμη από οποιονδήποτε ενδιαφερόμενο.

2.3.2 ΔΗΜΟΣΙΕΥΣΗ ΚΑΤΑΛΟΓΟΥ ΙΣΧΥΡΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Με την έκδοση και την ενεργοποίηση ενός πιστοποιητικού, δημοσιεύεται στο ‘ηλεκτρονικό αποθετήριο’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ **πλήρες αντίγραφο του εκδιδόμενου πιστοποιητικού**, διαθέσιμο για λήψη του (download) από οποιονδήποτε ενδιαφερόμενο, εκτός εάν ο συνδρομητής-κάτοχός του έχει εκφράσει ρητά την αντίθεσή του στην κοινόχρηστη δημοσίευση του.

Η δημοσίευση των πιστοποιητικών γίνεται είτε με το πρωτόκολλο LDAP είτε με άλλη αναγνώσιμη ηλεκτρονική μορφή που επιλέγει η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ.

2.3.3 ΔΗΜΟΣΙΕΥΣΗ ‘ΛΙΣΤΩΝ ΑΝΑΚΛΗΘΕΝΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ’ (Λ.Α.Π.)

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ δημοσιεύει στο ‘Ηλεκτρονικό Αποθετήριό’ της, τις περιοδικά εκδιδόμενες ‘**Λίστες Ανακληθέντων Πιστοποιητικών**’ – (‘Λ.Α.Π.’ ή ‘Certificate Revocation Lists’ – ‘CRLs’) με όλα τα προσωρινά (παυθέντα) ή οριστικάς ανακληθέντα πιστοποιητικά.

Οι λίστες αυτές ανανεώνονται σε τακτά χρονικά διαστήματα, είτε παραμένουν αναλλοίωτες είτε υπάρχει τροποποίησή τους (πχ. ανάκλησης πιστοποιητικού). Σε κάθε περίπτωση όμως, κάθε προσωρινή (παύση) ή οριστική ανάκληση πιστοποιητικού δημοσιεύεται -ακόμη και με έκτακτη δημοσίευση νέας λίστας- άμεσα μετά την εξέταση της εξακριβωμένης αίτησης ή διαπίστωση ικανού λόγου για την ανάκληση ή την παύση του πιστοποιητικού.

Σε περίπτωση άμεσης ανάγκης η διαδικασία γίνεται μέσω της τηλεφωνικής γραμμής επείγουσας ανάκλησης πιστοποιητικών +30 6951007878.

Η δημοσίευση των λιστών ανακληθέντων πιστοποιητικών (ΛΑΠ) γίνεται με το πρωτόκολλο ‘LDAP’ είτε με άλλη αναγνώσιμη ηλεκτρονική μορφή που επιλέγει η Χ.Α, σύμφωνα και με τα οριζόμενα στο Κεφάλαιο 5.2 ‘Περιγραφή της Λ.Α.Π.’.

2.3.4 ΔΗΜΟΣΙΕΥΣΗ ΚΑΝΟΝΙΣΜΟΥ ΠΙΣΤΟΠΟΙΗΣΗΣ & ΠΟΛΙΤΙΚΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Όλες οι εκδόσεις του ‘Κανονισμού Πιστοποίησης’ και των ‘Πολιτικών Πιστοποιητικών’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (ισχύουσες & προηγούμενες), καθώς και μια ‘Συνοπτική Διακήρυξη των Υπηρεσιών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ’ (που περιλαμβάνει περίληψη των βασικότερων όρων του Κανονισμού και των Πολιτικών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ) δημοσιεύονται σε **ηλεκτρονική μορφή** (αρχεία .pdf, .doc ή .html) στο ‘Ηλεκτρονικό Αποθετήριο’ (Repository) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

Ηλεκτρονικές ή **εκτυπωμένες μορφές** του ισχύοντος ‘Κανονισμού Πιστοποίησης’ και των υποστηριζόμενων Πολιτικών Πιστοποιητικών είναι επίσης διαθέσιμες από τις συνεργαζόμενες Τ.Υ.Υ. και από την έδρα του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (δες λεπτομέρειες Επικοινωνίας στην παράγραφο 1.2.5). Παράλληλα, μαζί με κάθε έντυπο ‘Αίτηση - Συνδρομητική Σύμβαση’ για την απόκτηση οποιουδήποτε πιστοποιητικού του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ **διανέμεται υποχρεωτικά** -σε έντυπη μορφή και στην γλώσσα (Ελληνική ή Αγγλική) που ο επιθυμεί ο υποψήφιος συνδρομητής- η ‘Συνοπτική Διακήρυξη των Υπηρεσιών’ (P.D.S.) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

Αναθεωρήσεις ή τροποποιήσεις του Κ.Π. που έχουν εγκριθεί από την ‘Επιτροπή Διαχείρισης Πολιτικής’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, δημοσιεύονται στο ηλεκτρονικό αποθετήριο του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ **τουλάχιστον σαράντα πέντε (45) ημέρες** πριν από την ενεργοποίησή τους και την θέση τους σε ισχύ.

2.3.5 ΑΣΦΑΛΗΣ ΔΙΑΝΟΜΗ ΔΗΜΟΣΙΟΥ ΚΛΕΙΔΙΟΥ

Η ηλεκτρονική σελίδα που φιλοξενεί το ‘ηλεκτρονικό αποθετήριο’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ βρίσκεται στην διεύθυνση <http://www.athexgroup.gr/web/guest/digital-certificates> **και περιέγει το δημόσιο κλειδί.**

2.4 ΠΟΛΙΤΙΚΗ ΟΝΟΜΑΣΙΑΣ ΥΠΟΚΕΙΜΕΝΩΝ

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ, στην παρούσα φάση, δεν επιτρέπει την αναγραφή ‘ψευδωνύμων’ στα πιστοποιητικά που εκδίδει και για τον λόγο αυτό **όλα τα ονόματα των υποκειμένων που περιλαμβάνονται στα πιστοποιητικά της πρέπει να αντιστοιχούν σε επιβεβαιωμένες και κατανοητές ονομασίες, όπως το ονοματεπώνυμο του φυσικού προσώπου (ή του νόμιμου εκπρόσωπου του νομικού προσώπου) ή/και η ονομασία της εκπροσωπούμενης εταιρίας.**

Από την άλλη πλευρά, για λόγους διεθνούς συμβατότητας των πιστοποιητικών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, όλα τα ονόματα που αναγράφονται σε αυτά είναι εκφρασμένα σε **λατινικούς χαρακτήρες** με μετατροπή (transcription) των ελληνικών χαρακτήρων σύμφωνα με το πρότυπο [ΕΛΟΤ 743], **ή στην Αγγλική γλώσσα όπως αυτό προκύπτει από επίσημο έγγραφο (π.χ. διαβατήριο)**, ή μεταφρασμένα **στην Αγγλική γλώσσα** -όπου είναι δυνατόν να εφαρμοστεί.

Περισσότερες πληροφορίες για τον τύπο και την μορφή των ονομάτων αναφέρονται στην παράγραφο 5.1.3 (στο κεφάλαιο ‘ΠΕΡΙΓΡΑΦΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ’) ενώ λεπτομέρειες για το περιεχόμενο των πεδίων των ονομάτων των υποκειμένων (‘subjects’) των πιστοποιητικών και την σχετική σημασία τους αναφέρονται στην σχετική Πολιτική του κάθε εκδιδόμενου πιστοποιητικού.

2.5 ΠΟΛΙΤΙΚΗ ΠΡΟΣΤΑΣΙΑΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΛΟΜΕΝΩΝ

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ συλλέγει, επεξεργάζεται, δημοσιοποιεί και αρχειοθετεί δεδομένα προσωπικού χαρακτήρα των συνδρομητών της στο πλαίσιο της εκπλήρωσης των προβλεπομένων στο παρόν

και στις οικείες συμβάσεις και της συμμόρφωσης προς τα προβλεπόμενα στο οικείο κανονιστικό πλαίσιο. Τα δεδομένα προσωπικού χαρακτήρα που συλλέγονται και υποβάλλονται σε περαιτέρω επεξεργασία, όπως αυτή ορίζεται στην οικεία νομοθεσία (ν. 2472/97) αφορά τα δεδομένα τα οποία είναι απαραίτητα για την παροχή προς τους συνδρομητές των υπηρεσιών πιστοποίησης και για την εμπορική συναλλαγή τους με το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ. Τα δεδομένα προσωπικού χαρακτήρα συλλέγονται αποκλειστικά από τους ίδιους τους συνδρομητές κατά την διαδικασία εγγραφής ή ανανέωσής της συνδρομής τους και διατηρούνται ακόμη και μετά την λήξη ή την ανάκληση των πιστοποιητικών τους (δες Κεφάλαιο 2.6 ΠΟΛΙΤΙΚΗ ΑΡΧΕΙΟΘΕΤΗΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ) ώστε να χρησιμοποιηθούν ιδίως για την παροχή **αποδεικτικών στοιχείων** σε τυχόν ‘διαδικασίες επίλυσης διαφορών’ σχετικές με την πιστοποίησή τους και για όσο διάστημα είναι αυτό αναγκαίο για την εκπλήρωση αυτών των σκοπών λαμβάνοντας ταυτόχρονα υπόψη τις ιδιαίτερες απαιτήσεις του κανονιστικού πλαισίου για τις ηλεκτρονικές υπογραφές, όπως οι υποχρεώσεις αρχειοθέτησης πληροφοριών.

Η συλλογή των προσωπικών δεδομένων από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ είναι σύμφωνη με τους όρους του ν. 2472/1997, όπως ισχύει για την προστασία του ατόμου από την επεξεργασία δεδομένων προσωπικού χαρακτήρα και του ν. 3471/06 για την προστασία των δεδομένων προσωπικού χαρακτήρα στον τομέα των ηλεκτρονικών επικοινωνιών. Τα δεδομένα αυτά **δεν χρησιμοποιούνται για άλλους σκοπούς**, εκτός και αν υπάρχει ρητή (και έγγραφη) συγκατάθεση του υποκειμένου κατά τα οριζόμενα στο ν. 2472/97.

Ο συνδρομητής, κατά την απόλυτη κρίση του που εκφράζεται με δήλωσή του στην αίτηση πιστοποίησης (και που μπορεί να τροποποιηθεί και αργότερα με νέα έγγραφη δήλωσή του προς το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ), μπορεί να επιτρέψει ή όχι την δημοσίευση αντιγράφου του προσωπικού πιστοποιητικού του (και άρα των προσωπικών δεδομένων του που αναγράφονται σ' αυτό) στον **κοινόχρηστο Κατάλογο (Directory)** του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ που γίνεται για λόγους ευκολότερης επιβεβαίωσης της ηλεκτρονικής υπογραφής του από τρίτους.

Η ΧΑ ενημερώνει τους συνδρομητές για τα οριζόμενα στο άρθρο 11 του ν. 2472/97 στοιχεία. Σε κάθε περίπτωση ο συνδρομητής έχει δικαίωμα να απευθυνθεί στην ‘Υπηρεσία Εγγραφής’ του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (η οποία αποτελεί για την περίπτωση του ‘Υπεύθυνο Επεξεργασίας των δεδομένων του’) για να ασκήσει το δικαίωμα πρόσβασης σύμφωνα με το άρθρο 12 του ν. 2472/1997.

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ διατηρεί το δικαίωμα, και οι συνδρομητές της, αφού προηγουμένως ενημερωθούν, συναίνούν ρητά, να μεταβιβάζει το σύνολο των τηρούμενων αρχείων της σε τρίτο φορέα της επιλογής της, στην περίπτωση παύσης, για τη μεταβίβαση σε αυτόν των σχετικών δραστηριοτήτων της.

2.6 ΠΟΛΙΤΙΚΗ ΑΡΧΕΙΟΘΕΤΗΣΗΣ ΠΛΗΡΟΦΟΡΙΩΝ

Με την λήξη ή την ανάκληση ενός ‘αναγνωρισμένου πιστοποιητικού’ που είχε εκδοθεί από τις Υπηρεσίες Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, **αρχειοθετούνται για μια περίοδο τριάντα (30) ετών** τα εξής στοιχεία:

- Σε ηλεκτρονική μορφή, το ίδιο το πιστοποιητικό του συνδρομητή καθώς και ‘ημερολόγιο σημαντικών κινήσεων’ (*logs*) για αυτό το πιστοποιητικό (όπως παύση, ανάκληση ή ενεργοποίηση πιστοποιητικού, οι ανανέωσεις τους κ.λ.π.).
- Σε έντυπη ή ηλεκτρονική μορφή, όλα τα έγγραφα ταυτοποίησης και η υπογεγραμμένη ‘Αίτηση-Συνδρομητική Σύμβαση’ του συνδρομητή, καθώς και στοιχεία για κάθε αίτηση παύσης, ανάκλησης, ή επαναφοράς, επίλυσης διαφοράς ή διευθέτησης παραπόνων σχετικά με το πιστοποιητικό αυτό.

Παράλληλα διατηρούνται, για το ίδιο διάστημα, στοιχεία για όλες τις ‘Λίστες Ανακληθέντων Πιστοποιητικών’ (Λ.Α.Π.) που εκδόθηκαν και υπογράφθηκαν από τους Εκδότες ‘αναγνωρισμένων’ πιστοποιητικών.

Η αρχειοθέτηση αυτή είναι υποχρεωτική για τα ‘αναγνωρισμένα πιστοποιητικά’ για τις ηλεκτρονικές υπογραφές και έχει ως σκοπό την **δυνατότητα παροχής αποδεικτικών στοιχείων πιστοποίησης σε διαδικασίες επίλυσης διαφορών**.

Για τα **υπόλοιπα πιστοποιητικά** ('μη αναγνωρισμένα') η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ υποχρεούται να αρχειοθετεί ανάλογα δεδομένα για μια περίοδο πέντε (5) ετών από την λήξη ή την ανάκλησή τους, εκτός αν ορίζεται διαφορετικά στην συγκεκριμένη Πολιτική του πιστοποιητικού.

Καμία εγγύηση για την δυνατότητα επίλυσης διαφορών (δες αμέσως επόμενο Κεφάλαιο) σχετικά με ένα πιστοποιητικό του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ δεν δίνεται στον συνδρομητή-πιστοποιούμενο ή στον οποιοδήποτε τρίτο που βασίσθηκε στο πιστοποιητικό αυτό, μετά το πέρας της παραπάνω περιόδου.

2.7 ΠΟΛΙΤΙΚΗ ΕΠΙΛΥΣΗΣ ΔΙΑΦΟΡΩΝ

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, μέσω της 'Επιτροπής Διευθέτησης Παραπόνων και Επίλυσης Διαφορών' (ΕΔΠΕΔ), προσφέρει στους συνδρομητές της και στους βασιζόμενους στα πιστοποιητικά της τρίτους, **αξιόπιστες** (τόσο από νομική όσο και από τεχνική πλευρά) **πληροφορίες** και διευκρινίσεις για τα δεδομένα των επίμαχων πιστοποιητικών καθώς και **συμβουλές** για την ερμηνεία και την επίλυση πιθανών διαφορών που σχετίζονται με την πιστοποίηση και την χρήση των ηλεκτρονικών πιστοποιητικών της.

Για να κάνουν χρήση της διαμεσολαβητικής υπηρεσίας από την ΕΔΠΕΔ οι ενδιαφερόμενοι πρέπει να υποβάλλουν γραπτώς την διαφορά τους στην Επιτροπή, η οποία οφείλει να τους απαντήσει γραπτώς εντός το πολύ 30 ημερών από την λήψη της γραπτής αίτησης για τη διαμεσολάβηση.

Στην περίπτωση που η διαφορά στρέφεται εναντίον της ίδιας του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ ή τρίτου μέλους του δικτύου της στην παροχή υπηρεσιών πιστοποίησης (παράπονο), η Επιτροπή απαλλάσσεται από την υποχρέωση απάντησης στο αίτημα του ενδιαφερόμενου αν αυτός προβεί, πριν την λήξη της παραπάνω προθεσμίας των 30 ημερών, σε δικαστική ή άλλης μορφής διεκδίκηση κατά αυτών.

2.8 ΠΟΛΙΤΙΚΗ ΕΛΕΓΧΟΥ ΣΥΜΜΟΡΦΩΣΗΣ

2.8.1 ΕΘΕΛΟΝΤΙΚΗ ΔΙΑΠΙΣΤΕΥΣΗ ΚΑΙ ΔΙΑΠΙΣΤΩΣΗ

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ προτίθεται να υποβάλλει αίτηση για '**εθελοντική διαπίστευσή**' της στην Εθνική Επιτροπή Τηλεπικοινωνιών & Ταχυδρομείων – (Ε.Ε.Τ.Τ.) η οποία έχει αναλάβει από τον νόμο την εθελοντική διαπίστωση των Παρόχων Υπηρεσιών Πιστοποίησης στην Ελλάδα, εντός ενός εξαμήνου από την δημοσίευση του σχετικού Κανονισμού Εθελοντικής Διαπίστευσης της Ε.Ε.Τ.Τ..

