ATHEX
Χρηματιστήριο Αθηνών

ΥΠΗΡΕΣΙΕΣ ΨΗΦΙΑΚΗΣ ΠΙΣΤΟΠΟΙΗΣΗΣ

ΠΟΛΙΤΙΚΗ ΑΝΑΓΝΩΡΙΣΜΕΝΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

‘*SMART-SIGN™*’

(Qualified Certificate Policy *‘SMART-SIGN™’*)

Έκδοση 1.2 – 1/06/2017

ΠΕΡΙΛΑΜΒΑΝΕΙ ΤΙΣ ΠΟΛΙΤΙΚΕΣ ΓΙΑ ΤΑ ΠΙΣΤΟΠΟΙΗΤΙΚΑ:

(INCLUDES POLICIES FOR THE CERTIFICATES:)

1. «Αναγνωρισμένο Προσωπικό Πιστοποιητικό SMART-SIGN™ »
(*για Αναγνωρισμένες Ηλεκτρονικές Υπογραφές*)
(1. Qualified Personal Certificate ‘Smart-Sign –’ (for Qualified Electronic Signatures)**)**

Αναγνωριστικός Αριθμός Πολιτικής (OID): **1.3.6.1.4.1.29402.*1.2.1.1.1.1***

{ εσκεμμένα κενή }

- ΠΕΡΙΕΧΟΜΕΝΑ -

1 ΕΙΣΑΓΩΓΗ 5
1.1 ΓΕΝΙΚΗ ΕΠΙΣΚΟΠΗΣΗ 5
1.1.1 Προσωπικά Πιστοποιητικά τύπου SMART-SIGN™ (διπλού κλειδιού) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ 5
1.1.2 Προσωπικά Πιστοποιητικά τύπου SMART-SIGN™ (Remote sign) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ 5
1.1.3 Κλάσεις των προσωπικών πιστοποιητικών SMART-SIGN™ 6
1.1.4 Βασικές ιδιότητες των πιστοποιητικών 'SMART-SIGN ™' 6
1.2 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΑΙ ΤΑΥΤΟΤΗΤΑ ΤΩΝ ΠΟΛΙΤΙΚΩΝ 6
1.2.1 Φύση της 'Πολιτικής Αναγνωρισμένου Πιστοποιητικού' και σχέση της με τον 'Κανονισμό Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών' (C.P.S. Q.C.) 6
1.2.2 Δομή και περιεχόμενο του κειμένου - Συμμόρφωση με πρότυπα 7
1.2.3 Αναφορές και 'Αναγνωριστικοί Αριθμοί' (OIDs) 7

2 ΚΟΙΝΟΤΗΤΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΤΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ 9
2.1 ΚΟΙΝΟΤΗΤΑ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ 9
2.1.1 Πάροχος Υπηρεσιών Πιστοποίησης, Εκδότης Πιστοποιητικών (CA) & Υπο-εκδότες (Sub-CAs) 9
2.1.2 Υπηρεσία Εγγραφής (RA) 9
2.1.3 Υπηρεσία Προετοιμασίας Φορέα Συνδρομητή (Υ.Π.Φ.Σ.) 10
2.1.4 Τοπικές Υπηρεσίες Υποβολής (Τ.Υ.Υ.) 10
2.1.5 Συνδρομητής (υποκείμενο πιστοποίησης) 10
2.1.6 Αποδέκτης (ή 'χρήστης' ή 'τρίτο βασιζόμενο μέρος') 11
2.2 ΕΦΑΡΜΟΓΕΣ ΚΑΙ ΠΕΡΙΟΡΙΣΜΟΙ ΧΡΗΣΗΣ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ 11
2.2.1 Εφαρμογές των πιστοποιητικών 'SMART-SIGN' 11
2.2.2 Περιορισμοί στην χρήση των πιστοποιητικών 'SMART-SIGN' 12
2.2.3 Όρια στην αξία των συναλλαγών με χρήση των πιστοποιητικών 'SMART-SIGN –Κλάσης 2ης' 12

3 ΥΠΟΧΡΕΩΣΕΙΣ, ΕΓΓΥΗΣΕΙΣ ΚΑΙ ΟΡΙΑ ΕΥΘΥΝΗΣ 13
3.1 ΥΠΟΧΡΕΩΣΕΙΣ ΤΩΝ ΕΜΠΛΕΚΟΜΕΝΩΝ ΜΕΡΩΝ 13
3.1.1 Υποχρεώσεις του Παρόχου Υπηρεσιών Πιστοποίησης 13
3.1.2 Υποχρεώσεις του συνδρομητή – υποκείμενου πιστοποίησης 13
3.1.3 Υποχρεώσεις τρίτων αποδεκτών –χρηστών του πιστοποιητικού 14
3.2 ΕΓΓΥΗΣΕΙΣ, ΑΠΟΠΟΙΗΣΗ ΕΥΘΥΝΗΣ ΚΑΙ ΑΝΩΤΑΤΟ ΟΡΙΟ ΕΥΘΥΝΗΣ ΤΟΥ Π.Υ.Π. ... 14
3.2.1 Εγγυήσεις του Παρόχου Υπηρεσιών Πιστοποίησης 14
3.2.2 Αποποίηση ευθύνης -εξαιρέσεις 14

4 ΤΑΥΤΟΠΟΙΗΣΗ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ 16
4.1 ΠΟΛΙΤΙΚΗ ΟΝΟΜΑΣΙΑΣ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ 16
4.1.1 Προσωπικά στοιχεία του υποκειμένου που εμφανίζονται στο πιστοποιητικό 16
4.1.2 Απόδοση του ονόματος με λατινικούς χαρακτήρες (ΕΛΟΤ 743) 16
4.1.3 Επίλυση διαφορών στην ονομασία του υποκειμένου 16
4.2 ΕΞΑΚΡΙΒΩΣΗ ΤΗΣ ΤΑΥΤΟΤΗΤΑΣ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ 16
4.2.1 Στην αρχική εγγραφή 16
4.2.2 Στην τακτική ανανέωση των πιστοποιητικών (πριν λήξουν ή ανακληθούν) 17
4.2.3 Στην ανανέωση πιστοποιητικών μετά από λήξη ή ανάκλησή τους 17
4.2.4 Στην αίτηση αναστολής ή ανάκλησης 17
4.2.5 Στην αίτηση επαν-ενεργοποίησης (μετά από παύση) 17
4.3 ΑΠΟΔΕΙΞΗ ΚΑΤΟΧΗΣ ΤΟΥ ΙΔΙΩΤΙΚΟΥ ΚΛΕΙΔΙΟΥ ΑΠΟ ΤΟ ΥΠΟΚΕΙΜΕΝΟ 17
4.3.1 Δημιουργία των κλειδιών σε εξατομικευμένο φορέα 'α.δ.δ.υ.' 17
4.3.2 Αποστολή του φορέα 'α.δ.δ.υ.' και κωδικού ενεργοποίησής του (PIN) στον συνδρομητή 18

4.3.3 Αναστολή των πιστοποιητικών έως την Αρχική Ενεργοποίηση 18

5 ΟΡΟΙ ΔΙΑΧΕΙΡΙΣΗΣ ΚΥΚΛΟΥ ΖΩΗΣ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ 19
5.1 ΑΙΤΗΣΗ, ΕΚΔΟΣΗ ΚΑΙ ΕΝΕΡΓΟΠΟΙΗΣΗ 19
5.1.1 Αίτηση του υποκειμένου και διαδικασία έγκρισης της αίτησης 19
5.1.2 Εξατομίκευση φορέα και δημιουργία ζεύγους κλειδιών 19
5.1.3 Έκδοση των πιστοποιητικών και αποστολή τους στον συνδρομητή 20
5.1.4 Αρχική Ενεργοποίηση των πιστοποιητικών 20
5.2 ΙΣΧΥΣ, ΛΗΞΗ ΚΑΙ ΑΝΑΝΕΩΣΗ 20
5.2.1 Διάρκεια ισχύος των πιστοποιητικών 20
5.2.2 Λήξη ισχύος των πιστοποιητικών 20
5.2.3 Ανανέωση των πιστοποιητικών 21
5.3 ΑΝΑΣΤΟΛΗ, ΑΝΑΚΛΗΣΗ ΚΑΙ (ΕΠΑΝ-)ΕΝΕΡΓΟΠΟΙΗΣΗ 21
5.3.1 Αναστολή και ανάκληση του πιστοποιητικού 21
5.3.2 Ενεργοποίηση μετά από αναστολή 22
5.4 ΥΠΗΡΕΣΙΕΣ ΔΗΜΟΣΙΕΥΣΗΣ ΚΑΤΑΣΤΑΣΗΣ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ 22
5.4.1 Υπηρεσία Καταλόγου εκδοθέντων πιστοποιητικών 22
5.4.2 Υπηρεσία καταλόγου ανασταλθέντων και ανακληθέντων πιστοποιητικών (CRL) 23