2.9 ΠΟΛΙΤΙΚΗ ΤΙΜΟΛΟΓΗΣΗΣ & ΕΠΙΣΤΡΟΦΗΣ ΧΡΗΜΑΤΩΝ

Οι συνεργαζόμενες Τ.Υ.Υ. διαμορφώνουν ελεύθερα την δική τους Τιμολογιακή Πολιτική για τα τέλη εγγραφής και έκδοσης ή ανανέωσης των πιστοποιητικών που εκδίδονται από το δίκτυο των Υπηρεσιών Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, καθώς και για την τυχόν παροχή εξατομικευμένων φορέων 'α.δ.δ.υ.' προς τους συνδρομητές τους.

Οι υπηρεσίες παύσης και ανάκλησης πιστοποιητικού, οι υπηρεσίες καταλόγου εκδοθέντων πιστοποιητικών και οι υπηρεσίες ελέγχου της κατάστασης των πιστοποιητικών μέσω των δημοσιεύμενων 'Λιστών Ανακληθέντων Πιστοποιητικών' (ΛΑΠ) **παρέχονται δωρεάν.**

Σε περίπτωση μη έγκριση της αίτησης ενός υποψήφιου συνδρομητή από την Υ.Ε., αυτός δικαιούται την πλήρη επιστροφή των χρημάτων του από την Τ.Υ.Υ., στην οποία πιθανώς τα κατέβαλε.

Επίσης, στην περίπτωση που η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ προχωρήσει σε ανάκληση του πιστοποιητικού ενός συνδρομητή της χωρίς δική του υπαιτιότητα ή αίτηση, τότε η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ υποχρεούται **είτε** σε μερική επιστροφή στον συνδρομητή του ποσού της συνδρομής που κατέβαλε, **είτε** σε έκδοση νέου πιστοποιητικού, ανάλογα με το εναπομείναν -έως τη φυσιολογική λήξη του πιστοποιητικού- χρονικό διάστημα.

2.10 ΠΝΕΥΜΑΤΙΚΗ ΙΔΙΟΚΤΗΣΙΑ ΚΑΙ ΆΛΛΑ ΔΙΚΑΙΩΜΑΤΑ

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ διατηρεί όλα τα δικαιώματα πνευματικής και βιομηχανικής ιδιοκτησίας που έχει στις βάσεις δεδομένων της, στα περιεχόμενα των ηλεκτρονικών σελίδων της, στα ηλεκτρονικά πιστοποιητικά που εκδίδει, στα εμπορικά σήματα και λογότυπα καθώς και σε όλα τα κείμενα που δημοσιεύει.

Απαγορεύεται ρητά κάθε δημοσίευση ή αναπαραγωγή του συνόλου ή μέρους του παρόντος ή εν γένει εκμετάλλευσή του από τρίτους χωρίς σχετική γραπτή άδεια.

2.11 ΕΡΜΗΝΕΙΑ ΚΑΙ ΕΚΤΕΛΕΣΤΟΤΗΤΑ

2.11.1 ΕΝΣΩΜΑΤΩΣΗ ΜΕ ΑΝΑΦΟΡΑ ΣΕ ΆΛΛΑ ΚΕΙΜΕΝΑ

Ο παρών Κανονισμός Πιστοποίησης, μέσω της ‘**ενσωμάτωσής του με αναφορά**’, τόσο στις συμβάσεις του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ με τρίτους-συνεργαζόμενους στην πιστοποίηση φορείς όσο και στις ‘**Συνδρομητικές Συμβάσεις**’ με τους πιστοποιούμενους-κατόχους, καθώς και στις ‘**συμβάσεις αποδέκτη**’ με τους χρήστες (βασιζόμενα μέρη) των πιστοποιητικών της, διέπει, -μαζί με τους λοιπούς όρους της σύμβασης και τους όρους που αναφέρονται στην Πολιτική του σχετικού πιστοποιητικού-, τις σχέσεις του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ με κάθε συμβαλλόμενο μέρος.

2.11.2 ΣΥΓΚΡΟΥΣΗ ΔΙΑΤΑΞΕΩΝ ΚΑΙ ΣΕΙΡΑ ΙΣΧΥΟΣ

Σε τυχόν σύγκρουση της ερμηνείας των διατάξεων του ελληνικού κειμένου του Κανονισμού με τις αντίστοιχες του ίδιου κειμένου στην αγγλική ή σε άλλη γλώσσα, κατισχύει το ελληνικό κείμενο.

Σε περίπτωση ασυμφωνίας του Κανονισμού με όρους άλλων συμβατικών κειμένων, η σειρά ισχύος τους είναι η εξής: α) το κείμενο του παρόντος Κανονισμού Πιστοποίησης, β) το κείμενο της σχετικής Πολιτικής Πιστοποιητικού, και, γ) το κείμενο της ‘**Συνδρομητικής Σύμβασης**’ και της ‘**Σύμβασης Χρήστη/Αποδέκτη**’.

2.11.3 ΔΙΑΤΗΡΗΣΗ ΙΣΧΥΟΣ ΤΩΝ ΜΗ ΑΚΥΡΩΝ ΟΡΩΝ

Στην περίπτωση που κάποιος όρος ή διάταξη του παρόντος κανονισμού κριθεί άκυρος ή μη εφαρμοστέος για οποιοδήποτε λόγο, οι λοιπές διατάξεις του συνεχίζουν να ισχύουν ως έχουν, εκτός αν εξαιτίας του άκυρου όρου επηρεάζεται η ουσία του περιεχομένου των εναπομεινάντων όρων, οπότε και αυτοί ερμηνεύονται πλέον με τρόπο τέτοιο ώστε να είναι έγκυροι, εφαρμόσιμοι και στο μέτρο που είναι δυνατόν σύμφωνοι με το σκοπό του αρχικού κειμένου.

2.11.4 ΕΦΑΡΜΟΣΤΕΟ ΔΙΚΑΙΟ – ΑΡΜΟΔΙΑ ΔΙΚΑΣΤΗΡΙΑ

Το εφαρμοστέο δίκαιο είναι το ελληνικό και κάθε διαφορά που σχετίζεται με την παροχή των περιγραφόμενων στο παρόντα Κανονισμό υπηρεσιών ψηφιακής πιστοποίησης συμφωνείται ότι θα υπάγεται στην αποκλειστική αρμοδιότητα των Δικαστηρίων των Αθηνών.

ΜΕΡΟΣ ΙII: ΛΕΙΤΟΥΡΓΙΚΟΙ ΟΡΟΙ

3.1 ΑΙΤΗΣΗ ΚΑΙ ΕΓΚΡΙΣΗ ΕΚΔΟΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

3.1.1 ΠΟΙΟΙ ΚΑΙ ΠΩΣ ΜΠΟΡΟΥΝ ΝΑ ΑΙΤΗΘΟΥΝ ΤΗΝ ΕΚΔΟΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ

Αίτηση για έκδοση πιστοποιητικών από τις Υπηρεσίες Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ μπορούν να κάνουν **νομικοί εκπρόσωποι νομικών προσώπων** (για την έκδοση ‘προσωπικών πιστοποιητικών’ ή/και ‘πιστοποιητικών συσκευών’ της κυριότητάς τους), **είτε και νομικά πρόσωπα** (μόνο όμως για την έκδοση ‘πιστοποιητικών συσκευών’ της κυριότητάς τους) η ταυτότητα των οποίων είναι γνωστή σε μιας συνεργαζόμενη με το δίκτυο του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ ‘Τοπικής Υπηρεσίας Υποβολής’ (ΤΥΥ).

Για τον σκοπό αυτό οι υποψήφιοι συνδρομητές συμπληρώνουν και υπογράφουν την σχετική ‘*Αίτηση-Συνδρομητική Σύμβαση*’ που τους προμηθεύει η ΤΥΥ, παρέχοντας ταυτόχρονα και τα σχετικά δικαιολογητικά που αποδεικνύουν την ταύτισή τους ή την σχέση τους με το θέμα (υποκείμενο) του ζητούμενου πιστοποιητικού.

3.1.2 ΣΥΜΠΡΑΞΗ ΤΗΣ Τ.Υ.Υ. ΣΤΗΝ ΑΙΤΗΣΗ ΤΟΥ ΥΠΟΨΗΦΙΟΥ ΣΥΝΔΡΟΜΗΤΗ

Η συμβεβλημένη ΤΥΥ του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ υποχρεούται να συμπράξει κατά την υποβολή μιας αίτησης για έκδοση πιστοποιητικών από έναν υποψήφιο συνδρομητή.

Έτσι, ο αρμόδιος υπάλληλος (*Διαχειριστής*) της ΤΥΥ που παραλαμβάνει μια συμπληρωμένη αίτηση συνδρομητή, αφού ελέγξει πρόχειρα την ‘πληρότητά’ της (σύμφωνα με την Πολιτική του ζητούμενου πιστοποιητικού), **συνυπογράφει την αίτηση** και την στέλνει (μέσα σε σφραγισμένο φάκελο μαζί με την υπογεγραμμένη ‘Συνδρομητική Σύμβαση’ και τα προσκομισθέντα δικαιολογητικά του συνδρομητή) στην συνεργαζόμενη ‘*Υπηρεσία Εγγραφής*’ (ΥΕ) **προς έγκριση**.

3.1.3 ΕΓΚΡΙΣΗ ΑΠΟ ΤΗΝ ΥΠΗΡΕΣΙΑ ΕΓΓΡΑΦΗΣ

Η ΥΕ, έχοντας την ευθύνη για τον τελικό έλεγχο της αίτησης, και αφού προβεί σε ‘εξακρίβωση της ταυτότητας και της γνησιότητας’ του υποκειμένου της πιστοποίησης -σύμφωνα με το αμέσως επόμενο Κεφάλαιο-, **εγκρίνει ή απορρίπτει** την αίτηση **ή ζητά την συμπλήρωση** τυχόντων ελλείψεων άμεσα από τον αιτούντα, εντός το πολύ πέντε (5) εργάσιμων ημερών από την παραλαβή της αίτησης.

Στην περίπτωση έγκρισης της αίτησης, η ΥΕ συνεργάζεται με την ‘*Υπηρεσία Προετοιμασίας Φορέα Συνδρομητών*’ (ΥΠΦΣ) που δημιουργεί τα πιστοποιούμενα κλειδιά του συνδρομητή και **στέλνει την σχετική εντολή** με τις απαραίτητες πληροφορίες για τα περιεχόμενα (ονομασία ή περιγραφή υποκειμένου και το σχετικό δημόσιο κλειδί) του πιστοποιητικού που πρέπει να εκδοθεί στην ‘*Υπηρεσία Έκδοσης Πιστοποιητικών*’ (ΥΕΠ).

3.2 ΕΞΑΚΡΙΒΩΣΗ ΤΑΥΤΟΤΗΤΑΣ & ΓΝΗΣΙΟΤΗΤΑΣ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ

3.2.1 ΣΤΗΝ ΑΡΧΙΚΗ ΕΓΓΡΑΦΗ

Κατά την αρχική εγγραφή για την έκδοση ενός πιστοποιητικού, απαιτείται η φυσική παρουσία του Αιτούντα πιστοποιητικό στο ΧΑ (ή του νόμιμου εκπροσώπου του) στο αρμόδιο τμήμα και συγκεκριμένα στην ΥΕ. Η τελευταία πρέπει να προβεί σε **έλεγχο και εξακρίβωση** της ταυτότητας και της γνησιότητας του υποκειμένου (‘θέματος’) του πιστοποιητικού και της πραγματικής κατοχής από αυτόν (*Proof of Possession - POP*) των πιστοποιούμενων κλειδιών υπογραφής, σύμφωνα και με τα οριζόμενα στην σχετική Πολιτική του ζητούμενου πιστοποιητικού.

Για τον λόγο αυτό, κατά την αρχική εγγραφή, ζητούνται και ελέγχονται διεξοδικά από την ΥΕ του δικτύου, τα εξής στοιχεία:

- **Η νομιμοποίηση των συνδρομητών νομικών προσώπων** και των εκπροσώπων τους, βάσει των κατάλληλων νομιμοποιητικών εγγράφων (π.χ. καταστατικό, δημοσίευση ΦΕΚ, απόφαση Δ.Σ. κ.λ.π.),

3.2.2 ΣΤΗΝ ΑΙΤΗΣΗ ΑΝΑΚΛΗΣΗΣ & ΕΝΕΡΓΟΠΟΙΗΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ

Η αίτηση ανάκλησης μπορεί να πραγματοποιηθεί μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής, μέσω της οποίας πραγματοποιείται η διαχείριση του αναγνωρισμένου πιστοποιητικού. Επιπλέον, η αναστολή ή η ανάκληση του πιστοποιητικού μπορεί να πραγματοποιηθεί από το ΧΑ. εφόσον εξακριβώθουν τα στοιχεία του αιτούντος με έναν από τους ακόλουθους τρόπους:

- είτε με την αυτοπρόσωπη παρουσία του αιτούντος και με την επίδειξη επίσημου εγγράφου ταυτοποίησής του (π.χ. αστυνομικής ταυτότητας) ενώπιον της ‘Υπηρεσίας Διαχείρισης Ανάκλησης’ (ΥΔΑ) ή μιας ΤΥΥ του δικτύου,
- είτε με -ιδιοχείρως υπογεγραμμένη- γραπτή αίτηση του αιτούντα προς την ΥΔΑ του δικτύου,
- είτε (μόνο για την αίτηση ‘προσωρινής ανάκλησης’ (παύσης) του πιστοποιητικού) με απλή αντιπαράθεση των προσωπικών στοιχείων που δηλώνει ο αιτών-συνδρομητής με τα σχετικά στοιχεία που διατηρεί στο αρχείο της η ΥΕ του δικτύου.

(Σύμφωνα με τη σύσταση θα πρέπει να ζητείται και να ελέγχεται ότι ακριβώς και στην περίπτωση της αίτησης εγγραφής.)

3.2.3 ΣΤΗΝ ΑΝΑΝΕΩΣΗ ΤΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ

3.2.3.1 Φυσιολογική ανανέωση

Κατά την διαδικασία ‘φυσιολογικής’ ανανέωσης ενός πιστοποιητικού (δηλαδή, πριν από την προκαθορισμένη λήξη του ισχύοντος πιστοποιητικού) ο κάτοχος δύναται να πραγματοποιήσει την ανανέωση μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής διαχείρισης του αναγνωρισμένου πιστοποιητικού του.

Επιπλέον δίνεται η δυνατότητα ‘φυσιολογικής ανανέωσης’ ενός πιστοποιητικού (δηλαδή, πριν από την προκαθορισμένη λήξη του ισχύοντος πιστοποιητικού) μέσω κατάθεσης μίας ηλεκτρονικά υπογεγραμμένης ‘αίτησης ανανέωσης’ από τον συνδρομητή -βασιζόμενη στο ισχύον πιστοποιητικό του -, όπου ο συνδρομητής **θα δηλώνει** ότι δεν έχει τροποποιηθεί οποιοδήποτε από τα στοιχεία που περιέχονται στο προηγούμενο πιστοποιητικό του ή θα επισημάνει τις σχετικές αλλαγές.

3.2.3.2 Ανανέωση μετά από λήξη ή ανάκληση του πιστοποιητικού λόγω έκθεσης κλειδιών

Αναφορικά με την ανανέωση των πιστοποιητικών μετά από την λήξη τους ή την ανάκλησή τους λόγω έκθεσής τους σε κίνδυνο των σχετικών κρυπτογραφικών κλειδιών (λ.χ. κλοπή πιστοποιητικού), ο κάτοχος δύναται να χρησιμοποιήσει την ειδικά διαμορφωμένη διαδικτυακή εφαρμογή διαχείρισης του πιστοποιητικού του και εφόσον καταργήσει το προηγούμενο ανακληθέν ή ληγμένο πιστοποιητικό, να δημιουργήσει καινούργιο. Επιπλέον δίνεται η δυνατότητα χρήσης νέας ‘χειρόγραφης’ αίτησης του συνδρομητή με βεβαίωση για το γνήσιο της υπογραφής του χωρίς όμως να απαιτείται να προσκομίσει εκ νέου αντίγραφα των εγγράφων ταυτοποίησης του και επικαλεσθεί τα ίδια ισχύοντα έγγραφα ταυτοποίησης με αυτά που είχε προσκομίσει κατά την αρχική του εγγραφή. Σε περίπτωση δε που το εν λόγω πιστοποιητικό χρησιμοποιηθεί από νόμιμο εκπρόσωπο νομικού προσώπου, θα πρέπει να προσκομισθούν κατάλληλα νομιμοποιητικά έγγραφα (π.χ. καταστατικό, δημοσίευση ΦΕΚ, απόφαση Δ.Σ. κ.λ.π.), τα οποία θα αποδεικνύουν την σχέση του αιτούντα με το νομικό πρόσωπο.

3.2.3.3 Ανανέωση μετά από ανάκληση του πιστοποιητικού (όχι λόγω έκθεσης κλειδιών)

Κατά την διαδικασία ανανέωσης ενός πιστοποιητικού μετά από ανάκληση που προκλήθηκε για άλλον λόγο πλην της περίπτωσης της έκθεσης των κρυπτογραφικών κλειδιών του συνδρομητή (π.χ. στην περίπτωση ανάκλησης του πιστοποιητικού από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ λόγω μη έγκαιρης εκπλήρωσης των οικονομικών υποχρεώσεων από τον συνδρομητή) είναι δυνατόν να παρακαμφθεί η διαδικασία εξακρίβωσης της ταυτότητας του συνδρομητή που προβλέπεται κατά την αρχική εγγραφή και η ΥΕ να προβεί σε εντολή έκδοσης νέων πιστοποιητικών προς την ΥΕΠ, βασιζόμενη στα ήδη υπάρχοντα στοιχεία της αρχικής εγγραφής, εφόσον ο συνδρομητής δηλώνει την διατήρηση της ισχύος των.