6 ΕΓΚΥΡΟΤΗΤΑ ΚΑΙ ΑΠΟΔΕΙΚΤΙΚΗ ΙΚΑΝΟΤΗΤΑ 24
6.1 ΕΛΕΓΧΟΣ ΕΓΚΥΡΟΤΗΤΑΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ & ΥΠΟΓΕΓΡΑΜΜΕΝΩΝ ΕΓΓΡΑΦΩΝ ..24
6.1.1 Έλεγχος εγκυρότητας των προσωπικών πιστοποιητικών SMART-SIGN™ 24
6.1.2 Εγκατάσταση και έλεγχος εγκυρότητας της αλυσίδας των ιεραρχικά ανώτερων πιστοποιητικών 24
6.1.3 Μακροχρόνιος έλεγχος υπογεγραμμένων εγγράφων -Χρονοσήμανση (time stamping) 24
6.2 ΣΤΟΙΧΕΙΑ ΠΟΥ ΚΑΤΑΧΩΡΟΥΝΤΑΙ – ΠΡΟΣΒΑΣΗ - ΧΡΟΝΟΣ ΑΡΧΕΙΟΘΕΤΗΣΗΣ 25
6.2.1 Αποδεικτικά στοιχεία που καταχωρούνται κατά τη διαχείριση των πιστοποιητικών 25
6.2.2 Περίοδος αρχειοθέτησης 25
6.2.3 Πρόσβαση στα αποδεικτικά στοιχεία 25

7 ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ & ΑΞΙΟΠΙΣΤΙΑΣ 26
7.1 ΤΕΧΝΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ 26
7.1.1 Κρυπτογραφικά κλειδιά του Εκδότη των πιστοποιητικών 26
7.1.2 Κρυπτογραφικά κλειδιά και Φορέας 'α.δ.δ.υ.' των ιδιωτικών κλειδιών των συνδρομητών 26
7.1.3 Απαγόρευση επιμερισμού (escrow) ή άλλης διαδικασίας ανάκτησης των ιδιωτικών κλειδιών 26
7.2 ΑΛΛΕΣ ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΑΞΙΟΠΙΣΤΙΑΣ ΤΟΥ Π.Υ.Π. 26
7.2.1 Αξιοπιστία συστήματος του Π.Υ.Π. – Συμμόρφωση με διεθνή πρότυπα ασφάλειας 26
7.2.2 Φυσική ασφάλεια, Ασφάλεια διαδικασιών, Εκπαίδευση και έλεγχος αξιοπιστίας προσωπικού 27
7.2.3 Οικονομική αξιοπιστία και επιβιωσιμότητα του Π.Υ.Π. 27
7.2.4 Λειτουργική αυτοτέλεια 27

8 ΠΕΡΙΓΡΑΦΗ (PROFILE) ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ & Λ.Α.Π. (C.R.L.) 28
8.1 ΠΕΡΙΓΡΑΦΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ 28
8.1.1 Τύπος και αριθμός έκδοσης 28
8.1.2 Περιεχόμενο και σημασία των πεδίων των πιστοποιητικών 28
8.1.3 Τύπος και περιεχόμενο των διακεκριμένων ονομάτων (dn) 29
8.1.4 Διακεκριμένο όνομα (DN) του 'Εκδότη Πιστοποιητικών' (Issuer) 29
8.1.5 Διακεκριμένο όνομα (DN) του 'Συνδρομητών' ('Θέμα' ή 'Subject') 29
8.1.6 Πεδία που χαρακτηρίζονται 'Κρίσιμα' (Critical) 30
8.2 ΔΙΑΡΘΡΩΣΗ (PROFILE) ΛΙΣΤΑΣ ΑΝΑΚΛΗΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ (ΛΑΠ ή CRL) 30
8.2.1 Τύπος και αριθμός έκδοσης 30
8.2.2 Περιεχόμενο και σημασία των πεδίων της ΛΑΠ 30
8.2.3 Πεδία που χαρακτηρίζονται 'Κρίσιμα' (Critical) 31

9 ΑΛΛΟΙ ΓΕΝΙΚΟΙ ΟΡΟΙ 32
9.1 ΔΙΚΑΙΩΜΑΤΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ 32
9.1.1 Δικαιώματα πνευματικής ιδιοκτησίας 32
9.1.2 Εμπορικά σήματα και άλλες ιδιοκτησίες 32
9.1.3 Προστασία δεδομένων προσωπικού χαρακτήρα 32
9.1.4 Πολιτική επίλυσης διαφορών και παραπόνων 32
9.2 ΤΙΜΟΛΟΓΙΑΚΗ ΠΟΛΙΤΙΚΗ 33
9.2.1 Δημοσίευση τιμολογιακής πολιτικής 33
9.2.2 Περιπτώσεις επιστροφής της καταβληθείσας συνδρομής 33
9.3 ΕΡΜΗΝΕΙΑ ΚΑΙ ΕΚΤΕΛΕΣΤΟΤΗΤΑ 33
9.3.1 Αυθεντική ερμηνεία των όρων του παρόντος στις συγκριτικές αξιολογήσεις 33
9.3.2 Εκτελεστότητα - Διατηρησιμότητα των μη άκυρων όρων 33
9.3.3 Εφαρμοστέο δίκαιο και αρμόδια δικαστήρια 34

10 ΔΙΑΧΕΙΡΙΣΗ ΚΑΙ ΑΝΑΘΕΩΡΗΣΗ ΤΗΣ ΠΟΛΙΤΙΚΗΣ 35
10.1 ΥΠΕΥΘΥΝΟΣ ΕΚΔΟΣΗΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗΣ 35
10.1.1 Ονομασία – Αρμοδιότητες –Υποχρεώσεις 35
10.1.2 Στοιχεία Επικοινωνίας 35
10.2 ΑΝΑΘΕΩΡΗΣΗ ΤΩΝ ΠΟΛΙΤΙΚΩΝ 36
10.2.1 Υποβολή, έγκριση και δημοσίευση των αναθεωρημένων εκδόσεων 36
10.2.2 Κρισιμότητα των αναθεωρήσεων και σχετική αριθμοδότηση 36
10.2.3 Αναδρομικότητα ισχύος της αναθεωρημένης έκδοσης 36
10.3 ΣΥΓΚΡΙΤΙΚΕΣ ΑΞΙΟΛΟΓΗΣΕΙΣ ΣΧΕΤΙΚΑ ΜΕ ΤΙΣ ΠΑΡΟΥΣΕΣ ΠΟΛΙΤΙΚΕΣ 37
10.3.1 Απόδοση ισοδυναμίας με άλλες πολιτικές πιστοποιητικών (policy mapping) 37
10.3.2 Έγκριση Κανονισμών Πιστοποίησης ως σύμφωνων με τις παρούσες πολιτικές 37

ΠΟΛΙΤΙΚΕΣ ΠΡΟΣΩΠΙΚΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

ΤΥΠΟΥ 'SMART-SIGN™' ΤΟΥ ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ,

ΣΗΜΑΝΤΙΚΕΣ ΔΗΛΩΣΕΙΣ:

1) Το πιστοποιητικό που συμμορφώνεται με την εμπεριεχόμενη στο παρόν κείμενο «**Πολιτική Αναγνωρισμένου Προσωπικού Πιστοποιητικού 'SMART-SIGN'™ -Κλάσης 2ης, Έκδοση 1.1» (OID 11.3.6.1.4.1.29402.1.2.1.1.1.1)**, εκδίδεται **με πρόθεση** ως «**Αναγνωρισμένο Πιστοποιητικό**» και ο Εκδότης του **δηλώνει** ότι η έκδοσή του συμμορφώνεται με τις απαιτήσεις του Κανονισμού 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές

1 ΕΙΣΑΓΩΓΗ

1.1 ΓΕΝΙΚΗ ΕΠΙΣΚΟΠΗΣΗ

1.1.1 Προσωπικά Πιστοποιητικά τύπου SMART-SIGN™ (διπλού κλειδιού) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ

Οι '*Υπηρεσίες Ψηφιακής Πιστοποίησης*' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ Α.Ε. δημιούργησαν, υποστηρίζουν και διαχειρίζονται -διαμέσου της 'Επιτροπής Διαχείρισης Πολιτικής'- τον 'τύπο' ηλεκτρονικών προσωπικών πιστοποιητικών '**SMART-SIGN™ (διπλού κλειδιού)**' για την πιστοποίηση των «δεδομένων επαλήθευσης ηλεκτρονικής υπογραφής» (δημόσια κλειδιά) **φυσικών προσώπων**. Ο τύπος '**SMART-SIGN™ (διπλού κλειδιού)**' χαρακτηρίζεται από την παράλληλη έκδοση και διαχείριση **δύο διαφορετικών συμπληρωματικών πιστοποιητικών** (*που αντιστοιχούν σε δύο διαφορετικά ζεύγη κρυπτογραφικών κλειδιών*) **σε έναν εξατομικευμένο φορέα** που αποτελεί «ασφαλή διάταξη δημιουργίας υπογραφής».

Με το σχήμα αυτό, οι '*Υπηρεσίες Ψηφιακής Πιστοποίησης*' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ Α.Ε. (στο εξής 'ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ'), επιτυγχάνουν την συνέκδοση και συνύπαρξη:

(α) ενός '**αναγνωρισμένου προσωπικού πιστοποιητικού**' (*για την ασφαλή υπογραφή ηλεκτρονικών εγγράφων με εξασφαλισμένη και ισότιμη με την ιδιόχειρη υπογραφή ισχύ*) και

(β) ενός '**προσωπικού πιστοποιητικού ταυτοποίησης**' ('authentication' – *για την ασφαλή αναγνώριση και ταυτοποίηση του κατόχου του σε συμβατές τηλεματικές εφαρμογές*),

με την **εύκολη χρήση κοινού φορέα** (και την χρήση ενός κοινού κωδικού ενεργοποίησής 'PIN'), **τηρώντας ταυτόχρονα και τις πιο αυστηρές προδιαγραφές** όπως προσδιορίζονται στον Κανονισμό 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές.

Σημειώνεται, ότι κατά την παρούσα εισαγωγή, για λόγους πληρότητας και άμεσης σχέσης μεταξύ των πιστοποιητικών διπλού κλειδιού, πραγματοποιείται αναφορά τόσο στα αναγνωρισμένα πιστοποιητικά όσο και στα μη-αναγνωρισμένα. Για λεπτομέρειες αναφορικά με τα μη-αναγνωρισμένα πιστοποιητικά παρακαλώ όπως αναφερθείτε στην Πολιτική Μη Αναγνωρισμένων Πιστοποιητικών OID 1.3.6.1.4.1.294021.1.2.2.1.1.1.

Συγκεκριμένα, η χρήση των δύο διαφορετικών πιστοποιητικών SMART-SIGN (για δύο διαφορετικά κρυπτογραφικά ζεύγη κλειδιών) **διαχωρίζει απόλυτα** την χρήση της 'προηγμένης ηλεκτρονικής υπογραφής' του υποκειμένου για '*ενσυνείδητη δημιουργία υπογραφής χωρίς την δυνατότητα αποκήρυξής της*' (Non-Repudiation), από **άλλες χρήσεις** των ηλεκτρονικών υπογραφών (π.χ. ταυτοποίηση σε περιβάλλον web, 'υπογραφή' ηλεκτρονικού ταχυδρομείου, κρυπτογράφηση κλειδιών και δεδομένων, κ.ά) των οποίων η νομική τους υπόσταση περιορίζεται σ' αυτήν των 'αποδεικτικών στοιχείων', σύμφωνα με τον νόμο.

1.1.2 Προσωπικά Πιστοποιητικά τύπου SMART-SIGN™ (Remote sign) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ

Οι '*Υπηρεσίες Ψηφιακής Πιστοποίησης*' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ Α.Ε. δημιούργησαν, υποστηρίζουν και διαχειρίζονται -διαμέσου της 'Επιτροπής Διαχείρισης Πολιτικής'- τον 'τύπο' ηλεκτρονικών προσωπικών πιστοποιητικών '**SMART-SIGN™ (**Remote sign**)**' για την πιστοποίηση των «δεδομένων

επαλήθευσης ηλεκτρονικής υπογραφής» (δημόσια κλειδιά) **φυσικών προσώπων** με την **χρήση cloud Hardware Security Module (HSM) τηρώντας ταυτόχρονα και τις πιο αυστηρές προδιαγραφές** όπως προσδιορίζονται στον Κανονισμό 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 σχετικά με την ηλεκτρονική ταυτοποίηση και τις υπηρεσίες εμπιστοσύνης για τις ηλεκτρονικές συναλλαγές.

1.1.3 Κλάσεις των προσωπικών πιστοποιητικών SMART-SIGN™

Τα προσωπικά πιστοποιητικά '**SMART-SIGN™** διακρίνονται σε '**Κλάσεις**' οι οποίες προσδιορίζουν κυρίως το πεδίο εφαρμογής και το ύψος των συναλλαγών για τα οποία επιτρέπεται η χρησιμοποίησή τους και, αντίστοιχα, το ανώτατο όριο ευθύνης που αναλαμβάνει ο εκδότης τους. Με τις κλάσεις δημιουργείται διαβάθμιση των πιστοποιητικών '**SMART-SIGN™**' σε διαφορετικά προσφερόμενα επίπεδα εγγυήσεων και τιμολογιακής πολιτικής προοριζόμενα για διαφορετικές συναλλακτικές ανάγκες του κατόχου τους στην κοινωνία της πληροφορίας.

Ένα 'πακέτο' προσωπικών πιστοποιητικών '**SMART-SIGN™ (διπλού κλειδιού)**' περιέχει **πάντα δύο συμπληρωματικά πιστοποιητικά της ίδιας 'κλάσης'** (ένα 'αναγνωρισμένο πιστοποιητικό' & ένα 'πιστοποιητικό ταυτοποίησης').

1.1.4 Βασικές ιδιότητες των πιστοποιητικών 'SMART-SIGN ™'

Τα προσωπικά πιστοποιητικά '**SMART-SIGN™** ' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, εκδίδονται μόνο σε φυσικά πρόσωπα ή νόμιμους εκπροσώπους νομικών προσώπων κατόπιν κοινής αίτησης-σύμβασής τους με τον εκδότη τους (συνδρομητική σύμβαση) και εναποθηκεύονται πάντα στον ίδιο εξατομικευμένο φορέα -μαζί με τα σχετικά ζεύγη κρυπτογραφικών κλειδιών που πιστοποιούν.

Η συνύπαρξή τους σε κοινό φορέα και η στήριξή τους σε κοινή αίτηση-σύμβαση και δικαιολογητικά έκδοσής τους συνεπάγεται την **πλήρη αλληλοεπίδραση στην ισχύ τους**. Αυτό σημαίνει ότι οποιαδήποτε πράξη επιδρά στην ισχύ του ενός από τα πιστοποιητικά του ζεύγους πιστοποιητικών '**SMART-SIGN™ (διπλού κλειδιού)**' –όπως π.χ. ενεργοποίηση, παύση, ανάκληση ή λήξη-, επιδρά ταυτόχρονα και ανάλογα και στο άλλο πιστοποιητικό.

Επακόλουθο της κοινής διαχείρισης και της αλληλεξάρτησης των πιστοποιητικών που απαρτίζουν ένα ζεύγος πιστοποιητικών τύπου '**SMART-SIGN™**' είναι η υπαγωγή τους σε κοινή -σχεδόν- 'πολιτική' που διαφοροποιείται κυρίως στους περιορισμούς του πεδίου εφαρμογής τους (*βλ. παραγρ. 2.2 'Εφαρμογές και περιορισμοί χρήσης των πιστοποιητικών'*) και σε ορισμένες από τις τεχνικές προδιαγραφές τους.

Με το παραπάνω σχήμα, το υψηλό επίπεδο ασφάλειας και διαχείρισης που επιβάλλουν η κείμενη νομοθεσία και τα ευρωπαϊκά πρότυπα για το 'αναγνωρισμένο πιστοποιητικό' (ώστε να είναι ικανό να υποστηρίζει υπογραφές ηλεκτρονικών εγγράφων ισότιμες σε ισχύ με τις ιδιόχειρες υπογραφές), προσφέρεται ταυτόχρονα και στο συνοδευόμενο 'πιστοποιητικό ταυτοποίησης', το οποίο, μόνο κατά δήλωση της παρούσας πολιτικής του, **δεν** εκδίδεται ως 'αναγνωρισμένο' (σύμφωνα με τον ορισμό του νόμου).

1.2 ΧΑΡΑΚΤΗΡΙΣΤΙΚΑ ΚΑΙ ΤΑΥΤΟΤΗΤΑ ΤΩΝ ΠΟΛΙΤΙΚΩΝ

1.2.1 Φύση της 'Πολιτικής Αναγνωρισμένου Πιστοποιητικού' και σχέση της με τον 'Κανονισμό Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών' (C.P.S. Q.C.)

Η 'Πολιτική Αναγνωρισμένου Πιστοποιητικού' *(Qualified Certificate Policy – Q.C.P.)* ορίζει τους βασικούς όρους έκδοσης, διαχείρισης και χρήσης καθώς και τις προδιαγραφές ενός συγκεκριμένου τύπου ηλεκτρονικού πιστοποιητικού, **ανεξάρτητα από το ποιος είναι ο εκδότης του.**

Έτσι, η πολιτική πιστοποιητικού προσδιορίζει «***ένα σύνολο κανόνων, ικανών να υποδείξουν την καταλληλότητα του πιστοποιητικού σε μια συγκεκριμένη κοινότητα ή/και κλάση εφαρμογών με κοινές απαιτήσεις ασφαλείας***» και απευθύνεται ταυτόχρονα τόσο στον 'Πάροχο Υπηρεσιών Πιστοποίησης' *(Certification Service Provider – CSP)*, όσο και στο κάτοχο του πιστοποιητικού *(υποκείμενο πιστοποίησης - subject)* καθώς και στους τρίτους-αποδέκτες *(βασιζόμενα μέρη –relying parties)* του πιστοποιητικού αυτού, **έχοντας την νομική ισχύ να δεσμεύει ή/και να λειτουργεί προς όφελος όλων των εμπλεκόμενων μερών.**