(Σύμφωνα με τη σύσταση θα πρέπει να ζητείται και να ελέγχεται ότι ακριβώς και στην περίπτωση της αίτησης εγγραφής. Συνεπώς τα χρωμοσκιασμένα μέρη της αίτησης θα πρέπει να παραληφθούν.)

3.3 ΔΗΜΙΟΥΡΓΙΑ ΖΕΥΓΟΥΣ ΚΛΕΙΔΙΩΝ ΚΑΙ ΦΟΡΕΑΣ ‘Α.Δ.Δ.Υ.’

Οι συσκευές Α.Δ.Δ.Υ. που χρησιμοποιούνται από το Χ.Α. είναι σύμφωνες με τον κανονισμό eIDAS και περιλαμβάνονται στον κατάλογο των ασφαλών συσκευών που τηρεί η Ευρωπαϊκή Επιτροπή. Το Χ.Α. παρακολουθεί τακτικά τον κατάλογο για να διασφαλίσει ότι οι συσκευές Α.Δ.Δ.Υ. παραμένουν ασφαλείς. Με βάση την καθορισμένη ημερομηνία λήξης της συσκευής Α.Δ.Δ.Υ., όπως απεικονίζεται στον κατάλογο της Ε.Ε., το Χ.Α. δεν εκδίδει πιστοποιητικά συνδρομητών σε συσκευές Α.Δ.Δ.Υ., εάν η περίοδος ισχύος της συσκευής δεν καλύπτει ολόκληρη την περίοδο ισχύος του πιστοποιητικού συνδρομητή υπό έκδοση.

3.3.1 ΕΙΔΙΚΑ ΣΤΑ ΠΡΟΣΩΠΙΚΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ

3.3.1.1 Φορέας Έξυπνη Κάρτα

3.3.1.1.1 Δημιουργία και εναποθήκευση των κλειδιών σε φορέα ‘α.δ.δ.υ.’

Αμέσως μόλις η ΥΕ ελέγχει και εγκρίνει την αίτηση με τα απαραίτητα έγγραφα του αιτούντα που της έχουν σταλεί από την ΤΥΥ, ζητά από την ΥΠΦΣ την **δημιουργία κατάλληλου ζεύγους κρυπτογραφικών κλειδιών** (του οποίου το δημόσιο κλειδί θα περιληφθεί στο πιστοποιητικό) και την **ασφαλή εναπόθεσή** τους σε εξατομικευμένο για τον συνδρομητή φορέα ‘ασφαλούς διάταξης δημιουργίας υπογραφής’ (π.χ. έξυπνη κάρτα), ο οποίος παρέχεται για αυτόν το σκοπό από την συμπράξασα στην αίτηση ΤΥΥ. Επιπλέον ο Συνδρομητής έχει την δυνατότητα να χρησιμοποιήσει την ειδικά διαμορφωμένη διαδικτυακή εφαρμογή για την παραγωγή του Αναγνωρισμένου Πιστοποιητικού. Συνεπώς, η παραγωγή του εν λόγω αναγνωρισμένου πιστοποιητικού και των ασύμμετρων κρυπτογραφικών κλειδιών μεταφέρεται πλήρως στην πλευρά του Συνδρομητή.

3.3.1.1.2 Εξατομίκευση φορέα ‘α.δ.δ.υ.’ και καταγραφή ‘κωδικού ενεργοποίησής’ (PIN) του

Ο φορέας **εξατομικεύεται** από την ΥΠΦΣ με την έννοια ότι αναγράφεται στην επιφάνειά του το όνομα του συνδρομητή καθώς και ο μοναδικός ‘Προσωπικός Κωδικός Αναγνώρισής’ (Π.Κ.Α.) του, ο οποίος διακρίνει τον συγκεκριμένο συνδρομητή μέσα στο περιβάλλον του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

Παράλληλα, η ΥΠΦΣ εκτυπώνει σε **ειδικό αδιαφανή φάκελο** τον ‘κωδικό ενεργοποίησής’ (PIN) του φορέα και αναμένει την έκδοση και παραλαβή των συγκεκριμένων πιστοποιητικών από την ΥΕΠ ώστε να τα αποθηκεύσει και αυτά στον εξατομικευμένο φορέα του συνδρομητή.

Η παραπάνω διαδικασία, σε συνδυασμό με την ασφαλή αποστολή του φορέα και του ‘κωδικού ενεργοποίησής’ του στον πιστοποιούμενο, **εξασφαλίζει** την αποκλειστική κατοχή από τον συνδρομητή του συγκεκριμένου ιδιωτικού κλειδιού (*‘Proof of Possession’ – ‘POP’*) που αντιστοιχεί στο δημόσιο κλειδί που αναφέρεται στο πιστοποιητικό.

Επιπλέον στην περίπτωση δημιουργίας του Πιστοποιητικού από τον ίδιο τον συνδρομητή μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής, ο ‘κωδικός ενεργοποίησής’ (PIN), παράγεται αυτόματα και αποστέλλεται στον συνδρομητή μέσω αυτής.

3.3.1.1.3 Παράδοση του φορέα στον συνδρομητή

Η παράδοση του εξατομικευμένου φορέα που περιέχει τα ιδιωτικά κλειδιά και τα αντίστοιχα πιστοποιητικά, αλλά και του φακέλου με τον κωδικό ενεργοποίησής (PIN) του φορέα στον συνδρομητή, γίνεται **με ξεχωριστές συστημένες ταχυδρομικές αποστολές** στην διεύθυνση που έχει δηλώσει στην αίτησή του ο συνδρομητής.

Η αποστολή του φακέλου με το ‘PIN’ στον συνδρομητή γίνεται απ’ ευθείας από την ΥΠΦΣ, ενώ ο ίδιος ο φορέας μπορεί, εναλλακτικά, να παραδοθεί στον συνδρομητή και διαμέσου της σχετικής ΤΥΥ.

Επιπλέον στην περίπτωση δημιουργίας του Αναγνωρισμένου Πιστοποιητικού από τον ίδιο τον συνδρομητή μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής, η παράδοση του φορέα πραγματοποιείται από την Υπηρεσία Εγγραφής κατά την αρχική εγγραφή του και εφόσον έχει εγκριθεί η

αίτησή του. Αν ο συνδρομητής επιθυμεί, ο φορέας μπορεί να αποσταλεί με συστημένη ταχυδρομική επιστολή στην διεύθυνση που έχει δηλώσει κατά την αίτησή του.

3.3.1.2 Συσκευή απομακρυσμένης υπογραφής

Αμέσως μόλις η ΥΕ ελέγξει και εγκρίνει την αίτηση με τα απαραίτητα έγγραφα του αιτούντα που της έχουν σταλεί από την ΤΥΥ, ζητά από την ΥΠΦΣ να δημιουργήσει τον λογαριασμό του συνδρομητή στην ειδικά διαμορφωμένη εφαρμογή. Με την δημιουργία αποστέλλεται στον συνδρομητή ηλεκτρονικό μήνυμα (e-mail) με οδηγίες για την δημιουργία και ενεργοποίηση των πιστοποιητικών του καθώς και με τα διαπιστευτήρια (όνομα χρήστη, αρχικό κωδικό πρόσβασης) για πρόσβαση στην εφαρμογή της υπηρεσίας. Τα κλειδιά του συνδρομητή και τα σχετικά πιστοποιητικά δημιουργούνται από τον ίδιο τον συνδρομητή με χρήση του προσωπικού κωδικού πρόσβασης καθώς και του κωδικού μιας χρήστης (one time password – OTP) από συσκευή την οποία έχει εγγράψει στην υπηρεσία. Ο προσωπικός κωδικός πρόσβασης και ο κωδικός μιας χρήστης (OTP) είναι απαραίτητος για τη χρήση των ιδιωτικών κλειδιών και πιστοποιητικών που βρίσκονται στην συσκευή πιστοποιητικών σε κατοχή του ΠΥΠ (Remote Sign).

3.4 ΕΚΔΟΣΗ ΚΑΙ ΑΡΧΙΚΗ ΕΝΕΡΓΟΠΟΙΗΣΗ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

3.4.1 ΕΚΔΟΣΗ ΑΠΟ ΤΟΝ ΚΑΤΑΛΛΗΛΟ ΛΕΙΤΟΥΡΓΙΚΟ ΕΚΛΟΤΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Όταν μια ηλεκτρονικά υπογεγραμμένη εντολή για έκδοση πιστοποιητικού φθάσει από την ΥΕ στην ‘Υπηρεσία Έκδοσης Πιστοποιητικών’ (ΥΕΠ), η τελευταία προχωρεί υποχρεωτικά στην **έκδοση του συγκεκριμένου πιστοποιητικού**.

Η έκδοση και η υπογραφή του πιστοποιητικού γίνεται από τον κατάλληλο ‘*Υπο- Εκδότη Πιστοποιητικών*’ (*Subordinate ή Operational CA*) της υπηρεσίας, ο οποίος πρέπει να είναι εξουσιοδοτημένος να εκδίδει το συγκεκριμένο είδος πιστοποιητικών που αντιστοιχεί σε μία καθορισμένη ‘Πολιτική Πιστοποιητικών’ (*Certificate Policy* – ‘CP’).

3.4.2 ΔΙΑΔΙΚΑΣΙΑ ΑΡΧΙΚΗΣ ΕΝΕΡΓΟΠΟΙΗΣΗΣ ΤΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ

Κάθε πιστοποιητικό που εκδίδεται από το δίκτυο του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, αμέσως μετά την έκδοσή του τίθεται σε κατάσταση ‘**αναστολής**’ (προσωρινής ανάκλησης ή ‘παύσης’ –βλ. επόμενο κεφάλαιο 3.7) για λόγους ασφαλείας, ωστόυντα ενεργοποιηθεί με αίτηση του ίδιου του συνδρομητή, μετά την παραλαβή του.

Η διαδικασία για την αρχική ενεργοποίηση περιγράφεται στον συνδρομητή με την αποστολή **σχετικών οδηγιών** για τον τρόπο ενεργοποίησης ταυτόχρονα με την αποστολή του φορέα του πιστοποιητικού του.

Η αίτηση για αρχική ενεργοποίηση από τον συνδρομητή περιλαμβάνει την ηλεκτρονική, ταχυδρομική ή με τηλεομοιοτυπία (fax) αποστολή δήλωσης του συνδρομητή, η οποία περιέχει τα εξής σημεία:

- την αποδοχή από τον συνδρομητή της ορθότητας των στοιχείων που περιλαμβάνονται στο παραληφθέν πιστοποιητικό του,
- την διαβεβαίωση ότι την στιγμή εκείνη είναι κάτοχος τόσο του φορέα των ιδιωτικών κλειδιών που έχει οριστεί κατά την έκδοση του πιστοποιητικού, όσο και του σχετικού κωδικού ενεργοποίησής των.
- την διαβεβαίωση ότι είναι γνώστης των όρων και των προϋποθέσεων χρήσης του πιστοποιητικού που περιλαμβάνονται στον παρόντα Κανονισμό Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών (*CPS Q.C.*) και στο κείμενο της Πολιτικής Αναγνωρισμένων Πιστοποιητικών (*CP Q.C.*) του συγκεκριμένου πιστοποιητικού,
- τέλος, την βούλησή του να ενεργοποιηθεί το πιστοποιητικό του.

Αμέσως μόλις παραληφθεί η παραπάνω δήλωση από τον συνδρομητή, η ‘Υπηρεσία Διαχείρισης Ανάκλησης’ (ΥΔΑ) μεριμνά για την επαναφορά των πιστοποιητικών σε ισχύ (αρχική ενεργοποίηση), σύμφωνα και με τα οριζόμενα στην παράγραφο 3.7.3 ΔΙΑΔΙΚΑΣΙΑ ΑΝΑΣΤΟΛΗΣ, ΑΝΑΚΛΗΣΗΣ ΚΑΙ (ΕΠΑΝ-)ΕΝΕΡΓΟΠΟΙΗΣΗΣ.

Επιπλέον στην περίπτωση δημιουργίας του Αναγνωρισμένου Πιστοποιητικού από τον ίδιο τον συνδρομητή, η ενεργοποίηση του Αναγνωρισμένου Πιστοποιητικού του γίνεται απευθείας από την ειδικά διαμορφωμένη διαδικτυακή εφαρμογή.

3.5 ΔΙΑΡΚΕΙΑ ΚΑΙ ΛΗΞΗ ΙΣΧΥΟΣ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

3.5.1 ΔΙΑΡΚΕΙΑ ΙΣΧΥΟΣ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Η διάρκεια ισχύος των πιστοποιητικών των τελικών οντοτήτων καθορίζεται στο κείμενο της σχετικής Πολιτικής τους και συνήθως είναι **ένα έτος**.

Για λόγους καλύτερης και ομαδοποιημένης διαχείρισης της διαδικασίας ανανέωσης, (βλ. το αμέσως επόμενο Κεφάλαιο), **η ακριβής ημερομηνία λήξης των εκδιδόμενων από το δίκτυο του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ πιστοποιητικών των τελικών οντοτήτων, υπολογίζεται ως εξής:**

- Για τα πιστοποιητικά που εκδίδονται στο διάστημα μεταξύ της 1^{ης} και της 15^{ης} ημέρας ενός μήνα του έτους, ορίζεται ως ημερομηνία λήξης η πρώτη (1^η) ημέρα του επόμενου -από αυτόν της έκδοσης- μήνα, του επόμενου ή του μεθεπόμενου έτους (ανάλογα με το αν προβλέπεται επήσια ή διετή διάρκεια)
- Για τα πιστοποιητικά που εκδίδονται στο διάστημα μεταξύ της 16^{ης} και της 31^{ης} ημέρας ενός μήνα του έτους, ορίζεται ως ημερομηνία λήξης η δέκατη πέμπτη (15^η) ημέρα του επόμενου -από αυτόν της έκδοσης- μήνα, του επόμενου ή του μεθεπόμενου έτους (ανάλογα με το αν προβλέπεται επήσια ή διετή διάρκεια)

(Σημείωση: Για την διάρκεια ισχύος των πιστοποιητικών (αλλά και των κρυπτογραφικών κλειδιών) του ‘Θεμελιώδη Εκδότη Πιστοποιητικών’ (ΘΕΠ) και των λοιπών ‘Υπο-Εκδοτών Πιστοποιητικών’ (Λειτουργικοί Εκδότες) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, δείτε την παράγραφο 4.1.1.3 στο Κεφάλαιο ‘Τεχνικά μέτρα Ασφαλείας’).

3.5.2 ΑΥΤΟΜΑΤΗ ΛΗΞΗ ΤΗΣ ΙΣΧΥΟΣ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Με την συμπλήρωση της ημερομηνίας λήξης της ισχύος τους, η οποία αναγράφεται σε σχετικό πεδίο μέσα στα ίδια τα πιστοποιητικά (βλ. Κεφάλαιο 5.1 ΠΕΡΙΓΡΑΦΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ για τα πεδία των πιστοποιητικών), αυτά **χάνουν αυτομάτως την ισχύ τους, χωρίς να απαιτείται να λάβει χώρα καμιά άλλη διαδικασία**, όπως π.χ. η εγγραφή του πιστοποιητικού στην ‘Λίστα Ανακληθέντων Πιστοποιητικών’ (ΛΑΠ).

Το λογισμικό και οι εφαρμογές για δημιουργία ή επαλήθευση υπογραφών που χρησιμοποιεί ο συνδρομητής ή ο χρήστης (αποδέκτης) των πιστοποιητικών, είναι υποχρεωμένα για είναι σε θέση να επεξεργαστούν το σχετικό πεδίο για την λήξη της ισχύος του πιστοποιητικού και να ενημερώσουν σχετικά τον χρήστη τους.

ΠΡΟΣΟΧΗ! Μετά την λήξη της ισχύος του, **ένα πιστοποιητικό δεν επιτρέπεται να χρησιμοποιείται για καμιά χρήση, πλην της επαλήθευσης ή επικύρωσης ήλεκτρονικών υπογραφών που δημιουργήθηκαν στηριζόμενες στο πιστοποιητικό αυτό κατά την διάρκεια της ισχύος του.**

3.6 ΑΝΑΝΕΩΣΗ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

3.6.1 ΠΕΡΙΠΤΩΣΕΙΣ ΑΝΑΝΕΩΣΗΣ

Η ανανέωση των πιστοποιητικών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ μπορεί να είναι είτε ‘**τακτική**’, όπου ο συνδρομητής συμπληρώνει και υπογράφει ηλεκτρονικά την αίτηση ανανέωσης που του στέλνει η ΥΕ του δικτύου πριν λήξουν ή ανακληθούν τα υπάρχοντα πιστοποιητικά του, είτε ‘**έκτακτη**’, όπου τα πιστοποιητικά του συνδρομητή έχουν λήξει ή ανακληθεί οπότε και ο συνδρομητής υποχρεούται να

επαναλάβει την διαδικασία χειρόγραφης αίτησης και εξακρίβωσης της ταυτότητάς του όπως και στην αρχική εγγραφή -σύμφωνα με τα οριζόμενα στην παράγραφο 3.2.3.2.

Ταυτόχρονα στην περίπτωση δημιουργίας του Αναγνωρισμένου Πιστοποιητικού από τον ίδιο τον συνδρομητή, η ανανέωση του Αναγνωρισμένου Πιστοποιητικού του θα γίνεται απευθείας από την ειδικά διαμορφωμένη διαδικτυακή εφαρμογή.

3.6.2 ΠΡΟΫΠΟΘΕΣΕΙΣ ΑΝΑΝΕΩΣΗΣ

Η ΥΕ, εφόσον υπάρχει η σύμφωνη γνώμη μιας ΤΥΥ, **είκοσι (20) τουλάχιστον ημέρες πριν την λήξη των πιστοποιητικών** των συνδρομητών, στέλνει ηλεκτρονική φόρμα ανανέωσης στην ηλεκτρονική διεύθυνση (*e-mail*) που έχει δηλώσει ο συνδρομητής. Σε περίπτωση που το πιστοποιητικό του τελευταίου έχει εκδοθεί από το ΧΑ και την ανάλογη υπηρεσία, ο συνδρομητής πρέπει να την συμπληρώσει, να την υπογράψει ηλεκτρονικά με το ισχύον –ακόμη- πιστοποιητικό του, και να την στείλει πίσω στην οριζόμενη ηλεκτρονική διεύθυνση (*e-mail*) της ΥΕ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ. Σε διαφορετική περίπτωση όπου το πιστοποιητικό έχει εκδοθεί από τον συνδρομητή μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής δεν είναι απαραίτητη η συμπλήρωση και η αποστολή της ηλεκτρονικής αίτησης. Η ανανέωση του πιστοποιητικού θα πραγματοποιηθεί μέσω την εν λόγω εφαρμογής.

Στην περίπτωση όπου το πιστοποιητικό έχει εκδοθεί από το ΧΑ και ο συνδρομητής δεν έχει κάνει χρήση της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής, η ηλεκτρονική φόρμα αίτησης ανανέωσης, αλλά και οι χειρόγραφες αιτήσεις για την περίπτωση της ‘έκτακτης’ ανανέωσης, περιλαμβάνουν δεδομένα σχετικά με:

- Την αποδοχή της χρέωσης για την ανανέωση από τον συνδρομητή και ρύθμιση του τρόπου εξόφλησής της,
- Την συμφωνία για την προμήθεια του νέου φορέα ‘α.δ.δ.ν.’ του συνδρομητή που πιθανώς είναι απαραίτητος για την ανανέωση προσωπικών πιστοποιητικών,
- Την δήλωση του συνδρομητή ότι τα κατατεθειμένα δικαιολογητικά κατά την αρχική εγγραφή εξακολουθούν να ισχύουν, καθώς και ότι δεν έχει αλλάξει κανένα από τα δεδομένα του υποκειμένου (θέματος) που περιλαμβάνονται στο υπό λήξη πιστοποιητικό του, ή τις τυχών τροποποιήσεις τους,
- Άλλες πιθανές δηλώσεις ή γνωστοποίησεις από τον συνδρομητή που πιθανώς απαιτούνται από την Πολιτική του συγκεκριμένου πιστοποιητικού που ανανεώνεται.

3.6.3 ΤΡΟΠΟΣ ΑΝΑΝΕΩΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Η ανανέωση των πιστοποιητικών συνίσταται στην έκδοση νέων πιστοποιητικών για τον συνδρομητή με τα ίδια ή κατάλληλα τροποποιημένα στοιχεία. Ανάλογα με τα οριζόμενα στην Πολιτική του ανανεούμενου πιστοποιητικού, μπορεί να απαιτείται δημιουργία νέου ζεύγους κρυπτογραφικών κλειδιών για το νέο πιστοποιητικό. Ειδικά στα προσωπικά πιστοποιητικά είναι πιθανόν να προβλέπεται στην πολιτική τους η χρησιμοποίηση και νέου φορέα για τα ιδιωτικά κλειδιά και πιστοποιητικά.

Κατά τα λοιπά, η ανανέωση των πιστοποιητικών διεξάγεται με τις ανάλογες διαδικασίες που προβλέπονται από τον παρόντα Κανονισμό και για την έκδοση των πιστοποιητικών μετά την έγκριση της αρχικής αίτησης έκδοσής τους είτε μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής.

3.7 ΑΝΑΣΤΟΛΗ ΚΑΙ ΑΝΑΚΛΗΣΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

3.7.1 ΕΝΝΟΙΑ ‘ΠΑΥΣΗΣ/ΑΝΑΣΤΟΛΗΣ’ ΚΑΙ ‘ΑΝΑΚΛΗΣΗΣ’ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ

Η ‘παύση’ ενός πιστοποιητικού συνίσταται στην -για κάποιον από τους αναφερόμενους στην αμέσως επόμενη παράγραφο λόγους – αναστολή της ισχύος ενός πιστοποιητικού, (η οποία όμως μπορεί να επανέλθει με την διαδικασία της ‘(επαν-)ενεργοποίησεως’ του πιστοποιητικού, εφόσον, επιβεβαιωμένα, εκλείψουν οι παραπάνω λόγοι), ενώ η (οριστική) ‘ανάκληση’ του πιστοποιητικού επιφέρει την οριστική απώλεια της ισχύος του, χωρίς να δύναται η με οποιονδήποτε τρόπο επαναφορά του σε ισχύ.

3.7.2 ΛΟΓΟΙ ΑΝΑΣΤΟΛΗΣ' ή/ΚΑΙ 'ΑΝΑΚΛΗΣΗΣ' ΕΝΟΣ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ

Οι λόγοι αναστολής και (οριστικής) ανάκλησης **είναι κοινοί**, με την διαφορά ότι η αίτηση και η πραγματοποίηση της αναστολής είναι επιβεβλημένες ακόμη και στην απλή υποψία ότι συντρέχει κάποιος από τους κοινούς λόγους, ενώ για την αίτηση και την πραγματοποίηση της ανάκλησης απαιτείται στοιχειώδης βεβαιότητα για το ότι υφίσταται ο συγκεκριμένος λόγος.

Ειδικά για την αναστολή των πιστοποιητικών προβλέπεται εξαιρετικά ως λόγος και η **έκδοση των πιστοποιητικών** με την έννοια της αναμονής για την 'αρχική ενεργοποίηση' του πιστοποιητικού από τον συνδρομητή μετά την παραλαβή ή/και την εγκατάστασή του.

Έτσι, ανάλογα με τον υπόχρεο ή τον δικαιούχο για την αναστολή ή ανάκληση ενός πιστοποιητικού που έχει εκδοθεί από το δίκτυο του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, οι λόγοι που μπορούν να αναφερθούν είναι οι εξής:

3.7.2.1 Λόγοι ανάκλησης από τις Υπηρεσίες του Δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ

Οι υπηρεσίες του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ δικαιούνται να ζητήσουν την αναστολή ή ανάκληση του πιστοποιητικού ενός συνδρομητή, εφόσον:

- Υπάρχουν οικονομικές εκκρεμότητες σχετικά με την έκδοση του πιστοποιητικού από την πλευρά του συνδρομητή,
- Επιβάλλεται για την διατήρηση της αξιοπιστίας του συστήματος και της υποδομής δημόσιων κλειδιών (PKI) του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, ιδίως στις περιπτώσεις που γίνεται γνωστή η απώλεια του ελέγχου ή της νόμιμης κατοχής των ιδιωτικών κλειδιών ή του κωδικού ενεργοποίησής τους από τον συνδρομητή ή στην περίπτωση που η ΥΕ του δικτύου έχει ενδείξεις ή αποδείξεις για την μη ορθότητα των αναφερόμενων στο πιστοποιητικό δεδομένων.
- Υπάρχει τελεσίδικη απόφαση δικαστηρίου ή άλλης σχετικής αρχής ή εισαγγελική εντολή που το επιβάλλει,
- Επιβάλλεται λόγω απώλειας δικαιοπρακτικής ικανότητας του συνδρομητή.

3.7.2.2 Λόγοι για υποβολή αίτησης ανάκλησης από τον Συνδρομητή

Ο συνδρομητής έχει υποχρέωση να ζητήσει την αναστολή ή ανάκληση του πιστοποιητικού του όταν:

- Έχει απολέσει τον έλεγχο ή την νόμιμη κατοχή των σχετικών ιδιωτικών κλειδιών του ή του κωδικού ενεργοποίησής τους,
- Έχει υποψία ή βεβαιότητα για την έκθεση των σχετικών ιδιωτικών κλειδιών του ή του κωδικού ενεργοποίησής τους σε τρίτους,
- Έχει τροποποιηθεί οποιοδήποτε από τα στοιχεία που τον αφορούν και αναγράφονται στο πιστοποιητικό,
- ‘Έχει απολέσει τη δικαιοπρακτική του ικανότητα (ΣΗΜΕΙΟ 1.2)
- Υποχρεύται να πράξει σχετικά σύμφωνα με τα οριζόμενα σε άλλα σημεία του παρόντα Κανονισμού Πιστοποίησης, στο κείμενο της σχετικής Πολιτικής του πιστοποιητικού ή στην Συνδρομητική Σύμβαση.

Επίσης ο συνδρομητής έχει δικαίωμα να ζητήσει την αναστολή ή ανάκληση του πιστοποιητικού του όποτε το θελήσει ο ίδιος και χωρίς να απαιτείται η δικαιολόγηση της αίτησης.

3.7.2.3 Άλλοι λόγοι Αναστολής ή Ανάκλησης

Άλλοι λόγοι που μπορούν να δικαιολογήσουν την αναστολή ή ανάκληση ενός πιστοποιητικού, είναι οι εξής:

- Υπάρχει σχετική πρόβλεψη (δικαίωμα ή υποχρέωση) σε άλλα σημεία του παρόντα Κανονισμού Πιστοποίησης, στο κείμενο της σχετικής Πολιτικής του πιστοποιητικού ή στην Συνδρομητική Σύμβαση.

- Μετά από αίτηση τρίτου, στις διαβεβαιώσεις του οποίου έχει πιθανώς στηριχθεί η έγκριση για την έκδοση του συγκεκριμένου πιστοποιητικού του συνδρομητή.

3.7.3 ΔΙΑΔΙΚΑΣΙΑ ΑΝΑΣΤΟΛΗΣ, ΑΝΑΚΛΗΣΗΣ ΚΑΙ (ΕΠΑΝ-)ΕΝΕΡΓΟΠΟΙΗΣΗΣ

Τόσο η αναστολή όσο και η ανάκληση ενός πιστοποιητικού πραγματοποιούνται, από την ΥΔΑ που παρέλαβε την σχετική αίτηση, με την εγγραφή του μοναδικού ‘Σειριακού Αριθμού’ (Serial Number) που χαρακτηρίζει το συγκεκριμένο πιστοποιητικό και του σχετικού λόγου ανάκλησής του (βλ. ειδικότερα και Κεφάλαιο 5.2 ΠΕΡΙΓΡΑΦΗ ‘ΛΙΣΤΑΣ ΑΝΑΚΛΗΘΕΝΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ’ (ΛΑΠ)) σε μια υπογεγραμμένη από τον εκδότη του πιστοποιητικού και ηλεκτρονικά δημοσιευόμενη προς το κοινό ‘Λίστα Ανακληθέντων Πιστοποιητικών’ (ΛΑΠ ή στα αγγλικά ‘Certificate Revocation List’ –‘CRL’).

Η εγγραφή του ‘σειριακού αριθμού’ ενός πιστοποιητικού στην ΛΑΠ και άρα η αναστολή ή η (οριστική) ανάκλησή του, είναι δυνατόν να ανιχνευτεί **είτε** με την χρήση ειδικού λογισμικού επαλήθευσης ισχύος πιστοποιητικών, **είτε** ακόμη και άμεσα από τον ίδιο τον χρήστη που θα διαβάσει την συγκεκριμένη λίστα και θα αντιπαραθέσει τους εκεί αναγραφόμενους ‘σειριακούς αριθμούς’ με τον αντίστοιχο του πιστοποιητικού που τον ενδιαφέρει.

Η σχετική ΥΔΑ του δικτύου είναι υποχρεωμένη να εκτελέσει την ληφθείσα αίτηση για αναστολή ή ανάκληση **εντός το πολύ 24 ωρών** από την εξακρίβωση της γνησιότητας της αίτησης (σύμφωνα και με τα αναφερόμενα στην παραπάνω παράγραφο 3.2.2) και να ενημερώσει σχετικά τον συνδρομητή.

Η (επαν-)ενεργοποίηση της ισχύος ενός ανασταλθέντος πιστοποιητικού γίνεται μετά από σχετική εξακριβωμένη αίτηση του προκαλέσαντα την αναστολή με την έκδοση νέας ΛΑΠ από την ΥΔΑ όπου εκλείπει η συγκεκριμένη εγγραφή.

Σε περίπτωση που τα Αναγνωρισμένα Πιστοποιητικά έχουν εκδοθεί από τον ίδιο τον συνδρομητή, ο τελευταίος δύναται να αναστείλει, να ανακαλέσει και να (επαν-)ενεργοποιήσει το αναγνωρισμένο πιστοποιητικό του μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής. Στις περιπτώσεις αναστολής ή ανάκλησης πιστοποιητικού η ενημέρωση της ΛΑΠ γίνεται αυτόματα από την ειδικά διαμορφωμένη διαδικτυακή εφαρμογή.

3.7.4 ΥΠΟΧΡΕΩΤΙΚΗ (ΕΠΑΝ-)ΕΝΕΡΓΟΠΟΙΗΣΗ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Εκτός από τα πιστοποιητικά που έχουν τεθεί σε (αναστολή) λόγω έκδοσης και αναμονής για την αίτηση ‘αρχικής ενεργοποίησής’ τους από τον συνδρομητή και τα οποία επαναφέρονται σε ισχύ αμέσως μετά την λήψη της αίτησης της παραγράφου 3.4.2, τα λοιπά παυθέντα πιστοποιητικά **δεν επιτρέπεται να παραμείνουν σε κατάσταση παύσης/αναστολής για διάστημα μεγαλύτερο της μίας (1) εβδομάδας.**

Ο συνδρομητής, ο οποίος ενημερώνεται αμέσως για την θέση σε αναστολή της ισχύος των πιστοποιητικών του από την ΥΔΑ, πρέπει να ζητήσει αιτιολογημένα μέσα στο παραπάνω χρονικό διάστημα την (επαν-)ενεργοποίηση του πιστοποιητικού του, άλλως αυτό τίθεται σε κατάσταση οριστικής ανάκλησης χωρίς καμιά ευθύνη του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ και του δικτύου της.

Αν την αναστολή του πιστοποιητικού την έχει προκαλέσει το ίδιο το δίκτυο του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ για κάποιον από τους περιεχόμενους στην παράγραφο 3.7.2.1 λόγους και δεν προχωρήσει μέσα στο ίδιο χρονικό διάστημα στην οριστική ανάκληση του συγκεκριμένου πιστοποιητικού τότε αυτό επαναφέρεται αυτόματα σε ισχύ (επανενεργοποιείται) χωρίς την ανάγκη σύμπραξης του συνδρομητή.

3.7.5 ΣΥΧΝΟΤΗΤΑ ΕΚΔΟΣΗΣ ΛΙΣΤΑΣ ΑΝΑΚΛΗΘΕΝΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ (CRL)

Η σχετική ‘Λίστα Ανακληθέντων Πιστοποιητικών’ (ΛΑΠ) του κάθε Λειτουργικού Εκδότη Πιστοποιητικών του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ πρέπει να ανανεώνεται και να επαναδημοσιεύεται **το πολύ κάθε εικοσιτέσσερις (24) ώρες**, αναφέροντας κάθε φορά σε σχετικά πεδία της (βλ. σχετικά Κεφάλαιο 5.2) τον αύξοντα αριθμό έκδοσής της και την ακριβή ημερομηνία και ώρα της επόμενης τακτικής δημοσίευσής της.

Σε περιπτώσεις που η ΥΔΑ κρίνει αναγκαίο, μπορεί να εκδοθεί και να δημοσιευτεί ‘**έκτακτη ενημερωμένη έκδοση**’ μιας ΛΑΠ, δηλαδή να εκδοθεί μια νέα ενημερωμένη ΛΑΠ πριν από την προγραμματισμένη ώρα έκδοσής της.

3.8 ΑΛΛΑΓΗ ΚΛΕΙΔΙΩΝ ΚΑΙ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΤΗΣ ΥΠΟΔΟΜΗΣ ‘ΡΚΙ’

Τα χρησιμοποιούμενα κλειδιά και τα πιστοποιητικά της υποδομής PKI του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (τόσο των Υπο-Εκδοτών όσο και το βασικό πιστοποιητικό του ΘΕΠ) υπόκεινται και αυτά σε αλλαγή (ανανέωση) για λόγους ασφάλειας (βλ. σχετικά παράγραφο 4.1.1.3).