Από την άλλη μεριά, ο 'Κανονισμός Πιστοποίησης για Αναγνωρισμένα Πιστοποιητικά' *(Certification Practice Statement for Qualified Certificates – C.P.S Q.C..)* έχει ως αντικείμενο «***να προσδιορίσει τον τρόπο οργάνωσης και λειτουργίας καθώς και τις πρακτικές και τους κανόνες ασφαλείας***» που ακολουθούνται από έναν συγκεκριμένο Πάροχο Υπηρεσιών Πιστοποίησης *(Certification Service Provider – CSP*), **αναφορικά με τα αναγνωρισμένα πιστοποιητικά.**

Συμπερασματικά, η 'Πολιτική Αναγνωρισμένου Πιστοποιητικού' ορίζει «***τι*** *κανόνες πρέπει να ακολουθηθούν*» για την έκδοση και διαχείριση ενός συγκεκριμένου πιστοποιητικού ενώ ο 'Κανονισμός Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών' καθορίζει «***πως*** *εφαρμόζονται οι κανόνες*» από έναν Πάροχο Υπηρεσιών Πιστοποίησης (στο εξής Π.Υ.Π.). Άρα, για να εκδώσει ένας Π.Υ.Π. ένα συγκεκριμένο πιστοποιητικό θα πρέπει να έχει διαπιστωθεί από τον 'Υπεύθυνο Διαχείρισης Πολιτικής' (Policy Management Authority) του πιστοποιητικού, η συμμόρφωση του 'Κανονισμού Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών' του με τις απαιτήσεις της σχετικής 'Πολιτικής Πιστοποιητικού για Αναγνωρισμένα Πιστοποιητικά'.

Σημείωση: '*Υπεύθυνος Διαχείρισης Πολιτικής' αρμόδιος να διαπιστώνει την συμμόρφωση του 'Κανονισμού Πιστοποίησης' ενός Π.Υ.Π. (-ακόμη και της ίδιας του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ!) με τις παρούσες πολιτικές των πιστοποιητικών τύπου SMART-SIGN™, είναι η «Επιτροπή Διαχείρισης Πολιτικών» του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ –βλ. τελευταίο κεφάλαιο για περισσότερες πληροφορίες και στοιχεία επικοινωνίας.*

1.2.2 Δομή και περιεχόμενο του κειμένου - Συμμόρφωση με πρότυπα

Η δομή του κειμένου **βασίζεται** στο πρότυπο *IETF 2527 (1999) 'Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework'.*

Όσον αφορά την 'διάρθρωση' των πιστοποιητικών (certificate profile) και της Λίστας Ανακληθέντων Πιστοποιητικών ('ΛΑΠ' ή 'CRL'), τους χρησιμοποιούμενους αλγόριθμους, την χρήση των πεδίων X.509 - RFC 5280 και τις επιταγές του Κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014 για το περιεχόμενο και τις δηλώσεις του 'αναγνωρισμένου πιστοποιητικού', οι παρούσες πολιτικές (ακόμη και η πολιτική των μη αναγνωρισμένων πιστοποιητικών) υιοθετούν τις υποδείξεις των προτύπων *IETF RFC 5280 (2008): 'Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile', IETF RFC 3739 (2004): 'Internet X.509 Public Key Infrastructure: Qualified Certificates Profile'', ETSI EN 319 412-2 (2016-02) Certificate profile for certificates issued to natural persons* και *ETSI EN 319 412-5 (2016-02): QC Statements*.

Η παρούσα πολιτική του 'αναγνωρισμένου προσωπικού πιστοποιητικού' τύπου 'SMART-SIGNTM' – Κλάσης 1ης, σε συνδυασμό με την τήρηση των απαιτήσεων ασφαλείας που απαιτεί από τον Εκδότη του Πιστοποιητικού και την υποχρεωτική χρήση 'ασφαλούς διατάξεως δημιουργίας υπογραφής' από τον συνδρομητή (δες παράγραφο 4.3.1) δηλώνει συμμόρφωση με την πολιτική 'QCP-n-qscd' (=πολιτική πιστοποιητικού για EU 'αναγνωρισμένα πιστοποιητικά' που εκδίδονται σε φυσικά πρόσωπα και το ιδιωτικό κλειδί που σχετίζεται με το δημόσιο κλειδί απαιτεί την χρήση 'ασφαλούς διατάξεως δημιουργίας υπογραφής') με αριθμό αναγνώρισης (OID): 0.4.0.194112.1.2 που καθορίζει το πρότυπο ETSI EN 319 411-2 (2016-02): Policy requirements for certification authorities issuing qualified certificates.

1.2.3 Αναφορές και 'Αναγνωριστικοί Αριθμοί' (OIDs)

Το παρόν κείμενο πρέπει να αναφέρεται με τον τίτλο «*Πολιτική Αναγνωρισμένων Πιστοποιητικών τύπου 'SMART-SIGN™') του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ*» ή με την σύμπτυξη: «**Π.Α.Π. SMART-SIGN** ».

Σε μηχανογραφικές εφαρμογές, καθώς και στο σχετικό πεδίο του κάθε πιστοποιητικού, οι παρούσες πολιτικές αναφέρονται με τους - παγκοσμίως μοναδικούς - **αναγνωριστικούς αριθμούς (OID)** του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ:

1.3.6.1.4.1.29402.1.2.1.1.1.1	για την «**Πολιτική Α.Π.Π. 'SMART-SIGN' - Κλάσης 2ης, Έκδοση 1.0**»

όπου:

1.3.6.1.4.1.29402	Αριθμός Αναγνώρισης (OID) του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΏΝ,
1	Ανεξάρτητο τμήμα «Υπηρεσιών Δημοσίας Πιστοποίησης» του
2	Πολιτικές Πιστοποιητικών
1	'Αναγνωρισμένο Πιστοποιητικό'
1	Κλάση πιστοποιητικού (2η)
1.1	Πρώτο και δεύτερο ψηφίο του αριθμού έκδοσης

2 ΚΟΙΝΟΤΗΤΑ ΚΑΙ ΕΦΑΡΜΟΓΕΣ ΤΟΥ ΠΙΣΤΟΠΟΙΗΤΙΚΟΥ

2.1 ΚΟΙΝΟΤΗΤΑ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

2.1.1 Πάροχος Υπηρεσιών Πιστοποίησης, Εκδότης Πιστοποιητικών (CA) & Υπο-εκδότες (Sub-CAs)

Ο συμμορφούμενος με τις παρούσες πολιτικές Π.Υ.Π. υποστηρίζεται λειτουργικά τουλάχιστον από μία '*Υπηρεσία Έκδοσης Πιστοποιητικών*', από μία '*Υπηρεσία Εγγραφής*' (βλ. παρακάτω), από μία '*Υπηρεσία Διαχείρισης Ανάκλησης*' (για την διαχείριση των αιτήσεων παύσης, ανάκλησης ή/και ενεργοποίησης των πιστοποιητικών), από μία '*Υπηρεσία Προετοιμασίας Φορέα Συνδρομητών*' (βλ. παρακάτω) και από μία '*Υπηρεσία Δημοσίευσης*' η οποία δημοσιεύει προς το κοινό όλες τις απαραίτητες πληροφορίες.

Η 'Υπηρεσία Έκδοσης Πιστοποιητικών' (Υ.Ε.Π.) ή αλλιώς ο 'Εκδότης' των πιστοποιητικών (Certification Authority –C.A.) αποτελεί τον **βασικό κορμό** στην λειτουργία του 'Παρόχου Υπηρεσιών Πιστοποίησης' (Π.Υ.Π.) και είναι αυτός που υπογράφει (ψηφιακά) τα πιστοποιητικά τύπου SMART-SIGN και τις σχετικές Λίστες (καταλόγους) με τα ανασταλθέντα ή ανακληθέντα πιστοποιητικά (ΛΑΠ). Ο Εκδότης των πιστοποιητικών, σε σχέση με τους τρίτους, **ταυτίζεται -νομικά- με τον Π.Υ.Π.,** ο οποίος εκδίδει τον δικό του **Κανονισμό Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών** ('Κ.Π. Α.Π.' ή 'C.P.S. Q.C.') και ελέγχει για την τήρησή του ολόκληρο το δίκτυο παροχής των 'Υπηρεσιών Ψηφιακής Πιστοποίησής' του, **αναλαμβάνοντας εξ ολοκλήρου την ευθύνη απέναντι στους τρίτους/αποδέκτες που βασίζονται δικαιολογημένα στα πιστοποιητικά του.**

Επειδή το κρυπτογραφικό ζεύγος κλειδιών που χρησιμοποιείται για την ηλεκτρονική υπογραφή του 'αναγνωρισμένου πιστοποιητικού' (και της σχετικής ΛΑΠ) που περιλαμβάνεται στο πακέτο SMART-SIGN **δεν** πρέπει να χρησιμοποιείται για την υπογραφή και άλλων ειδών πιστοποιητικού, ο Εκδότης των πιστοποιητικών τύπου SMART-SIGN χρησιμοποιεί **δύο διαφορετικούς 'Υπο-Εκδότες Πιστοποιητικών'** ή αλλιώς '**Λειτουργικούς Εκδότες Πιστοποιητικών**' ('Sub-CAs' ή 'Operational CAs'), κατόχους διαφορετικών κρυπτογραφικών κλειδιών, (όπου ο ένας υπογράφει το 'αναγνωρισμένο' πιστοποιητικό και ο άλλος υπογράφει το πιστοποιητικό 'ταυτοποίησης'), των οποίων όμως τα πιστοποιητικά υπογράφει ο ίδιος ο Π.Υ.Π.. Έτσι, στο πεδίο '**Issuer**' (Εκδότης) που εμφανίζεται στα πιστοποιητικά SMART-SIGN, ο Π.Υ.Π. αναφέρεται στο υποπεδίο «**O**» (=**O**rganization) ενώ ο αντίστοιχος Υπο-εκδότης του στο πρώτο υποπεδίο «**OU**» (=Organization Unit).