Για να γίνεται ομαλά η αλλαγή των πιστοποιητικών των Εκδοτών Πιστοποιητικών και να διατηρείται έτσι η δυνατότητα επαλήθευσης της γνησιότητας των πιστοποιητικών των τελικών οντοτήτων διαμέσου μιας έγκυρης ‘Αλυσίδας Εμπιστοσύνης’ πιστοποιητικών, προβλέπεται η διαρκής συνύπαρξη δύο διαφορετικών πιστοποιητικών και αντίστοχων κρυπτογραφικών κλειδιών για κάθε εκδότη πιστοποιητικών του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (εκτός από το αρχικό διάστημα λειτουργίας τους), σύμφωνα με τις παρακάτω διαδικασίες:

3.8.1 ΑΛΛΑΓΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ ΤΩΝ ‘ΥΠΟ-ΕΚΔΟΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ’

Τα κρυπτογραφικά κλειδιά και τα πιστοποιητικά ενός Υπο-Εκδότη Πιστοποιητικών του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ έχουν διάρκεια ισχύος δέκα (10) έτη (βλ. παράγραφο 4.1.1.3) και χρησιμοποιούνται αποκλειστικά για την υπογραφή πιστοποιητικών των τελικών οντοτήτων (που έχουν μέγιστη διάρκεια τα δύο (2) έτη) καθώς και για την υπογραφή της σχετικής ‘Λίστας Ανακληθέντων Πιστοποιητικών’ ΛΑΠ για τα πιστοποιητικά αυτά.

Δύο (2) έτη πριν την λήξη των πιστοποιητικών των Υπο-Εκδοτών (όση είναι δηλαδή και η μέγιστη διάρκεια ισχύος των εκδιδόμενων από αυτούς πιστοποιητικών για τις τελικές οντότητες), δημιουργείται **νέο ζεύγος κρυπτογραφικών κλειδιών** και εκδίδεται σχετικά **νέο πιστοποιητικό** για τους Εκδότες αυτούς (από τον ΘΕΠ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ), το οποίο χρησιμοποιείται **αποκλειστικά** -από την στιγμή εκείνη και έπειτα- για την υπογραφή των νέων πιστοποιητικών που εκδίδονται για τις τελικές οντότητες και των σχετικών με αυτά ‘Λιστών Ανακληθέντων Πιστοποιητικών’ (ΛΑΠ), ενώ το προηγούμενο πιστοποιητικό του Υπο-Εκδότη που παραμένει σε ισχύ, χρησιμοποιείται **μόνο** -κατά το υπόλοιπο διάστημα έως την λήξη του- για την υπογραφή των ΛΑΠ που αναφέρονται στα πιστοποιητικά των τελικών οντοτήτων που είχαν εκδοθεί με βάση αυτό το πιστοποιητικό και τα οποία, πιθανώς, βρίσκονται ακόμη σε ισχύ.

3.8.2 ΑΛΛΑΓΗ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ ΤΟΥ ‘Θ.Ε.Π.’ ΤΟΥ ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (ROOT CA)

Αντίστοιχα, τα κρυπτογραφικά κλειδιά και το αυτο-υπογραφόμενο πιστοποιητικό του Θεμελιώδη Εκδότη Πιστοποιητικών (ΘΕΠ) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (X.A. Root CA) έχουν διάρκεια ισχύος είκοσι (20) έτη (βλ. παράγραφο 4.1.1.3) και χρησιμοποιούνται αποκλειστικά για την υπογραφή των πιστοποιητικών των Υπο-Εκδοτών καθώς και για την υπογραφή της πιθανής ‘Λίστας Ανακληθέντων Πιστοποιητικών’ ΛΑΠ για τα πιστοποιητικά αυτά.

Έτσι, **δέκα (10) έτη** πριν την λήξη του πιστοποιητικού του ΘΕΠ (όση είναι δηλαδή και η μέγιστη διάρκεια ισχύος των εκδιδόμενων από αυτόν πιστοποιητικών για τους Υπο-Εκδότες), **εκδίδεται παράλληλα νέο αυτο-υπογραφόμενο πιστοποιητικό** από τον ΘΕΠ, το οποίο χρησιμοποιείται **αποκλειστικά** -από την στιγμή εκείνη και έπειτα- για την υπογραφή των νέων πιστοποιητικών και των σχετικών με αυτά ‘Λιστών Ανακληθέντων Πιστοποιητικών’ (ΛΑΠ) που εκδίδει ο ΘΕΠ για τους Υπο-Εκδότες του, ενώ το προηγούμενο πιστοποιητικό του ΘΕΠ που παραμένει σε ισχύ, χρησιμοποιείται **μόνο** -κατά το υπόλοιπο διάστημα έως την λήξη του- για την υπογραφή μιας -όχι πιθανής υπό φυσιολογικές συνθήκες- (ΛΑΠ) που θα αναφέρεται στα πιστοποιητικά των Υπο-Εκδοτών που είχαν εκδοθεί με βάση το πιστοποιητικό αυτό, και τα οποία βρίσκονται ακόμη σε ισχύ.

3.9 ΠΑΥΣΗ ΠΑΡΟΧΗΣ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ ΑΠΟ ΤΟ ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ

Στην περίπτωση απόφασης για παύση της παροχής των υπηρεσιών ψηφιακής πιστοποίησης από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ, η εταιρία δεσμεύεται να προβεί στις παρακάτω πράξεις:

- Έγκαιρη ενημέρωση –τρείς (3) τουλάχιστον μήνες πριν- για την επερχόμενη παύση της παροχής των υπηρεσιών με κάθε πρόσφορο μέσο προς κάθε επηρεαζόμενο από την παύση αυτή (συνδρομητές, αποδέκτες και πελάτες).
- Ανάκληση όλων των πιστοποιητικών που έχουν εκδοθεί από το δίκτυο του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ και των πιστοποιητικών αλληλο-διαπίστευσης (cross-certification) που πιθανώς έχουν εκδοθεί από και προς άλλους φορείς πιστοποίησης.
- Καταστροφή όλων των ιδιωτικών κλειδιών του ΘΕΠ και των Υπο-Εκδοτών Πιστοποιητικών του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.
- Μεταβίβαση όλων των αρχείων και των εγγραφών που προβλέπονται στο Κεφάλαιο 2.6 ‘Πολιτική Αρχειοθέτησης Πληροφοριών’ σε διάδοχο φορέα που θα αναλάβει την διατήρησή τους για το χρονικό διάστημα που προβλέπεται από τις Πολιτικές των σχετικών πιστοποιητικών και από το νόμο.

Για την κάλυψη του κόστους των παραπάνω ενεργειών για την περίπτωση που η παύση της παροχής των υπηρεσιών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ προκληθεί λόγω πτώχευσής της, η εταιρία θα προβεί σε αντίστοιχη ασφαλιστική κάλυψη από αξιόπιστη ασφαλιστική εταιρία.

ΜΕΡΟΣ IV: ΑΞΙΟΠΙΣΤΙΑ ΚΑΙ ΑΣΦΑΛΕΙΑ ΣΥΣΤΗΜΑΤΟΣ

4.1 ΤΕΧΝΙΚΑ ΜΕΤΡΑ ΑΣΦΑΛΕΙΑΣ

4.1.1 ΔΗΜΙΟΥΡΓΙΑ ΤΩΝ ΚΡΥΠΤΟΓΡΑΦΙΚΩΝ ΚΛΕΙΔΙΩΝ

Όλα τα ζεύγη κρυπτογραφικών κλειδιών που δημιουργούνται για τους Εκδότες Πιστοποιητικών (CAs), τις εσωτερικές λειτουργίες της Υποδομής (PKI), και τους Συνδρομητές (Subscribers) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, χρησιμοποιούν για την δημιουργία τους μόνο εγκεκριμένο από το **ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ** υλικό (*hardware*) και λογισμικό (*software*). Ειδικά η δημιουργία των κλειδιών και των πιστοποιητικών των Εκδοτών Πιστοποιητικών (*CA certificates*) και των σχετικών με την εσωτερική λειτουργία της υποδομής PKI του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ πιστοποιητικών (*PKI certificates*) διενεργείται μόνο με την χρήση εγκεκριμένης και διαπιστευμένης κάρτας.

4.1.1.1 Δημιουργία και αποθήκευση κλειδιών των Εκδοτών Πιστοποιητικών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ

Η αρχική δημιουργία και αποθήκευση (creation and storage) των κλειδιών του ‘Θεμελιώδη Εκδότη Πιστοποιητικών’ (*Root CA*) και των Υπο-Εκδοτών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ συντελείται κάτω από ειδική «Τελετή Ιδρυσης» (*Root Key Generation Ceremony for Certification Authority*) με την παρουσία τρίτων ανεξάρτητων ελεγκτικών φορέων που πιστοποιούν την τήρηση όλων των προβλεπόμενων διαδικασιών και των σχετικών μέτρων ασφάλειας του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ. Όλες οι ενέργειες κατά την διάρκεια της τελετής καταγράφονται και διατηρούνται για πιθανό μελλοντικό έλεγχο των διαδικασιών.

Η δημιουργία και αποθήκευση των κρυπτογραφικών κλειδιών του ‘Θεμελιώδη Εκδότη Πιστοποιητικών’ (*Root CA*) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ και κάθε ‘Υπο-Εκδότη Πιστοποιητικών’ (*Subordinate CA* ή *Sub-CA*) του δικτύου της, εκπονείται μόνο μέσω ειδικής ‘**ασφαλούς μονάδας υλικού**’ (*Hardware Security Module*) που η λειτουργία του είναι πιστοποιημένη βάσει του προτύπου [FIPS 140-2 level 3]. Η χρήση της ‘ασφαλούς μονάδας υλικού’ για την δημιουργία και αποθήκευση του ζεύγους κρυπτογραφικών κλειδιών για κάθε Εκδότη Πιστοποιητικών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ απαιτεί την σύμπραξη τουλάχιστον δύο (2) διαφορετικών προσώπων που ενεργούν σε διαπιστευμένους ‘έμπιστους ρόλους’ (βλ. Κεφάλαιο 4.3).

4.1.1.2 Δημιουργία κλειδιών των συνδρομητών (τελικών οντοτήτων)

Η δημιουργία των κρυπτογραφικών κλειδιών των συνδρομητών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, ανάλογα με τις προβλέψεις της πολιτικής του εκδιδόμενου πιστοποιητικού, γίνεται:

- **είτε** από την ‘Υπηρεσία Προετοιμασίας Φορέα Συνδρομητών’, (για τα προσωπικά πιστοποιητικά φυσικών προσώπων), η οποία χρησιμοποιεί για τον σκοπό αυτό ‘αυτοτελή κρυπτογραφική μονάδα’ (*Hardware Cryptographic Module*) σύμφωνη με το πρότυπο [FIPS 140-2 level 3],
- **είτε** από τον ίδιο τον Συνδρομητή μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής.
- **είτε** από τον ίδιο τον Συνδρομητή (κυρίως για τα πιστοποιητικά των συσκευών τους, π.χ. Servers), ο οποίος τότε πρέπει να χρησιμοποιεί κρυπτογραφική μονάδα βασισμένη σε λογισμικό (Software-based Cryptographic Module) που συμφωνεί με το παραπάνω πρότυπο.

Στην περίπτωση που τα πιστοποιούμενα κλειδιά τα δημιουργεί ο ίδιος ο Συνδρομητής, η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ δεν παρέχει καμιά εγγύηση για την δημιουργία των κλειδιών και απλώς περιορίζεται στην υπόδειξη της χρήσης λογισμικού που βασίζεται στα διεθνώς αποδεχτά βιομηχανικά πρότυπα. Την τελική ευθύνη για την ορθότητα της διαδικασίας δημιουργίας των κλειδιών από τον συνδρομητή για τα οποία στέλνει αίτηση πιστοποίησής τους στο ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ, την αναλαμβάνει ο ίδιος ο συνδρομητής.

4.1.1.3 Μέγεθος και διάρκεια ισχύος των κλειδιών

Το μέγεθος των χρησιμοποιούμενων κλειδιών είναι εκθετικά ανάλογο με την ασφάλεια που προσφέρουν κατά μιας πιθανολογούμενης μελλοντικής ‘αποκρυπτογράφησής’ τους, αλλά όμως και ανάλογο με την υπολογιστική ισχύ που απαιτούν κατά την χρησιμοποίησή τους.

Από την άλλη, τα χρησιμοποιούμενα κρυπτογραφικά κλειδιά στην υποδομή PKI του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ έχουν περιορισμένη διάρκεια ισχύος και υπόκεινται σε τακτική λήξη ή ανάκληση και σε αντίστοιχη ανανέωσή τους (όπως και τα σχετικά πιστοποιητικά τους) για λόγους ασφαλείας.

Επισι,

- τα κρυπτογραφικά κλειδιά του ‘Θεμελιώδη Εκδότη Πιστοποιητικών’ (Root CA) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ έχουν μέγεθος **4096 bits** και διάρκεια ισχύος τα **20 έτη** (όση και τα σχετικά πιστοποιητικά του).
- τα κρυπτογραφικά κλειδιά των ‘Υπο-Εκδοτών Πιστοποιητικών’ (Subordinate CAs) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ έχουν μέγεθος **2048 bits** και διάρκεια ισχύος τα **10 έτη** (όση και τα σχετικά πιστοποιητικά τους).
- τα κρυπτογραφικά κλειδιά των Συνδρομητών (Subscribers) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ έχουν μέγεθος τουλάχιστον **2048 bits** και διάρκεια ισχύος **1** (όση και τα σχετικά πιστοποιητικά τους), ανάλογα με τα προβλεπόμενα στην σχετική Πολιτική των εκδιδόμενων πιστοποιητικών.

Σημείωση: Δείτε παραγράφους 3.8.1 & 3.8.2 για την διαδικασία αλλαγής κλειδιών και πιστοποιητικών του Θ.Ε.Π. και των Λειτουργικών Εκδοτών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ και την παράγραφο 3.6 καθώς και τις σχετικές παραγράφους των αντίστοιχων Πολιτικών Πιστοποιητικών για την διαδικασία ανανέωσης κλειδιών και πιστοποιητικών των τελικών οντοτήτων (συνδρομητών).

4.1.1.4 Χρησιμοποιούμενοι Αλγόριθμοι από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ

Ο χρησιμοποιούμενος αλγόριθμος δημιουργίας των κρυπτογραφικών κλειδιών για όλους τους Εκδότες Πιστοποιητικών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (αλλά και για τα κλειδιά των συνδρομητών, που δημιουργεί η ΥΠΦΣ) είναι ο αλγόριθμος [Rivest - Shiman - Adleman Algorithm] (**RSA**)’.

Ο χρησιμοποιούμενος αλγόριθμος για τον κατακερματισμό (Hashing) κατά την δημιουργία προηγμένης ηλεκτρονικής υπογραφής είναι ο [Secure Hashing Algorithm – 1] (**SHA-256**).

4.1.2 ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΙΔΙΩΤΙΚΩΝ ΚΛΕΙΔΙΩΝ

4.1.2.1 Ασφαλής διαδικασία δημιουργίας και υποχρεωτική χρήση φορέα των ιδιωτικών κλειδιών

Όλα τα ζεύγη κρυπτογραφικών κλειδιών που πιστοποιούνται από τις Υπηρεσίες Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ πρέπει να έχουν δημιουργηθεί με τέτοιο τρόπο ώστε το ιδιωτικό (private) κλειδί να μην είναι γνωστό σε κανέναν άλλον πλην του δικαιούχου χρήσης των κλειδιών αυτών.

Για να επιτευχθεί αυτό, τα ιδιωτικά κλειδιά που δημιουργούνται από το ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ εναποθηκεύονται σε ασφαλείς φορείς (π.χ. αυτοτελείς κρυπτογραφικές μονάδες ή έξυπνες κάρτες) όπου για την χρησιμοποίησή τους απαιτούν ειδικό ‘**κωδικό ενεργοποίησης**’ (βλ. παρακάτω) τον οποίο γνωρίζει μόνο ο εξουσιοδοτημένος χρήστης τους. Οι φορείς αυτοί, εφόσον πρέπει να σταλούν σε δικαιούχους συνδρομητές, αυτό γίνεται με συστημένη αποστολή που απαιτεί την υπογραφή αποδεικτικού παραλαβής.

Κατ’ εξαίρεση, εάν ρητά το επιτρέπει η σχετική πολιτική του εκδιδόμενου πιστοποιητικού προς έναν συνδρομητή, το σχετικό ιδιωτικό κλειδί μπορεί να αποθηκευτεί και σε δισκέτα ή/και σε ‘μη κοινόχρηστο σκληρό δίσκο’ του συνδρομητή.

Επιπλέον τα ιδιωτικά κλειδιά των Αναγνωρισμένων Πιστοποιητικών δημιουργούνται απευθείας στον φορέα που έχει στην κατοχή ο συνδρομητής μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής. Με τον τρόπο αυτό ενισχύεται η διασφάλιση της μη γνώσης του ιδιωτικού κλειδιού από τρίτους πλην του δικαιούχου.

4.1.2.2 Αντιγραφή (back-up), εναποθήκευση και ανάκτηση των ιδιωτικών κλειδιών

Η δημιουργία, η εναποθήκευση, η χρήση, η αντιγραφή και η ανάκτηση των κρυπτογραφικών κλειδιών των Εκδοτών Πιστοποιητικών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, γίνεται πάντα με την χρήση ειδικής ‘**ασφαλούς μονάδας υλικού**’ (*Hardware Security Module*) η λειτουργία της οποίας είναι πιστοποιημένη βάσει του προτύπου [FIPS 140-1 level 3], ενώ σε κάθε σχετική πράξη απαιτείται η σύμπραξη τουλάχιστον δύο (2) διαφορετικών προσώπων που ενεργούν σε διαπιστευμένους ‘έμπιστους ρόλους’ (βλ. Κεφάλαιο 4.3).

Τα κρυπτογραφημένα αντίγραφα ασφαλείας (*back-up*) των ιδιωτικών κλειδιών των ‘Εκδοτών Πιστοποιητικών’ (*CAs*) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ φυλάσσονται -για το ενδεχόμενο ανάγκης χρησιμοποίησής τους, π.χ. καταστροφή φορέα των πρωτότυπων κλειδιών- σε ‘ασφαλείς χώρους’ εντός και εκτός του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (βλ. παράγραφο 4.2.1).

Κανένα ιδιωτικό κλειδί (αναγνωρισμένο πιστοποιητικό) που δημιουργείται για οποιοδήποτε συνδρομητή από την ‘Υπηρεσία Προετοιμασίας Φορέα Συνδρομητών’ είτε από τον ίδιο το συνδρομητή μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής όπως και κανένα ιδιωτικό κλειδί του ΠΥΠ, δεν αντιγράφεται, ούτε φυλάσσεται με οποιονδήποτε τρόπο (π.χ. με την μέθοδο επιμερισμού ή αλλιώς ‘*Key Escrow*’) που θα μπορούσε να συμβάλει στην ανάκτησή τους, από τις Υπηρεσίες του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ ή από οποιοδήποτε άλλον.

4.1.2.3 Κωδικός ενεργοποίησης του φορέα των ιδιωτικών κλειδιών

Όλα τα ιδιωτικά κλειδιά που χρησιμοποιούνται στις Υπηρεσίες Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (Εκδοτών, εσωτερικής λειτουργίας PKI και Συνδρομητών), ανεξάρτητα με το μέσον εναποθήκευσής τους, πρέπει **υποχρεωτικά** να προστατεύονται με την χρήση μυστικού ‘**κωδικού ενεργοποίησης**’ (PIN) ο οποίος επιτρέπει την ενεργοποίηση και την χρήση των ιδιωτικών κλειδιών ή του φορέα που περιέχει τα ιδιωτικά κλειδιά, μόνο από το εξουσιοδοτημένο πρόσωπο που τον γνωρίζει.

Οι **κωδικοί ενεργοποίησης των φορέων** των ιδιωτικών κλειδιών των συνδρομητών που δημιουργούνται από την ‘Υπηρεσία Προετοιμασίας Φορέα Συνδρομητών’, συνίστανται σε έναν αλφαριθμητικό κωδικό μεγέθους 8 ψηφίων, ο οποίος εκτυπώνεται σε προστατευμένο φάκελο που αποστέλλεται άμεσα στον σχετικό συνδρομητή χωρίς να καταχωρηθεί ή να απομνημονευθεί με οποιαδήποτε τρόπο από αυτήν ή άλλη Υπηρεσία του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

Επιπλέον στην περίπτωση δημιουργίας του Αναγνωρισμένου Πιστοποιητικού από τον ίδιο τον συνδρομητή μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής, ο ‘κωδικός ενεργοποίησης’ (PIN), παράγεται αυτόματα και αποστέλλεται στον συνδρομητή μέσω αυτής.

(ΠΡΟΣΟΧΗ! Η μη σωστή απομνημόνευση από τον συνδρομητή του κωδικού ενεργοποίησης του φορέα που του παραδίδεται, σε συνδυασμό με την απώλεια της εκτύπωσής του που περιέχεται στον παραπάνω φάκελο, έχει σαν αποτέλεσμα την οριστική αδυναμία ενεργοποίησης των ιδιωτικών κλειδιών που περιέχονται στον φορέα αυτόν!).

4.1.2.4 Περιορισμένη χρήση των ιδιωτικών κλειδιών

Τα κρυπτογραφικά κλειδιά που πιστοποιούνται στα πλαίσια της υποδομής PKI του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ έχουν **περιορισμένες χρήσεις**, που καθορίζονται ανάλογα από την σχετική Πολιτική Πιστοποιητικού που υπάγονται.

Συγκεκριμένα, τα ιδιωτικά κλειδιά όλων των Εκδοτών Πιστοποιητικών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (‘Root CA’ και ‘Operational CAs’) πιστοποιούνται για να χρησιμοποιηθούν **αποκλειστικά** για την υπογραφή ‘Πιστοποιητικών’ (είτε Εκδοτών είτε ‘τελικών οντοτήτων’) και των σχετικών ‘Λιστών Ανακληθέντων Πιστοποιητικών’ (‘ΛΑΠ’ ή ‘CRL’). **Καμιά άλλη χρήση των πιστοποιητικών αυτών δεν επιτρέπεται.**

Αντίστοιχα, τα ιδιωτικά κλειδιά των τελικών οντοτήτων πιστοποιούνται για να χρησιμοποιηθούν σε άλλες συγκεκριμένες χρήσεις (π.χ. υπογραφή εγγράφων, υπογραφή μηνυμάτων ηλεκτρονικού ταχυδρομείου, ταυτοποίηση, κρυπτογράφηση δεδομένων κ.λ.π.) ανάλογα με την **συγκεκριμένη ‘Πολιτική Πιστοποιητικού’ (CP)** βάσει της οποίας εκδίδονται.

4.1.2.5 Καταστροφή ιδιωτικών κλειδιών των Εκδοτών Πιστοποιητικών μετά την λήξη τους

Τόσο τα πρωτότυπα όσο και τα εφεδρικά (back-up) ιδιωτικά κλειδιά των Εκδοτών Πιστοποιητικών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ καταστρέφονται μετά την λήξη της περιόδου ισχύος τους, ώστε να υπάρξει εγγύηση για την μη ανάκτηση και επαναχρησιμοποίησή τους.

Η καταστροφή αυτή ενεργείται, είτε με την καταστροφή του φορέα των ιδιωτικών κλειδιών στην περίπτωση που αυτός είναι έχυπνη κάρτα ή μαγνητικός φορέας π.χ. CD-ROM), είτε με την απενεργοποίηση και επαναδιαμόρφωση της κρυπτογραφικής μονάδας στην οποία αυτά είναι καταχωρημένα.

Η διαδικασία της καταστροφής των αποσυρόμενων ιδιωτικών κλειδιών των Εκδοτών Πιστοποιητικών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ επιβλέπεται και καταγράφεται και οι σχετικές εγγραφές αρχειοθετούνται.

4.1.3 ΆΛΛΑ ΜΕΤΡΑ ΤΕΧΝΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ λαμβάνει κάθε δυνατό και ενδεδειγμένο μέσον και τεχνική για την προστασία και την αξιοπιστία του συστήματός της από εσωτερικές ή εξωτερικές απειλές, όπως προσβολή των κεντρικών εξυπηρετητών από κακόβουλο λογισμικό, ενέργειες hacking, λ ΑΘΗΝΩΝ λαμβάνει, ενδεικτικά, τα εξής μέτρα:

- Προστασία του δικτύου της με ‘firewalls’,
- Χρήση ειδικών ‘ασφαλών μονάδων υλικού’ (*Hardware Security Modules*) η λειτουργία των οποίων είναι πιστοποιημένη βάσει του προτύπου [FIPS 140-2 level 3],
- Έκδοση και χρήση προσωπικών κλειδιών και πιστοποιητικών για την λειτουργία των συστημάτων PKI για κάθε εξουσιοδοτημένο χρήστη του συστήματος (βλ. και επόμενες παραγράφους)
- Σχεδιασμός δικτύου με τις μικρότερες δυνατές διαδρομές μεταξύ των αναγκαίων servers,
- Αυστηρός περιορισμός των τερματικών που έχουν πρόσβαση στο σύστημα στα απαραιτήτως αναγκαία και με αποκλειστική χρήση από τους εξουσιοδοτημένους χρήστες τους,
- Έλεγχος για ιούς σε οποιοδήποτε λογισμικό πρέπει να εγκατασταθεί στο σύστημα, κ.ά.

4.2 ΜΕΤΡΑ ΦΥΣΙΚΗΣ ΑΣΦΑΛΕΙΑΣ

Τα μέτρα φυσικής ασφάλειας αφορούν όλους τους χώρους, στους οποίους εκτελούνται οι βασικές λειτουργίες της υποδομής PKI του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, περιλαμβάνοντας ιδίως τις λειτουργίες του ‘Θεμελιώδη Εκδότη Πιστοποιητικών’, των ‘Υπο-Εκδοτών Πιστοποιητικών’ και των ‘Υπηρεσιών Εγγραφής’ και ‘Προετοιμασίας Φορέα των Συνδρομητών’. Στην περίπτωση που κάποιες από τις υπηρεσίες αυτές έχουν ανατεθεί σε εξωτερικούς συνεργάτες του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, αυτοί υπόκεινται στα ίδια μέτρα φυσικής ασφάλειας των χώρων που αναπτύσσουν τις υπηρεσίες αυτές.

4.2.1 ΕΠΙΛΟΓΗ ΚΑΙ ΚΑΤΑΣΚΕΥΗ ΤΩΝ ΧΩΡΩΝ

Οι λειτουργίες της υποδομής ‘PKI’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ και ο σχετικός με αυτές εξοπλισμός εγκαθίστανται σε ένα κτήριο ώστε να περιορίζεται η έκθεση τους σε αναρμόδια πρόσβαση. Το προσωπικό που εργάζεται με τα δεδομένα και τον εξοπλισμό της υποδομής PKI βρίσκεται σε χώρους απομονωμένους από τους λοιπούς που δεν προορίζονται για ασφαλείς διαδικασίες. Τα σημεία εσόδου-εξόδου των χώρων αυτών περιορίζονται στο ελάχιστο βαθμό που επιτρέπουν οι κανόνες πυρασφάλειας.

Οι χώροι στους οποίους γίνεται η επεξεργασία ή/και η εναποθήκευση των πληροφοριακών δεδομένων της υποδομής PKI και στους οποίους είναι εγκατεστημένος ο σχετικός εξοπλισμός, είναι σχεδιασμένοι ως ‘ασφαλείς χώροι’, έχοντας λάβει ειδικές προβλέψεις στον σχεδιασμό των συστημάτων κλιματισμού, παροχής ηλεκτρικής ενέργειας και τηλεπικοινωνιακών υποδομών.

Στην είσοδο των παραπάνω χώρων αναρτείται ταμπέλα με την ένδειξη ‘Μόνο για εξουσιοδοτημένο προσωπικό’ ή κάποιο αντίστοιχο μήνυμα.

4.2.2 ΦΥΣΙΚΗ ΠΡΟΣΒΑΣΗ

Οι είσοδοι των χώρων της υποδομής PKI διαθέτουν πόρτες ασφαλείας με μηχανισμό κλειδώματος. Κάθε πρόσβαση στους χώρους αυτούς εποπτεύεται και ελέγχεται από μηχανισμούς ελέγχου που λειτουργούν σε διαρκή βάση. Οι χώροι ασφαλείας παρακολουθούνται ακόμη και τις ώρες μη εργασίας με αυτόματα συστήματα ανίχνευσης κίνησης και συναγερμού.

Μη εξουσιοδοτημένο προσωπικό και τυχόν επισκέπτες που πρέπει να εισέλθουν στους ασφαλείς χώρους συνοδεύονται υποχρεωτικά και καθ' όλη την διάρκεια της παραμονής τους σ' αυτούς από εξουσιοδοτημένο προσωπικό.

Για τη πρόσβαση σε όλους τους χώρους ασφαλείας χρησιμοποιούνται τεχνικές ελέγχου όπως κωδικοί εισόδου, μαγνητικές κάρτες ή/και γραφείο υποδοχής. Όλα τα δικαιώματα πρόσβασης σε συγκεκριμένους χώρους, σε ερμάρια ασφαλείας και σε ευαίσθητα έγγραφα, καθώς και τα διανευμένα εργαλεία πρόσβασης, όπως κλειδιά, μαγνητικές κάρτες και καρτέλες-εμβλήματα (badges) καταγράφονται σε ειδικές ‘καταστάσεις ελέγχου πρόσβασης’.

Σε ειδικό ‘Ημερολόγιο Ελέγχου Πρόσβασης’ γίνονται καταχωρήσεις για κάθε επίσκεψη στους ασφαλείς χώρους από τους επισκέπτες, από τους εξωτερικούς συνεργάτες συντήρησης και εφοδιασμού των συστημάτων αλλά και από το εξουσιοδοτημένο προσωπικό εκτός των ωρών εργασίας του. Οι καταχωρήσεις αυτές περιλαμβάνουν τα παρακάτω στοιχεία:

- *Ταυτότητα και ιδιότητα (προσωπικό ή συνεργάτης) του εισερχόμενου προσώπου,*
- *Συγκεκριμένοι χώροι που επιτρέπεται να επισκεφθεί,*
- *Ακριβή ώρα εισόδου και εξόδου,*
- *Ταυτότητα του επιβλέποντος την είσοδο.*

4.2.3 ΠΑΡΟΧΗ ΗΛΕΚΤΡΙΣΜΟΥ, ΚΛΙΜΑΤΙΣΜΟΣ, ΠΥΡΑΣΦΑΛΕΙΑ ΚΑΙ ΔΙΑΡΡΟΕΣ.

Η παροχή ηλεκτρισμού στα κεντρικά συστήματα της υποδομής PKI του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ και των παρεχόμενων από αυτήν καταλόγων (*Directories*) προστατεύεται από τυχόν διακοπές ρεύματος. Ειδικές διαδικασίες δημιουργίας αντιγράφων ασφαλείας και επαναφοράς του συστήματος εφαρμόζονται για την αποφυγή της απώλειας δεδομένων και για την διατήρηση υψηλών επιπέδων διαθεσιμότητας του.

Ο κλιματισμός των χώρων ασφαλείας προσφέρει το κατάλληλο περιβάλλον θερμοκρασίας για την λειτουργία των μηχανημάτων και του προσωπικού. Η εγκατάστασή του είναι σχεδιασμένη ώστε να μην επιδρά στην φυσική ασφάλεια του χώρου και να μην επηρεάζει την λειτουργία του εξοπλισμού σε περίπτωση δυσλειτουργίας του.

Οι χώροι ασφαλείας προστατεύονται από σύστημα πυρανίχνευσης και αυτόματης κατάσβεσης πυρκαγιάς. Τέλος, έχουν ληφθεί όλα τα μέτρα για την προστασία από τυχόν διαρροή υδραυλικών συστημάτων και γενικά από την έκθεση σε νερό των συστημάτων της υποδομής.

4.2.4 ΕΝΑΠΟΘΗΚΕΥΣΗ ΦΟΡΕΩΝ ΔΕΔΟΜΕΝΩΝ (MEDIA)

Οι φορείς των δεδομένων και των αντιγράφων τους που χρησιμοποιούνται από το σύστημα για την λειτουργία του, εναποθηκεύονται σε ασφαλή ερμάρια που τους προστατεύουν από απειλές του περιβάλλοντος σχετικές με την θερμοκρασία, την υγρασία και τα μαγνητικά πεδία. Τα αντίγραφα ασφαλείας δεν περιλαμβάνουν τα αναγνωρισμένα πιστοποιητικά των χρηστών.

4.2.5 ΔΙΑΘΕΣΗ ΕΡΓΑΛΕΙΩΝ ΚΑΙ ΔΕΛΟΜΕΝΩΝ ΑΣΦΑΛΕΙΑΣ

Η διάθεση των εργαλείων πρόσβασης στους φυσικούς χώρους αλλά και των άλλων δεδομένων ασφαλείας όπως κωδικοί ενεργοποίησης και αρχεία λειτουργίας, γίνονται με ασφαλείς και ελεγχόμενες διαδικασίες.

4.2.6 ΑΠΟΜΑΚΡΥΣΜΕΝΟ ΕΝΑΛΛΑΚΤΙΚΟ ΣΥΣΤΗΜΑ ΚΑΙ ΑΝΤΙΓΡΑΦΑ ΑΣΦΑΛΕΙΑΣ

Ένα **δεύτερο εναλλακτικό σύστημα**, ικανό να αντεπεξέλθει σε όλες τις βασικές λειτουργίες των υπηρεσιών πιστοποίησης (διαχείριση πιστοποιητικών και δημοσίευση καταλόγων) τηρείται από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ σε απομακρυσμένη, από το αρχικό σύστημα, τοποθεσία.