Το πιστοποιητικό του ίδιου του Εκδότη μπορεί να είναι **είτε** αυτο-υπογραφόμενο (*self-signed*) οπότε ο χρήστης/αποδέκτης των πιστοποιητικών του πρέπει να το έχει εγκαταστήσει στο τερματικό του ως αξιόπιστο '**Θεμελιώδη Εκδότη Πιστοποιητικών**' ('Θ.Ε.Π.' ή 'Root CA'), **είτε** υπογραφόμενο από άλλον αποδεκτό Θ.Ε.Π..

2.1.2 Υπηρεσία Εγγραφής (RA)

Η 'Υπηρεσία Εγγραφής' (Registration Authority –R.A.) είναι η υπηρεσία που ελέγχει τις αιτήσεις των φυσικών προσώπων που επιθυμούν να αποκτήσουν προσωπικά πιστοποιητικά SMART-SIGN ως προς την ακρίβεια και την αρτιότητά τους και εφόσον τις **εγκρίνει**, δίνει την σχετική εντολή προς τον Εκδότη για την έκδοσή τους, συνοδευόμενη με τα απαραίτητα στοιχεία σε περίπτωση που ο συνδρομητής επιλέξει τη δημιουργία του αναγνωρισμένου πιστοποιητικού του από το ΧΑ. Η Υπηρεσία Εγγραφής μπορεί να αποτελεί **εσωτερική λειτουργία** του Π.Υ.Π. ή να εκτελείται από εξωτερικό συνεργάτη του, ο οποίος αναλαμβάνει συγκεκριμένα καθήκοντα σύμφωνα με τα οριζόμενα στην παρούσα πολιτική, δεσμευόμενος συμβατικά με τον Π.Υ.Π..

Η Υπηρεσία Εγγραφής συνεργάζεται με μία ή περισσότερες '*Τοπικές Υπηρεσίες Υποβολής*' (Τ.Υ.Υ. –βλ. παρακάτω) και με την '*Υπηρεσία Προμήθειας Φορέα Συνδρομητών*' (Υ.Π.Φ.Σ. –βλ. επόμενη παράγραφο) για να συγκεντρώσει και να ελέγξει τα προσωπικά στοιχεία, την φυσική παρουσία και τα αντιστοιχούντα 'δημόσια κλειδιά' που πρέπει να συμπεριληφθούν στα πιστοποιητικά SMART-SIGN (σύμφωνα με την παρούσα Πολιτική και τον σχετικό Κανονισμό Πιστοποίησης), πριν τα στείλει στον Εκδότη. Επίσης συνεργάζεται με την σχετική 'Υπηρεσία Διαχείρισης Ανάκλησης' για την ταυτοποίηση των συνδρομητών που αιτούνται ανάκληση ή ενεργοποίηση των πιστοποιητικών τους SMART-SIGN.

Η Υπηρεσία Εγγραφής δεν εκδίδει η ίδια πιστοποιητικά, και γι' αυτό **δεν** συμμετέχει στην 'αλυσίδα εγκυροποίησης' των πιστοποιητικών μεταξύ του Θ.Ε.Π. και του φυσικού προσώπου που πιστοποιείται. Μπορεί όμως, αν προβλέπεται από τον Κ.Π. του Π.Υ.Π., να αναφέρεται και αυτή μέσα στα πιστοποιητικά SMART-SIGN που αυτή ενέκρινε, σε ένα πρόσθετο υποπεδίο με πρόθεμα 'OU' στο πεδίο του Εκδότη ('Issuer') με την μορφή «OU= RA: *'όνομα υπηρεσίας εγγραφής'*».

2.1.3 Υπηρεσία Προετοιμασίας Φορέα Συνδρομητή (Υ.Π.Φ.Σ.)

Η 'Υπηρεσία Προετοιμασίας Φορέα Συνδρομητών' (Υ.Π.Φ.Σ. ή 'Subscriber Device Provision Service') προετοιμάζει και παρέχει στους εγκεκριμένους 'συνδρομητές' (βλ. παρακάτω) των πιστοποιητικών SMART-SIGN τους εξατομικευμένους φορείς 'ασφαλούς διάταξης δημιουργίας υπογραφής' ('α.δ.δ.υ.', π.χ. έξυπνες κάρτες) που απαιτούνται από την παρούσα πολιτική, στους οποίους δημιουργεί και εναποθηκεύει κατάλληλα και μοναδικά ζεύγη κρυπτογραφικών κλειδιών, γνωστοποιώντας παράλληλα στην Υπηρεσία Εγγραφής τα δημιουργηθέντα **δημόσια κλειδιά του υποκειμένου** που πρέπει να πιστοποιηθούν. Η Υ.Π.Φ.Σ. μπορεί να αποτελεί εσωτερικό τμήμα του Π.Υ.Π. ή της Υπηρεσίας Εγγραφής που εξυπηρετεί, ή να παρέχεται από εξωτερικό συνεργάτη τους που δεσμεύεται μαζί τους συμβατικά.

Η Υ.Π.Φ.Σ. 'εξατομικεύει' για τον εγκεκριμένο συνδρομητή τον προοριζόμενο για αυτόν φορέα, αναγράφοντας σ' αυτόν σχετικά στοιχεία του υποκειμένου, σύμφωνα με τον Κ.Π.. Παράλληλα μπορεί να φροντίζει και για την παροχή προς τους συνδρομητές των σχετικών 'αναγνωστών' (readers) του φορέα, εφόσον ο συνδρομητής το έχει ζητήσει. Οι φορείς 'α.δ.δ.υ.' πρέπει να είναι εγκεκριμένης τεχνολογίας από τον Π.Υ.Π. και μπορεί να είναι **ιδιοκτησίας** της ίδιας της Υ.Π.Φ.Σ., του Π.Υ.Π. ή της συνεργαζόμενης Υπηρεσίας Εγγραφής, ή ακόμη και της σχετικής Τ.Υ.Υ. και να παρέχεται στον συνδρομητή **είτε** κατά κυριότητα, **είτε** για χρονικά περιορισμένη χρήση του (ανάλογα με τις προβλέψεις του Κ.Π. του Π.Υ.Π.).

2.1.4 Τοπικές Υπηρεσίες Υποβολής (Τ.Υ.Υ.)

Οι Τοπικές Υπηρεσίες Υποβολής (Τ.Υ.Υ. ή 'Local RA Assistants'- LRAAs) προσφέρουν προς το συγκεκριμένο ή το ευρύτερο κοινό που απευθύνονται την μοναδική πρόσβαση στις υπηρεσίες εγγραφής και έκδοσης του Π.Υ.Π. για τα προσωπικά πιστοποιητικά SMART-SIGN.

Αν και ο Π.Υ.Π. μπορεί να διαθέτει δική του Τ.Υ.Υ. για την άμεση προσφορά των υπηρεσιών ψηφιακής πιστοποίησης προς το κοινό, οι Τ.Υ.Υ. που προβλέπονται από την παρούσα πολιτική είναι συνήθως **τρίτοι συνεργαζόμενοι φορείς** που συμβάλλονται απ' ευθείας με τον Π.Υ.Π. (ή με τις -σχετικά εξουσιοδοτημένες- συνεργαζόμενες μαζί του Υπηρεσίες Εγγραφής), ώστε να βοηθήσουν **συγκεκριμένα ή απροσδιόριστα φυσικά πρόσωπα** στην εγγραφή τους για απόκτηση προσωπικών πιστοποιητικών SMART-SIGN, **είτε** διότι θέλουν οι ίδιες (οι Τ.Υ.Υ.) να χρησιμοποιήσουν τα πιστοποιητικά αυτά σε δικές τους 'κλειστές' τηλεματικές εφαρμογές (ως αποδέκτες/βασιζόμενα μέρη), **είτε** για εμπορικούς λόγους.

Οι Τ.Υ.Υ. μετά από εξακρίβωση της φυσικής ταυτότητας, προμηθεύουν τους υποψήφιους συνδρομητές με το απαραίτητο έντυπο υλικό (αιτήσεις, συμβάσεις, τεκμηρίωση κ.λ.π.) που παρέχει ο Π.Υ.Π., συνυπογράφουν (ως αντιπρόσωποι του Π.Υ.Π.) τις αιτήσεις-συμβάσεις των συνδρομητών μετά από πρόχειρο έλεγχο των δικαιολογητικών και τις στέλνουν στην αρμόδια Υπηρεσία Εγγραφής για έγκριση. Ενίοτε, και σε συνεργασία με την σχετική Υ.Π.Φ.Σ. που θα τους εξατομικεύσει, μπορεί να παρέχουν προς τους υποψήφιους συνδρομητές **κατάλληλους φορείς 'α.δ.δ.υ.' ιδιοκτησίας τους**, είτε μεταβιβάζοντάς τους των, είτε παρέχοντάς τους την κατοχή και το δικαίωμα χρήσης.

Οι Τ.Υ.Υ. βάσει της σύμβασής τους με τον Π.Υ.Π., **χρεώνουν και εισπράττουν** από τους συνδρομητές **τα τέλη εγγραφής και έκδοσης** των πιστοποιητικών SMART-SIGN, ακολουθώντας ανεξάρτητη τιμολογιακή πολιτική.

2.1.5 Συνδρομητής (υποκείμενο πιστοποίησης)

'Συνδρομητές' (subscribers) ή 'υποκείμενα' (subjects) πιστοποίησης κατά την παρούσα πολιτική θεωρούνται τα **φυσικά πρόσωπα** που είναι αποκλειστικοί κάτοχοι ψηφιακών κρυπτογραφικών κλειδιών κατάλληλα για την δημιουργία 'προηγμένων ηλεκτρονικών υπογραφών' τα οποία βρίσκονται εναποθηκευμένα σε φορέα 'ασφαλούς διάταξης δημιουργίας υπογραφής' (α.δ.δ.υ.), και των οποίων τα 'δεδομένα επαλήθευσης υπογραφής' (δημόσια κλειδιά – public keys) **έχουν ήδη πιστοποιηθεί με προσωπικά πιστοποιητικά τύπου**

SMART-SIGN από κάποιον συμμορφούμενο με την παρούσα πολιτική Πάροχο Υπηρεσιών Πιστοποίησης (στον οποίο και είναι 'συνδρομητές').

Για να γίνει κάποιος 'συνδρομητής' και 'κάτοχος προσωπικών πιστοποιητικών τύπου SMART-SIGN', πρέπει να απευθυνθεί σε κάποια 'Τοπική Υπηρεσία Υποβολής' (Τ.Υ.Υ.) του δικτύου ενός συμμορφούμενου με την παρούσα πολιτική Π.Υ.Π., να συμπληρώσει αίτηση απευθυνόμενη προς την σχετική Υπηρεσία Εγγραφής συνοδευόμενη από τα προβλεπόμενα από την παρούσα πολιτική **αποδεικτικά της ταυτότητάς του**, καθώς και να υπογράψει τη σχετική '**αίτηση-σύμβαση συνδρομητή**' ή άλλως '**συνδρομητική σύμβαση**'. Η αίτησή του, μετά από έλεγχο της πληρότητάς της και της καταλληλότητας των προσκομιζόμενων δικαιολογητικών, **πρέπει να εγκριθεί** από την σχετική Υπηρεσία Εγγραφής, η οποία θα δώσει και την τελική εντολή στον Εκδότη για την έκδοση των σχετικών πιστοποιητικών. Έως την παραλαβή του σχετικού φορέα και των πιστοποιητικών από τον αιτούντα, αυτός θεωρείται ως 'υποψήφιος συνδρομητής'.

Ο συνδρομητής μπορεί παράλληλα να είναι και 'Αποδέκτης' (ή 'χρήστης' ή 'τρίτο βασιζόμενο μέρος' –βλ. αμέσως παρακάτω) πιστοποιητικών άλλων συνδρομητών – υποκειμένων πιστοποιητικών.

2.1.6 Αποδέκτης (ή 'χρήστης' ή 'τρίτο βασιζόμενο μέρος')

'Αποδέκτης' **ή** 'χρήστης' (user) **ή** 'τρίτο βασιζόμενο μέρος' (relying party) των πιστοποιητικών SMART-SIGN είναι τα φυσικά ή νομικά πρόσωπα που αυτόγνωμα, ή με την χρήση αυτόματων εφαρμογών τους, **αφού ελέγξουν και επαληθεύσουν την εγκυρότητα ενός πιστοποιητικού SMART-SIGN** σύμφωνα με την παρούσα πολιτική (βλ. υποκεφάλαιο 6.1) και τους ειδικότερους όρους του 'Κανονισμού Πιστοποίησης' (C.P.S.) του Π.Υ.Π. που εξέδωσε το συγκεκριμένο πιστοποιητικό, **αποφασίζουν οι ίδιοι** αν το πιστοποιητικό τους προσφέρει το επιθυμητό –γι' αυτούς- επίπεδο ασφάλειας ώστε να βασισθούν ή όχι στα περιεχόμενα του και να προβούν σε μία συγκεκριμένη πράξη, ενέργεια ή παράλειψη, ή να αποκτήσουν δικαιολογημένη πεποίθηση για ένα γεγονός.

'Χρήστης Πιστοποιητικού' (αποδέκτης) μπορεί κάλλιστα να είναι ένας συνδρομητής ή ακόμη και ένα μέλος του ίδιου του δικτύου του Π.Υ.Π., που ακολουθώντας την παραπάνω διαδικασία, βασίζεται ή όχι στα περιεχόμενα ενός πιστοποιητικού τύπου SMART-SIGN.

2.2 ΕΦΑΡΜΟΓΕΣ ΚΑΙ ΠΕΡΙΟΡΙΣΜΟΙ ΧΡΗΣΗΣ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

2.2.1 Εφαρμογές των πιστοποιητικών 'SMART-SIGN'

Αν και συχνά τα πιστοποιητικά SMART-SIGN™ εκδίδονται με σκοπό να χρησιμοποιηθούν σε τηλεματικές εφαρμογές που σχετίζονται με την δραστηριότητα μιας Τ.Υ.Υ., οι τεχνικές προδιαγραφές των πιστοποιητικών αυτών και οι παρούσες πολιτικές τους, **επιτρέπουν** την χρήση τους και σε άλλες συμβατές εφαρμογές (που απαιτούν 'πιστοποιητικά ταυτοποίησης' ή/και 'αναγνωρισμένα πιστοποιητικά' για την δημιουργία ηλεκτρονικής υπογραφής) **εφόσον** ο υπεύθυνος διαχειριστής των εφαρμογών αυτών **αποδεχτεί και ορίσει ως κατάλληλες** τις παρούσες πολιτικές προσωπικών πιστοποιητικών 'SMART-SIGN™' στις λειτουργικές απαιτήσεις και στις απαιτήσεις ασφάλειας της εφαρμογής του.

Σε κάθε όμως περίπτωση, τα πιστοποιητικά τύπου SMART-SIGN, **με την χρήση κατάλληλου και συμβατού λογισμικού δημιουργίας και επαλήθευσης υπογραφών**, προσφέρονται για να χρησιμοποιηθούν από τους συνδρομητές-κατόχους τους, στις εξής εφαρμογές:

Το '**αναγνωρισμένο προσωπικό πιστοποιητικό**' του 'πακέτου' '**SMART-SIGN™**' , σε συνδυασμό με την υποχρεωτική χρήση του φορέα 'ασφαλούς διατάξεως δημιουργίας υπογραφής' που παρέχει ο Π.Υ.Π., είναι ικανό για να υποστηρίξει την υπογραφή 'ηλεκτρονικών εγγράφων' από τον κάτοχο του πιστοποιούμενου δημοσίου κλειδιού, τηρώντας **όλες τις προϋποθέσεις** της νομοθεσίας , ελληνικής και ευρωπαϊκής, για δημιουργία ηλεκτρονικής υπογραφής ισότιμης δικονομικά με την ιδιόχειρη.

Συγκεκριμένα, το '**αναγνωρισμένο προσωπικό πιστοποιητικό**' του 'πακέτου' '**SMART-SIGN™**' – **Κλάσης 1ης,** προορίζεται για την ηλεκτρονική υπογραφή ψηφιακών αρχείων και δεδομένων οποιασδήποτε μορφής (-δες όμως τις **εξαιρέσεις** της επόμενης παραγράφου 2.2.2) δημιουργώντας αρχεία που περιλαμβάνουν: α) το ίδιο το υπογεγραμμένο αρχείο, β) την ηλεκτρονική υπογραφή του υποκειμένου σ' αυτό, και (συνημμένο) γ) το ίδιο το 'αναγνωρισμένο' πιστοποιητικό του υποκειμένου, το οποίο, έχοντας την ένδειξη 'Non-

Repudiation' ('μη αποκήρυξη') στο πεδίο 'Key Usage' ('χρήση κλειδιού'), επιβεβαιώνει σε κάθε τρίτο-αποδέκτη του εγγράφου:

- Την **ταυτότητα** του υπογράφοντος *(ποιος είναι)*
- την **γνησιότητα** του υπογράφοντος *(ότι πράγματι είναι αυτός)*
- την **μη αλλοίωση** του υπογεγραμμένου εγγράφου *(από την στιγμή της υπογραφής)*
- την βούληση του υπογράφοντος να **δεσμευτεί νομικά** από την υπογραφή του στο έγγραφο *(όπως ακριβώς και με την εναπόθεση της ιδιόχειρης υπογραφής του σε χάρτινα έγγραφα)*