4.3 ΕΛΕΓΧΟΣ ΚΑΙ ΑΣΦΑΛΕΙΑ ΤΩΝ ΔΙΑΔΙΚΑΣΙΩΝ

Οι διάφορες εσωτερικές διαδικασίες ασφαλείας που τηρούνται στα πλαίσια της παροχής των υπηρεσιών πιστοποίησης περιγράφονται αναλυτικότερα σε εσωτερικά -μη δημοσιεύσιμα- κείμενα ‘πολιτικής και πρακτικής ασφάλειας’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

4.3.1 ΕΜΠΙΣΤΟΙ ΡΟΛΟΙ

Όλοι οι εργαζόμενοι, οι συμβατικά συνεργαζόμενοι και οι σύμβουλοι των ‘Υπηρεσιών Ψηφιακής Πιστοποίησης’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ που έχουν πρόσβαση ή έλεγχο σε κρυπτογραφικές λειτουργίες που αφορούν την έκδοση, χρήση, αναστολή ή ανάκληση πιστοποιητικών, καθώς και την διαχείριση των δημοσιεύσιμων καταλόγων και του ‘ηλεκτρονικού αποθετηρίου’, χαρακτηρίζονται, για τους σκοπούς του παρόντος κειμένου, ότι εξυπηρετούν ‘**έμπιστους ρόλους**’. Ως προσωπικό που εξυπηρετεί ‘έμπιστους ρόλους’ θεωρούνται επίσης οι διαχειριστές, οι τεχνικοί και οι λειτουργοί του συστήματος, καθώς και οι εντεταλμένοι για την επίβλεψη των λειτουργιών της υποδομής ‘PKI’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

4.3.2 ΕΜΠΙΣΤΟΙ ΡΟΛΟΙ ΤΗΣ ΥΠΗΡΕΣΙΑΣ ΕΚΔΟΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Το προσωπικό της Υπηρεσίας Έκδοσης Πιστοποιητικών (ΥΕΠ) έχει κατανεμηθεί σε ‘έμπιστους ρόλους’ που αναλαμβάνουν προσχεδιασμένες διαδικασίες έχοντας ο καθένας περιορισμένη και ελεγχόμενη πρόσβαση στις εργασίες που απαιτούνται για να εκτελεστούν με πληρότητα οι υποχρεώσεις της υπηρεσίας.

4.3.3 ΕΜΠΙΣΤΟΙ ΡΟΛΟΙ ΤΗΣ ΥΠΗΡΕΣΙΑΣ ΕΙΓΡΑΦΗΣ & ΔΙΑΧΕΙΡΙΣΗΣ ΑΝΑΚΛΗΣΗΣ

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ λαμβάνει κάθε πρόσφορο μέτρο ώστε το προσωπικό της Υπηρεσίας Εγγραφής (ΥΕ) και της Υπηρεσίας Διαχείρισης Ανάκλησης (ΥΔΑ) των πιστοποιητικών, να αντιλαμβάνονται την ευθύνη τους για την εξακρίβωση της ταυτότητας και της γνησιότητας των υποψηφίων ή εγγεγραμμένων συνδρομητών, κατά την εκτέλεση των λειτουργιών της επαλήθευσης και της έγκρισης μιας αίτησης για έκδοση, ανάκληση, αναστολή ή επανενεργοποίηση ενός πιστοποιητικού καθώς και για την ασφαλή μεταβίβαση των στοιχείων του αιτούντα στην Υπηρεσία Έκδοσης Πιστοποιητικών και των κωδικών ταυτοποίησης ή ενεργοποίησης στον συνδρομητή.

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ μπορεί να επιτρέψει την εκτέλεση όλων των λειτουργιών της Υπηρεσίας Εγγραφής και της Υπηρεσίας Διαχείρισης Ανακλήσεων σε ατομικούς ‘έμπιστους ρόλους’ που θα αναθέτονται σε έμπιστα πρόσωπα.

4.3.4 ΑΡΙΘΜΟΣ ΑΠΑΙΤΟΥΜΕΝΩΝ ΠΡΟΣΩΠΩΝ ΓΙΑ ΤΗΝ ΕΚΤΕΛΕΣΗ ΜΙΑΣ ΕΡΓΑΣΙΑΣ

Για να εξασφαλιστεί η μη παράκαμψη των κανόνων ασφαλείας από ένα πρόσωπο που λειτουργεί μόνο του, η διαχείριση του συστήματος και των λειτουργιών των Υπηρεσιών Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ διανέμεται σε πολλαπλούς ‘έμπιστους ρόλους’ και αντίστοιχα πρόσωπα. Κάθε λογαριασμός πρόσβασης στο σύστημα του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ θα έχει περιορισμένες δυνατότητες λαμβάνοντας υπόψη τον ‘ρόλο’ του κατέχοντος τον λογαριασμό.

Για τον λόγο αυτό, κάθε μέλος του προσωπικού των Υπηρεσιών Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ θα υπόκειται σε επαλήθευση της ταυτότητάς του και των αρμοδιοτήτων του, **πριν**:

- περιληφθεί στις καταστάσεις των ατόμων με πρόσβαση στους ασφαλείς χώρους,
- αποκτήσει λογαριασμό πρόσβασης στο σύστημα και τον εξοπλισμό,
- λάβει το απαραίτητο πιστοποιητικό για την εκτέλεση του ρόλου του.

Όλα τα δικαιώματα των Διαχειριστών του συστήματος ελέγχονται και πιστοποιούνται με την έκδοση ειδικών ‘πιστοποιητικών διαχειριστή’ τα οποία απαιτούνται για την πρόσβαση στις διαχειριστικές πράξεις και εργασίες των Υπηρεσιών Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

Κάθε τέτοιο πιστοποιητικό (και ο σχετικός με αυτό λογαριασμός πρόσβασης) έχει τα εξής χαρακτηριστικά:

- είναι σχετιζόμενο άμεσα με συγκεκριμένο φυσικό πρόσωπο,
- δεν επιτρέπεται να χρησιμοποιείται από άλλον,
- η χρήση του περιορίζεται σε πράξεις επιτρεπόμενες από τον ειδικότερο ρόλο του κατόχου του, μέσω της χρήσης ειδικού λογισμικού, του λειτουργικού συστήματος και διαδικαστικών ελέγχων.

Τα παραπάνω πιστοποιητικά των διαχειριστών εγκαθίστανται σε ειδικούς υλικούς φορείς (‘tokens’ – π.χ. έξυπνες κάρτες) που απαιτούν την χρήση ‘κωδικού ενεργοποίησης’, εξασφαλίζοντας έτσι στο μέγιστο βαθμό την ασφάλεια στις λειτουργίες των Υπηρεσιών Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

4.4 ΕΛΕΓΧΟΣ ΚΑΙ ΑΞΙΟΠΙΣΤΙΑ ΠΡΟΣΩΠΙΚΟΥ

4.4.1 ΑΠΑΙΤΗΣΕΙΣ ΕΜΠΕΙΡΙΑΣ, ΔΙΑΠΙΣΤΕΥΣΕΩΝ ΚΑΙ ΕΜΠΙΣΤΟΣΥΝΗΣ

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ εξασφαλίζει ότι, όλο το προσωπικό που αναλαμβάνει ‘έμπιστους ρόλους’ και ευθύνες σχετικά με την λειτουργία των Υπηρεσιών Ψηφιακής Πιστοποίησης της:

- έχει κριθεί θετικά σε εξετάσεις ασφαλείας του προσωπικού,
- έχει δεσμευτεί με σύμβαση ή δήλωσή του για την ανάληψη του ειδικού ρόλου και των σχετικών με αυτόν όρων και προϋποθέσεων,
- έχει λάβει την κατάλληλη εκπαίδευση για τον ρόλο και τα καθήκοντα που του ανατίθενται,
- έχει δεσμευτεί με σύμβαση ή δήλωσή του για την εχεμύθειά και την μη διάδοση των εναίσθητων πληροφοριών σχετικά με την ασφάλεια του συστήματος του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ και των προσωπικών δεδομένων των συνδρομητών,
- δεν αναλαμβάνει άλλα καθήκοντα που μπορεί να έρθουν σε σύγκρουση με τις υποχρεώσεις και τα καθήκοντά του ως προς τις Υπηρεσίες Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

Όλο το παραπάνω προσωπικό υλοποιεί και εφαρμόζει τις πολιτικές διοίκησης και προσωπικού της εταιρίας οι οποίες καθορίζουν τα απαραίτητα επίπεδα αξιοπιστίας και επάρκειας του προσωπικού για την ικανοποιητική εκτέλεση και απόδοση των υπηρεσιών Ψηφιακής Πιστοποίησης, με τρόπο σύμφωνο με τον παρόντα Κανονισμό Πιστοποίησης.

4.4.2 ΑΠΑΙΤΗΣΕΙΣ ΕΚΠΑΙΔΕΥΣΗΣ

Η ΧΡΗΜΑΤΙΣΤΗΡΙ ΑΘΗΝΩΝ παρέχει ειδική εκπαίδευση στο προσωπικό σχετικά με την εκτέλεση των καθηκόντων τους και προβαίνει σε διοργάνωση πρόσθετων σεμιναρίων όταν απαιτείται εκπαίδευση σε επίκαιρα θέματα. Η εκπαίδευση περιλαμβάνει:

- Τις αρχές και τους μηχανισμούς ασφάλειας των ‘Υπηρεσιών Ψηφιακής Πιστοποίησης’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ,
- Όλες τις εκδόσεις του λογισμικού PKI που χρησιμοποιούνται από το σύστημα του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ,
- Όλα τα καθήκοντα και οι διαδικασίες του συστήματος PKI που πρέπει να τηρηθούν,
- Η Πολιτική Ασφάλειας και η Πολιτική Προστασίας Προσωπικών Δεδομένων της εταιρίας,
- Καθήκοντα και υποχρεώσεις του προσωπικού,
- Διαδικασίες αναφοράς της παραβίασης της ασφάλειας και της εχεμύθειας.

Η παραπάνω εκπαίδευση του προσωπικού επαναλαμβάνεται σε περιοδική βάση (π.χ. ετήσια ή διετής) για την διατήρηση της επίγνωσης και της πληροφόρησης σε νέες πολιτικές και διαδικασίες.

Στο προσωπικό φάκελο του κάθε εκπαιδευόμενου της εταιρίας καταχωρείται ‘πιστοποιητικό παρακολούθησης’ του εκπαιδευτικού προγράμματος το οποίο φέρει την υπογραφή ανώτερου στελέχους της διοίκησης των Υπηρεσιών Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

4.4.3 ΔΙΕΝΕΡΓΕΙΑ ΕΛΕΓΧΩΝ ΚΑΙ ΚΥΡΩΣΕΙΣ

Το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ διενεργεί κατάλληλους ελέγχους για όλο το προσωπικό που θα χρησιμοποιηθεί σε ‘έμπιστους ρόλους’ (πριν την ανάθεση των ρόλων αυτών αλλά και μετέπειτα σε περιοδική βάση, εφόσον κριθεί αναγκαίο) για να επιβεβαιώσει την αξιοπιστία και την επάρκεια των προσόντων τους σε σχέση με τις απαιτήσεις του παρόντος Κανονισμού Πιστοποίησης και της γενικότερης πολιτικής προσωπικού του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ. Το προσωπικό που δεν θα ανταποκριθεί στα σχετικά κριτήρια κατά τον αρχικό ή τον περιοδικό έλεγχο δεν θα χρησιμοποιηθεί ή θα σταματήσει να χρησιμοποιείται σε ‘έμπιστους ρόλους’.

Εάν μέλος του προσωπικού, επιφορτισμένο με καθήκοντα σχετικά με την λειτουργία των Υπηρεσιών Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, προβεί -αποδεδειγμένα ή με σοβαρές ενδείξεις- σε πράξη που αντίκειται στους κανονισμούς ή στην εξουσιοδότησή του, θα αναστέλλεται άμεσα η άδεια πρόσβασής του στο σύστημα του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ. Στην περίπτωση όπου αποδειχθεί σοβαρή αμέλεια ή κακόβουλη πρόθεση από το πρόσωπο αυτό, όλα τα προνόμια και τα δικαιώματα πρόσβασής του στο σύστημα θα ανακαλούνται οριστικά, ενώ παράλληλα θα υπόκειται σε διορθωτικές και πειθαρχικές διαδικασίες.

4.4.4 ΠΡΟΣΩΠΙΚΟ ΣΥΜΒΕΒΛΗΜΕΝΩΝ ΣΥΝΕΡΓΑΤΩΝ

Η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ εξασφαλίζει ότι οι συμβεβλημένοι συνεργάτες της στην παροχή των υπηρεσιών πιστοποίησης και το σχετικό προσωπικό τους θα έχουν πρόσβαση στους χώρους και στο σύστημα του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ μόνο κατόπιν εξουσιοδότησης ή με συνοδεία κατάλληλου προσωπικού του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, κάθε τέτοιο δε γεγονός, θα καταγράφεται σε σχετικό βιβλίο συμβάντων ή ηλεκτρονικώς.

Κάθε σχετικά συμβεβλημένος συνεργάτης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ υπόκειται στον όρο ότι ο ίδιος και το προσωπικό του δεσμεύονται να τηρούν όλες τις πολιτικές και τις διαδικασίες του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ σχετικά με την ασφάλεια και την εχεμύθεια των δεδομένων του συστήματος, συνάπτοντας ‘Συμφωνία Μη Δημοσιοποίησης και Προστασίας Προσωπικών Δεδομένων’.

4.4.5 ΠΑΡΟΧΗ ΟΔΗΓΙΩΝ ΚΑΙ ΤΕΚΜΗΡΙΩΣΗΣ

Όλο το προσωπικό των Υπηρεσιών Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ προμηθεύεται με κατανοητές οδηγίες χρήσης και την τυχόν απαραίτητη τεκμηρίωση σχετικά με τις διαδικασίες για την έκδοση, την ενημέρωση, την ανανέωση, την αναστολή και την ανάκληση των πιστοποιητικών καθώς και την λειτουργία των σχετικού λογισμικού.

ΜΕΡΟΣ V: ΠΕΡΙΓΡΑΦΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ & Λ.Α.Π.

5.1 ΠΕΡΙΓΡΑΦΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

5.1.1 ΤΥΠΟΣ ΚΑΙ ΑΡΙΘΜΟΣ ΕΚΔΟΣΗΣ

Οι ‘Υπηρεσίες Ψηφιακής Πιστοποίησης’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ χρησιμοποιούν ηλεκτρονικά πιστοποιητικά τύπου [X.509, Version 3] (έκδοσης 3ης) τα οποία υποστηρίζουν την χρήση εκτεταμένων πεδίων (*extensions*). Ο αριθμός της έκδοσης αναφέρεται πάντα στο σχετικό πεδίο του πιστοποιητικού.

5.1.2 ΠΕΡΙΕΧΟΜΕΝΟ ΚΑΙ ΣΗΜΑΣΙΑ ΤΩΝ ΠΕΔΙΩΝ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

Τα πιστοποιητικά που εκδίδονται από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ προς τους συνδρομητές/τελικές οντότητες (*end-entities certificates*), περιέχουν τα εξής πεδία:

Όνομα πεδίου (*)	Υποχρεωτικό	Περιεχόμενο	Παρατηρήσεις
Έκδοση <i>Version</i>	ΝΑΙ	“V3”	Έκδοση ‘3’ του προτύπου ηλεκ. πιστοποιητικών ‘X.509 - RFC 5280’ που υποστηρίζει εκτεταμένα πεδία.
Σειριακός Αριθμός <i>Serial Number</i>	ΝΑΙ	[Ακέραιος αριθμός]	Μοναδικός αριθμός του εκδιδόμενου πιστοποιητικού από τον συγκεκριμένο εκδότη πιστοποιητικών
Αλγόριθμος Υπογραφής <i>Signature Algorithm</i>	ΝΑΙ	[Προσδιοριστικό]	Προσδιορίζει τον αλγόριθμο που χρησιμοποιήθηκε για τον κατακερματισμό (Hash) και την υπογραφή του πιστοποιητικού
Εκδότης <i>Issuer</i>	ΝΑΙ	(Διακεκριμένο Όνομα (DN) τύπου ‘X.501’ για τον Εκδότη)	Το όνομα του εκδότη, αναλυμένο σε υπο-πεδία. Δες ανάλυση στις επόμενες παραγγράφους 5.1.3.1 και 5.1.3.2
Ισχύει από <i>Valid From</i>	ΝΑΙ	[Ημερομηνία]	Η ημερομηνία έκδοσης του πιστοποιητικού.
Ισχύει μέχρι <i>Valid To</i>	ΝΑΙ	[Ημερομηνία]	Η ημερομηνία λήξης της ισχύος του πιστοποιητικού.
Θέμα (Υποκείμενο) <i>Subject</i>	ΝΑΙ	(Διακεκριμένο Όνομα (DN) τύπου ‘X.501’ για το υποκείμενο, είδος πιστοποιητικού, ήτοι Qualified)	Το όνομα του θέματος-υποκείμενου (κατόχου του πιστοποιούμενου δημόσιου κλειδιού), αναλυμένο σε υπο-πεδία.. Τα χρησιμοποιούμενα υποπεδία και το περιεχόμενό τους προσδιορίζεται στην σχετική πολιτική του κάθε πιστοποιητικού. Δες παράγραφο 5.1.3.3
Δημόσιο Κλειδί <i>Public Key</i>	ΝΑΙ	[Δεκαεξαδικός αριθμός]	Το πιστοποιούμενο ‘Δημόσιο Κλειδί’ του ‘Θέματος’ (υποκείμενο)
Σημεία Διανομής Λ.Α.Π. <i>CRL Distribution Points</i>	ΝΑΙ	(Στο υποπεδίο ‘Distribution Point Name:/Full Name:=’) [Διεύθυνση τύπου ‘URI’]	Η ηλεκτρονική διεύθυνση όπου δημοσιεύεται η σχετική ενημερωμένη ‘Λίστα Ανακληθέντων Πιστοποιητικών’ (‘Λ.Α.Π.’ ή ‘CRL’)
Πολιτικές Πιστοποιητικού <i>Certificate Policies</i>	ΝΑΙ	[Προσδιοριστικό Πολιτικών] (& στο υποπεδίο ‘Qualifier: CPSUri:=’) [Διεύθυνση τύπου ‘URI’]	Περιέχει τον αριθμό αναγνώρισης (OID) που αντιστοιχεί στο κείμενο μιας δημοσιευόμενης ‘Πολιτικής’ που διέπει τους όρους χρήσης του πιστοποιητικού καθώς και την ηλεκτρονική διεύθυνση που δημοσιεύεται ο παρών Κανονισμός Πιστοποίησης
Χρήσεις Κλειδιού <i>Key Usage</i>	ΝΑΙ	(Ενδείξεις για τις επιτρεπόμενες από την πολιτική χρήσεις του πιστοποιούμενου κλειδιού)	Προσδιορίζει τις επιτρεπόμενες χρήσεις του ιδιωτικού κλειδιού του συνδρομητή (π.χ. ταυτοποίηση, μη αποκόρυφη, κρυπτογράφηση δεδομένων, υπογραφή, κλπ)