Σημείωση: Τα υπογεγραμμένα με αυτό το πιστοποιητικό έγγραφα, μπορούν να σταλούν σε τρίτους με την χρήση του ηλεκτρονικού ταχυδρομείου (e-mail) ***μόνο ως 'συνημμένα έγγραφα'*** *(Attachments), αφού οι σχετικές δυνατότητες 'δημιουργίας υπογραφής' στα ηλεκτρονικά μηνύματα που προσφέρουν τα πιο δημοφιλή προγράμματα διαχείρισης ηλεκτρονικού ταχυδρομείου (όπως π.χ. το 'MS Outlook Express')* ***δεν υποστηρίζουν*** *–τουλάχιστον μέχρι την στιγμή έκδοσης της παρούσας πολιτικής-* ***τις τεχνικές προδιαγραφές*** *(συγκεκριμένα την αποκλειστική χρήση του πιστοποιούμενου κλειδιού για 'μη αποκήρυξη' ('Non-Repudiation'))* ***των 'αναγνωρισμένων πιστοποιητικών'*** *που προβλέπει η ευρωπαϊκή νομοθεσία.*}

2.2.2 Περιορισμοί στην χρήση των πιστοποιητικών 'SMART-SIGN'

Τα αναγνωρισμένα πιστοποιητικά SMART-SIGN™-Κλάσης 2ης ΔΕΝ ΕΠΙΤΡΕΠΕΤΑΙ να χρησιμοποιηθούν για την 'υπογραφή' αρχείων που αποτελούν άμεσα ή έμμεσα **εκτελέσιμο κώδικα για Η/Υ (**'software', όπως π.χ. αρχεία με καταλήξεις .exe ή .com) **ή προσθήκη** σε υπάρχοντα εκτελέσιμο κώδικα που επιφέρουν διαφορετικές δυνατότητες σε κάποιον Η/Υ (π.χ. με καταλήξεις .dll), ιδίως όταν αυτά παρουσιάζονται ως 'δημιούργημα' του υποκειμένου και η υπογραφή τους από αυτόν γίνεται για να παράσχει εγγύηση προς τρίτους αποδέκτες τους ότι είναι 'ασφαλή' (κοινώς 'CODE SIGNING').

2.2.3 Όρια στην αξία των συναλλαγών με χρήση των πιστοποιητικών 'SMART-SIGN –Κλάσης 2ης'

Τα πιστοποιητικά SMART-SIGN™-Κλάσης 2ης, βάση της παρούσας πολιτικής για την συγκεκριμένη κλάση**,** προορίζονται αποκλειστικά σε υπογραφή ή/και κρυπτογράφηση εγγράφων που χαρακτηρίζονται '**πληροφοριακά'** (π.χ. αναφορές, εκθέσεις, ανακοινώσεις, δηλώσεις, δημοσιεύσεις κ.λ.π.) ή προορίζονται για την ταυτοποίηση και την ελεγχόμενη πρόσβαση του υποκειμένου τους σε εφαρμογές που δεν σχετίζονται με την καταβολή άμεσης ή έμμεσης αμοιβής ή οποιουδήποτε αντιτίμου για την παροχή αγαθού ή υπηρεσίας (π.χ. ελεγχόμενη πρόσβαση σε βιβλιοθήκες, δίκτυα υπολογιστών, δωρεάν υπηρεσίες κ.λ.π.).

3 ΥΠΟΧΡΕΩΣΕΙΣ, ΕΓΓΥΗΣΕΙΣ ΚΑΙ ΟΡΙΑ ΕΥΘΥΝΗΣ

3.1 ΥΠΟΧΡΕΩΣΕΙΣ ΤΩΝ ΕΜΠΛΕΚΟΜΕΝΩΝ ΜΕΡΩΝ

3.1.1 Υποχρεώσεις του Παρόχου Υπηρεσιών Πιστοποίησης

Ο Π.Υ.Π. που εκδίδει προσωπικά πιστοποιητικά τύπου SMART-SIGN™, όπως και οι συμβεβλημένοι μ' αυτόν συνεργάτες του στην παροχή των υπηρεσιών πιστοποίησης (στο βαθμό που αναλογεί στον καθένα τους σύμφωνα με την παρούσα Πολιτική και τον σχετικό Κανονισμό Πιστοποίησης του Π.Υ.Π.), έχουν υποχρέωση:

1) να έχουν λάβει **γραπτή έγκριση** της συμμόρφωσης του Κανονισμού Πιστοποίησής τους από τον 'Υπεύθυνο Έκδοσης και Διαχείρισης' των Πολιτικών των 'προσωπικών πιστοποιητικών SMART-SIGN™' που ορίζεται στην παράγραφο 10.1, σύμφωνα με την διαδικασία της παραγράφου 10.3.2 '*Έγκριση Κανονισμών Πιστοποίησης'* **πριν** εκδώσουν οποιοδήποτε πιστοποιητικό που να αναφέρεται –άμεσα ή έμμεσα- στις παρούσες πολιτικές,

2) να διαφυλάττουν την **αξιοπιστία και την ασφάλεια της υποδομής** τους, συμμορφούμενοι με τις απαιτήσεις αξιοπιστίας και ασφάλειας που απαιτούνται από την παρούσα πολιτική (Κεφάλαιο 7),

3) να ελέγχουν και να διατηρούν για το χρονικό διάστημα που ορίζεται στην παρούσα πολιτική (παρ. 6.2.3) **τα αποδεικτικά ταυτοποίησης των συνδρομητών τους,** τα ίδια τα ηλεκτρονικά πιστοποιητικά τους και τις καταχωρήσεις σχετικά με τις αλλαγές της κατάστασης των πιστοποιητικών τους, για την περίπτωση επίλυσης πιθανών διαφορών,

4) να προβαίνουν σε **άμεσες διαδικασίες αναστολής ή ανάκλησης** των πιστοποιητικών SMART-SIGNTM σύμφωνα με τα οριζόμενα στην παρούσα πολιτική και στις εξειδικεύσεις του Κανονισμού Πιστοποίησης, ενημερώνοντας σχετικά τον κάτοχο του πιστοποιητικού,

5) να τηρούν στο σύνολό τους **τις διαδικασίες και τις προϋποθέσεις των διαδικασιών** που ορίζονται στην παρούσα πολιτική, όπως αυτές εξειδικεύονται στον Κανονισμό Πιστοποίησης του συμμορφούμενου Π.Υ.Π.,

6) να ενημερώνουν τους συνδρομητές και τα τρίτα βασιζόμενα μέρη **για τους όρους και τις προϋποθέσεις των υπηρεσιών τους**, παρέχοντάς τους **δωρεάν** μέσα από ευρέως προσβάσιμη ηλεκτρονική ιστοσελίδα αλλά **και** σε έντυπη μορφή σε όποιον τους το ζητήσει: α) τους **Κανονισμούς Πιστοποίησης**, β) τις **παρούσες** -τουλάχιστον- **Πολιτικές Πιστοποιητικών**, γ) την '**Συνδρομητική Σύμβαση**' και την '**Σύμβαση Αποδέκτη**', και δ) την '**Συνοπτική Διακήρυξη των Υπηρεσιών τους**' (**P**KI **D**isclosure **S**tatement –P.D.S) που θα περιλαμβάνει συνοπτικά τους βασικότερους όρους και την περιγραφή των προσφερόμενων υπηρεσιών του Π.Υ.Π., καθώς και όλες τις προηγούμενες εκδόσεις τους με έγκαιρες προειδοποιήσεις για τις τυχόν επερχόμενες τροποποιήσεις τους.

[Σημείωση: Πρόσθετο ενημερωτικό υλικό στην ιστοσελίδα τους, όπως π.χ. παραδείγματα για την κατανόηση και την χρήση των ηλεκτρονικών υπογραφών, ανάλυση στα τεχνικά χαρακτηριστικά των προϊόντων τους, και παραβολή της ισχύουσας νομοθεσίας, ***δεν επιβάλλεται*** *αλλά* ***συνιστάται*** *από την παρούσα πολιτική].*

3.1.2 Υποχρεώσεις του συνδρομητή – υποκείμενου πιστοποίησης

Τα υποκείμενα της πιστοποίησης (συνδρομητές) των πιστοποιητικών SMART-SIGN™ οφείλουν:

1) να παράσχουν **ακριβή στοιχεία ταυτοποίησής** τους κατά την αίτησή τους,

2) να ελέγξουν την **ορθότητά** τους στο πιστοποιητικό πριν ζητήσουν την 'αρχική ενεργοποίησή' του σύμφωνα με την παράγραφο 5.1.4,

3) να χρησιμοποιούν **αποκλειστικά τον εξατομικευμένο φορέα** που τους έχει δοθεί από την Υ.Π.Φ.Σ. του Π.Υ.Π. για την ενεργοποίηση του ιδιωτικού τους κλειδιού,

4) να ζητούν **την προσωρινή (παύση/αναστολή) ή την οριστική ανάκληση των πιστοποιητικών τους** όταν υποψιαστούν ή αντιληφθούν την πιθανή έκθεση των ιδιωτικών τους κλειδιών σε τρίτους, ή όταν προκύψει αιτία από αυτές που αναφέρονται στον 'Κανονισμό Πιστοποιήσεων' και στην 'Σύμβαση Συνδρομητή' που έχουν υπογράψει,

5) να **μην** χρησιμοποιούν τα πιστοποιητικά τους σε εφαρμογές ή συναλλαγές που έχει **ρητά απαγορεύσει** η παρούσα πολιτική ή ο Εκδότης των πιστοποιητικών μέσα από την 'Συνδρομητική Σύμβαση' ή/και τον 'Κανονισμό Πιστοποίησής' του,

6) να **μην** χρησιμοποιούν τα πιστοποιητικά ή τα σχετικά ιδιωτικά τους κλειδιά **μετά την λήξη τους**,

7) να προβαίνουν σε κάθε απαραίτητο μέτρο για να διαφυλάξουν την **ακεραιότητα, την μυστικότητα και την νόμιμη χρήση** του ιδιωτικού τους κλειδιού, του φορέα και του κωδικού ενεργοποίησής του (PIN).