QCStatements	NAI	id-etsi-qcs-Qccompliance (esi4-qcStatement-1) id-etsi-qcs-QcSSCD (esi4-qcStatement-4) Id-etsi-qcs-QcPDS (esi4-qcStatement-5)	Ενδειχη ότι το πιστοποιητιό εκδόθηκε βάση του Κανονισμού No 910/2014 και αποθηκεύεται σε Α.Δ.Δ.Υ
Πρόσθετες Χρήσεις Κλειδών <i>Extended Key Usage</i>	Προαιρετικό	(Ενδείξεις για πρόσθετες επιτρεπόμενες χρήσεις του πιστοποιούμενου κλειδιού)	Προσδιορίζει πρόσθετες χρήσεις των ιδιωτικού κλειδιού του συνδρομητή (π.χ. υπογραφή κώδικα, ασφαλές ηλ. ταχυδρομείο, χρονοσήμανση κ.λ.π.)
Προσδιοριστικό Κλειδιού Εκδότη <i>Authority Key Identifier</i>	ΠΡΟΑΙΡΕΤΙΚΟ	[Ακέραιος αριθμός]	Προσδιορίζει ποιο ζεύγος κλειδιών του Εκδότη Πιστοποιητικών χρησιμοποιήθηκε για να υπογράψει το συγκεκριμένο πιστοποιητικό
Προσδιοριστικό Κλειδιού Θέματος <i>Subject Key Identifier</i>	ΠΡΟΑΙΡΕΤΙΚΟ (στα πιστοπ. Εκδοτών)	[Ακέραιος αριθμός]	Προσδιορίζει ποιο ζεύγος κλειδιών του Εκδότη Πιστοποιητικών πιστοποιείται με το συγκεκριμένο πιστοποιητικό.

(*) = Τα ονόματα των πεδίων εμφανίζονται στα ελληνικά ή στα αγγλικά ανάλογα με την γλώσσα της εφαρμογής που χρησιμοποιείται για την 'ανάγνωση' του πιστοποιητικού (π.χ. MS Outlook Express).

Στα αναγνωρισμένα πιστοποιητικά που εκδίδονται από το ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ αναγράφεται υποχρεωτικά και το είδος αυτού ήτοι "Qualified". Η εν λόγω αναγραφή πραγματοποιείται στο Θέμα (Υποκείμενο) Subject του εκδιδόμενου Αναγνωρισμένου Πιστοποιητικού. Επίσης, μπορούν να υπάρχουν (προαιρετικά) και επιπλέον πεδία που περιέχουν κείμενο-δηλώσεις σχετικά με τους ιδιαίτερους όρους χρήσης (π.χ. ανώτατο όριο επιτρεπόμενων συναλλαγών) του πιστοποιητικού, καθώς και άλλα πεδία με ιδιότητες του πιστοποιητικού, όπως π.χ. η αποτύπωσή του και ο σχετικός αλγόριθμος της αποτύπωσης, κ.λ.π..

5.1.3 ΤΥΠΟΣ ΚΑΙ ΠΕΡΙΕΧΟΜΕΝΟ ΤΩΝ ΔΙΑΚΕΚΡΙΜΕΝΩΝ ΟΝΟΜΑΤΩΝ (DN)

Τα διακεκριμένα ονόματα (*Distinguished Names – DN*) που περιέχονται στα πεδία του 'Εκδότη' και του 'Θέματος' (υποκείμενου πιστοποίησης) των πιστοποιητικών του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ είναι της μορφής του προτύπου [X.501, Name] που περιλαμβάνει υποπεδία με συγκεκριμένες ιδιότητες. Οι ιδιότητες αυτές (όπως Όνομα, Επίθετο, Χώρα κ.λ.π.) προσδιορίζονται αναλυτικότερα στο [X.520].

Τα περιεχόμενα των υπο-πεδίων αυτών αναγράφονται με λατινικούς χαρακτήρες, είτε με την πιστή μετάφραση του περιεχομένου τους στα Αγγλικά, είτε με 'λατινικοποίηση' των ελληνικών χαρακτήρων σύμφωνα με το πρότυπο [ΕΛΟΤ 743], για λόγους διεθνούς συμβατότητας. (βλ. και σχετική παράγραφο 2.4 'Πολιτική Ονομασίας Υποκειμένων')

5.1.3.1 Διακεκριμένο όνομα (DN) του 'Θεμελιώδη Εκδότη Πιστοποιητικών' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ

Το διακεκριμένο όνομα (DN) του 'Θεμελιώδη Εκδότη Πιστοποιητικών' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ που καταγράφεται στο πεδίο 'Εκδότης' (Issuer) στα 'Πιστοποιητικά Εκδοτών (CA Certificates) - άλλα και στο πεδίο 'Θέμα' (Subject) στο 'αυτό-υπογραφόμενο πιστοποιητικό' (*self-signed certificate*) του-, έχει το εξής περιεχόμενο:

Υποπεδίο	Επεξήγηση	Περιεχόμενο
O=	Οργανισμός (Organization)	ATHENS STOCK EXCHANGE
CN=	Κοινό Όνομα (Common Name)	ATHEX Root CA G2
C=	Χώρα (Country)	GR

5.1.3.2 Διακεκριμένο όνομα (DN) των ‘Λειτουργικών Εκδοτών Πιστοποιητικών’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ

Το διακεκριμένο όνομα (DN) των ‘Λειτουργικών Εκδοτών Πιστοποιητικών’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ που καταγράφεται στο πεδίο ‘Εκδότης’ (Issuer) στα ‘Πιστοποιητικά των συνδρομητών/τελικών οντοτήτων’ (*end-entities certificates*) αλλά και στο πεδίο ‘Θέμα’ (Subject) στα ‘Πιστοποιητικά των Εκδοτών’ (CA Certificates) που εκδίδει ο ‘Θεμελιώδης Εκδότης Πιστοποιητικών’, έχει - για τον κάθε ένα από τους ‘Λειτουργικούς Εκδότες’ της ‘Υπηρεσίας Έκδοσης Πιστοποιητικών’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ- το εξής περιεχόμενο:

Α) Λειτουργικός Εκδότης ‘Γενικών Πιστοποιητικών Κλάσης 1^{ης}’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ:

Υποπεδίο	Επεξήγηση	Περιεχόμενο
O=	Οργανισμός (Organization)	ATHENS STOCK EXCHANGE
CN=	Κοινό Όνομα (Common Name)	ATHEX General Certificates CA G2
C=	Χώρα (Country)	GR

Β) Λειτουργικός Εκδότης ‘Αναγνωρισμένων Πιστοποιητικών Κλάσης 1^{ης}’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ:

Υποπεδίο	Επεξήγηση	Περιεχόμενο
O=	Οργανισμός (Organization)	ATHENS STOCK EXCHANGE
CN=	Κοινό Όνομα (Common Name)	ATHEX Qualified Certificates CA G2
C=	Χώρα (Country)	GR

5.1.3.3 Διακεκριμένο όνομα (DN) των ‘Θεμάτων’ (Υποκείμενα-Συνδρομητές)

Το διακεκριμένο όνομα (DN) των ‘Συνδρομητών’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ που καταγράφεται στο πεδίο ‘Θέμα’ (Subject) στα ‘Πιστοποιητικά των συνδρομητών/τελικών οντοτήτων’ (End-entities Certificates) που εκδίδει η ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ, ορίζεται -ως προς την δομή του- στην αντίστοιχη ‘Πολιτική Πιστοποιητικού’, ανάλογα και με το αν πρόκειται για ‘προσωπικά πιστοποιητικά’ ή ‘πιστοποιητικά συσκευών’ του συνδρομητή. Επιπλέον στα αναγνωρισμένα πιστοποιητικά που εκδίδονται από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ και αφορούν νομικά πρόσωπα αναγράφεται υποχρεωτικά και το όνομα της εταιρείας, π.χ. «Organization = “Athens Stock Exchange”.

5.1.4 ΧΑΡΑΚΤΗΡΙΣΜΟΣ ΚΡΙΣΙΜΟΤΗΤΑΣ ΤΩΝ ΕΚΤΕΤΑΜΕΝΩΝ ΠΕΔΙΩΝ ΤΟΥ

Αν και όλα τα πεδία του πιστοποιητικού θεωρούνται ‘κρίσιμα’ με την έννοια ότι περιλαμβάνουν απαραίτητες πληροφορίες για τον Εκδότη, το Θέμα, το Πιστοποιητικό και τους Όρους Χρησιμοποίησής του, τα εκτεταμένα πεδία ενός πιστοποιητικού [X.509 - RFC 5280] μπορούν να χαρακτηριστούν με την ένδειξη ‘Critical’ (κρίσιμα) με την έννοια ότι μια αυτοματοποιημένη εφαρμογή ανάγνωσής τους δεν επιτρέπεται να προχωρά στην αποδοχή του πιστοποιητικού στην περίπτωση που δεν μπορεί να ερμηνεύσει το περιεχόμενο ενός τέτοιου πεδίου.

Στα πιστοποιητικά του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ είναι χαρακτηρισμένο ως ‘critical’ το πεδίο ‘Χρήσεις Κλειδιού’ (Key Usage).

5.2 ΠΕΡΙΓΡΑΦΗ ‘ΛΙΣΤΑΣ ΑΝΑΚΛΗΘΕΝΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ’ (ΛΑΠ)

5.2.1 ΤΥΠΟΣ ΚΑΙ ΑΡΙΘΜΟΣ ΕΚΔΟΣΗΣ

Οι ‘Υπηρεσίες Ψηφιακής Πιστοποίησης’ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ χρησιμοποιούν, για τις εκδιδόμενες ΛΑΠ, μορφή σύμφωνη με τις προδιαγραφές [X.509, CRL Version 2] (έκδοση 2η) η οποία υποστηρίζει την χρήση εκτεταμένων πεδίων (extensions). Ο αριθμός της έκδοσης αναφέρεται πάντα στο σχετικό πεδίο του πιστοποιητικού.

5.2.2 ΠΕΡΙΕΧΟΜΕΝΟ ΚΑΙ ΣΗΜΑΣΙΑ ΤΩΝ ΠΕΔΙΩΝ ΜΙΑΣ ΛΑΠ

Οι ΛΑΠ που εκδίδονται από την ΥΔΑ και υπογράφονται από τον κάθε ‘Λειτουργικό Εκδότη’ του δικτύου του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ σχετικά με τα πιστοποιητικά των συνδρομητών/τελικών οντοτήτων που εκδίδονται (αλλά και αυτές που εκδίδονται από τον ΘΕΠ για τα τυχών ανακληθέντα πιστοποιητικά των Εκδοτών του δικτύου), περιέχουν τα εξής πεδία:

Όνομα πεδίου	Υποχρεωτικό	Περιεχόμενο	Παρατηρήσεις
Έκδοση <i>Version</i>	NAI	“V2”	Έκδοση ‘2’ του προτύπου ‘X.509 - RFC 2459 CRL’ που υποστηρίζει εκτεταμένα πεδία.
Αύξων Αριθμός ΛΑΠ <i>CRLNumber</i>	NAI	[Ακέραιος αριθμός]	Μοναδικός αύξων αριθμός που χαρακτηρίζει την συγκεκριμένη ΛΑΠ.
Αλγόριθμος Υπογραφής <i>Signature Algorithm</i>	NAI	[Προσδιοριστικό]	Προσδιορίζει τον αλγόριθμο που χρησιμοποιείται για τον κατακερματισμό (Hash) και την υπογραφή της λίστας.
Εκδότης <i>Issuer</i>	NAI	(Διακεκριμένο Όνομα (DN) τύπου ‘X.501’ για τον Εκδότη)	Το όνομα του εκδότη (που υπογράφει την ΛΑΠ), αναλυμένο σε υπο-πεδία. Δες ανάλυση στην παράγραφο 5.1.3
Παρούσα Έκδοση <i>This Update</i>	NAI	[Ημερομηνία]	Η ημερομηνία και ώρα έκδοσης της παρούσας ενημερωμένης ΛΑΠ.
Επόμενη Έκδοση <i>Next Update</i>	NAI	[Ημερομηνία]	Η ημερομηνία και ώρα της επόμενης προγραμματισμένης έκδοσης ΛΑΠ.
Προσδιοριστικό Κλειδιού Εκδότη <i>Authority Key Identifier</i>	OXI	[Ακέραιος αριθμός]	Προσδιορίζει σε ποιο ζεύγος κλειδιών τον Εκδότη αντιστοιχεί η συγκεκριμένη ΛΑΠ (από το οποίο και υπογράφηκε).
Ανακληθέντα Πιστοποιητικά <i>Revoked Certificates</i>	NAI	[Λίστα Πιστοποιητικών]	Η ενημερωμένη κύρια λίστα με πληροφορίες για τα –έως την έκδοση της ΛΑΠ- ανακληθέντα πιστοποιητικά. (Δες επόμενο πίνακα).

Στο πεδίο ‘Ανακληθέντα Πιστοποιητικά’ (που περιλαμβάνει την κυρίως λίστα των πιστοποιητικών που ανακαλούνται), ακολουθούν τα εξής υπο-πεδία, τα οποία επαναλαμβάνονται για την περιγραφή του κάθε ενός από τα ανακληθέντα πιστοποιητικά:

Όνομα πεδίου	Υποχρεωτικό	Περιεχόμενο	Παρατηρήσεις
Ανακληθέν Πιστοποιητικό ¹ <i>User Certificate</i>	NAI	[Ακέραιος αριθμός]	Ο μοναδικός ‘σειριακός αριθμός’ των πιστοποιητικού που ανακαλείται (-που απέκτησε από τον συγκεκριμένο Εκδότη)
Ημερομηνία Ανάκλησης <i>Revocation Date</i>	NAI	[Ημερομηνία]	Η ημερομηνία και ώρα της έκδοσης της ΛΑΠ με την οποία ανακλήθηκε το συγκεκριμένο πιστοποιητικό.
Αύξων Αριθμός ΛΑΠ <i>Reason Code</i>	NAI	(Byte με ενδείξεις για τον λόγο που ανακλήθηκε το πιστοποιητικό αυτό – σύμφωνα με RFC 2459 ή τα εκάστοτε ισχύοντα πρότυπα)	Προσδιορίζει τον λόγο ανάκλησης του πιστοποιητικού π.χ. ανάκληση λόγω έκθεσης κλειδιών ή απλή παύση (προσωρινή ανάκληση)
Ημερομηνία Απόλειας Ισχύος <i>Invalidity Date</i>	OXI	[Ημερομηνία]	Η ημερομηνία και ώρα της αίτησης για την ανάκληση του πιστοποιητικού αυτού.

5.2.3 ΧΑΡΑΚΤΗΡΙΣΜΟΣ ΚΡΙΣΙΜΟΤΗΤΑΣ ΤΩΝ ΕΚΤΕΤΑΜΕΝΩΝ ΠΕΔΙΩΝ ΤΗΣ

Αν και όλα τα πεδία της ΛΑΠ θεωρούνται ‘κρίσιμα’ με την έννοια ότι περιλαμβάνουν απαραίτητες πληροφορίες για τον Εκδότη, την Ημερομηνία Ανάκλησης, το Πιστοποιητικό που ανακαλείται και τους Λόγους Ανάκλησής του, τα εκτεταμένα πεδία μιας ΛΑΠ μπορούν να χαρακτηριστούν και με την ένδειξη ‘Critical’ (κρίσιμα), με την έννοια ότι μια αυτοματοποιημένη εφαρμογή δεν πρέπει να προχωρά στην επεξεργασία της συγκεκριμένης ΛΑΠ, εάν δεν μπορεί να ερμηνεύσει το περιεχόμενο ενός τέτοιου πεδίου της.

Στις ΛΑΠ που εκδίδονται από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ δεν είναι χαρακτηρισμένο ως ‘critical’ κανένα πεδίο.