3.1.3 Υποχρεώσεις τρίτων αποδεκτών –χρηστών του πιστοποιητικού

Κάθε τρίτος που γίνεται αποδέκτης ενός προσωπικού πιστοποιητικού SMART-SIGN, **πριν αποφασίσει να βασιστεί σ' αυτό για οποιαδήποτε λόγο**, οφείλει:

1) να είναι ενήμερος για τον **τρόπο λειτουργίας και χρήσης** των ηλεκτρονικών υπογραφών και των ηλεκτρονικών πιστοποιητικών και να έχει διαβάσει και κατανοήσει τους όρους της παρούσας Πολιτικής, του Κανονισμού Πιστοποίησης και της σχετικής 'Σύμβασης Αποδέκτη' του Π.Υ.Π. που έχει εκδώσει το σχετικό πιστοποιητικό SMART-SIGN,

2) να ελέγξει την **εγκυρότητα** και τη **μη πλαστότητα** του πιστοποιητικού, σύμφωνα με τα οριζόμενα στο υποκεφάλαιο 6.1 *'Έλεγχος Εγκυρότητας των Πιστοποιητικών'* αυτής της πολιτικής και τους τυχόν σχετικούς όρους του Π.Υ.Π., ανατρέχοντας στις οριζόμενες από Π.Υ.Π. σχετικές 'Λίστες Ανασταλέντων και Ανακληθέντων Πιστοποιητικών' (CRLs),

3) να λάβει υπ' όψιν του σε κάθε περίπτωση τα «**ανώτατα όρια ευθύνης του Π.Υ.Π.**» που αναφέρονται στην παρούσα πολιτική (βλ. παράγραφο 3.2.3) και τους **περιορισμούς στην εγγύηση** που δημοσιεύει ο Π.Υ.Π. στον 'Κανονισμό Πιστοποίησής' του ή/και στην 'Σύμβαση Αποδέκτη'.

3.2 ΕΓΓΥΗΣΕΙΣ, ΑΠΟΠΟΙΗΣΗ ΕΥΘΥΝΗΣ ΚΑΙ ΑΝΩΤΑΤΟ ΟΡΙΟ ΕΥΘΥΝΗΣ ΤΟΥ Π.Υ.Π.

3.2.1 Εγγυήσεις του Παρόχου Υπηρεσιών Πιστοποίησης

Ο Π.Υ.Π. που εξέδωσε ένα πιστοποιητικό SMART-SIGN™, **οφείλει να εγγυάται** προς κάθε τρίτο που βασίζεται **εύλογα** (δηλ. σύμφωνα με την προηγούμενη παράγραφο) στο πιστοποιητικό αυτό (είτε 'αναγνωρισμένο' είτε 'ταυτοποίησης'), τα εξής:

- την **ακρίβεια**, κατά τη στιγμή της 'αρχικής ενεργοποίησής' του (βλ. παρ. 5.1.4), **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 Κανονισμό Πιστοποίησής του και στην παρούσα Πολιτική,
- ότι **ο υπογράφων**, η ταυτότητα του οποίου βεβαιώνεται από τον Π.Υ.Π. στο πιστοποιητικό SMART-SIGN™, κατά τη στιγμή της αρχικής ενεργοποίησής του, **κατείχε τα 'δεδομένα δημιουργίας υπογραφής'** (ιδιωτικό κλειδί), που αντιστοιχούσαν 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 ο ίδιος στους συνδρομητές/πιστοποιούμενούς της, **μπορούν να χρησιμοποιηθούν συμπληρωματικά**.
- ότι καταβάλλει κάθε εύλογη προσπάθεια ώστε να δημοσιεύονται **οι ανακλήσεις των πιστοποιητικών**, σύμφωνα με τους όρους και την διαδικασία που περιγράφονται στην παρούσα Πολιτική και που εξειδικεύονται στον Κανονισμό Πιστοποιήσεών του.

3.2.2 Αποποίηση ευθύνης -εξαιρέσεις

Ο Π.Υ.Π. που εκδίδει πιστοποιητικά SMART-SIGN™, **μπορεί** να αποποιηθεί τις παραπάνω ευθύνες του, για τις παρακάτω περιπτώσεις:

- εάν για την δυσλειτουργία ή την αστοχία που προκάλεσε την ζημιά στον συνδρομητή του ή σε οποιονδήποτε τρίτο, ο Π.Υ.Π. δεν βαρύνεται με πταίσμα **ή** εάν οι πράξεις του ήταν σύμφωνες με τα οριζόμενα στον Κανονισμό Πιστοποίησής του για τα Αναγνωρισμένα πιστοποιητικά παράγραφος 2.2.2 και την παρούσα πολιτική,

- εάν ο ίδιος ο ζημιωθείς ή άλλος (–εκτός του δικτύου παροχής των υπηρεσιών του), προκάλεσε την ζημιά **παραβιάζοντας** τους όρους και τις προϋποθέσεις του Κανονισμού Πιστοποίησης του Π.Υ.Π. και της παρούσας Πολιτικής. **ή** αν ο ίδιος **προξένησε** την επίμαχη ζημιά με οποιαδήποτε λανθασμένη, απρόσφορη ή παράνομη πράξη του.

- εάν η μη τήρηση των όρων του Κανονισμού του και της παρούσας Πολιτικής από πλευράς του Π.Υ.Π. οφείλεται σε λόγους ανυπέρβλητης ‘ανωτέρας βίας’ (π.χ. σεισμοί, black out, απεργίες κ.λ.π.).

Επίσης ο Π.Υ.Π. που εκδίδει πιστοποιητικά SMART-SIGN™, εκτός από τις περιπτώσεις που διαφορετικά ορίζεται σ’ αυτή την Πολιτική, **δεν εγγυάται** και ούτε ευθύνεται για την προσφορότητα, την ποιότητα, την έλλειψη λάθους ή την καταλληλότητα για συγκεκριμένο σκοπό των πιστοποιητικών SMART-SIGN™.

Τέλος ο Π.Υ.Π. **μπορεί να εξαιρεί** από την ευθύνη του, που πηγάζει από την έκδοση των πιστοποιητικών SMART-SIGN, τα είδη έμμεσης ή αποθετικής ζημιάς, όπως π.χ. διαφυγόντα κέρδη, ποινικές ή πειθαρχικές ποινές ή πρόστιμα κ.λ.π.

4 ΤΑΥΤΟΠΟΙΗΣΗ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ

4.1 ΠΟΛΙΤΙΚΗ ΟΝΟΜΑΣΙΑΣ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ

4.1.1 Προσωπικά στοιχεία του υποκειμένου που εμφανίζονται στο πιστοποιητικό

Τα αναγνωρισμένα πιστοποιητικά SMART-SIGN τα οποία εκδίδονται, περιέχουν τα εξής στοιχεία του υποκειμένου:

- Όνομα
- Επώνυμο
- Πατρώνυμο (3 ψηφία)
- Εθνικότητα (Κωδικός χώρας)
- Κοινό Όνομα (συνδυασμός ονόματος, πατρώνυμου και επιθέτου)
- μία Ηλεκτρονική Διεύθυνση του υποκειμένου

καθώς επίσης και την **ένδειξη "QC Statement id-etsi-qcs-QcSSCD** [*Σημείωση: Η απόδοση ιδιοτήτων στα υποκείμενα μπορεί να γίνει με ειδικά, πρόσθετα '**πιστοποιητικά ιδιότητας'** (attribute certificates) τα οποία δεν αποτελούν αντικείμενο της παρούσας πολιτικής.]*

4.1.2 Απόδοση του ονόματος με λατινικούς χαρακτήρες (ΕΛΟΤ 743)

Για λόγους συμβατότητας των πιστοποιητικών SMART-SIGN™ με διεθνείς εφαρμογές, **όλα τα στοιχεία** των υποκειμένων αναγράφονται στα σχετικά πεδία του πιστοποιητικού **με λατινικούς χαρακτήρες,** σύμφωνα με το πρότυπο 'ΕΛΟΤ 743'.

Η σωστή μετατροπή των στοιχείων του υποκειμένου από την ελληνική στην λατινική γραφή θα διασφαλίζεται από την τυχόν προσκόμιση κατάλληλων εγγράφων από το ίδιο το υποκείμενο (π.χ. διαβατήριο ή νέα αστυνομική ταυτότητα), αλλιώς θα εφαρμόζεται το παραπάνω πρότυπο από τις υπηρεσίες του Π.Υ.Π..

4.1.3 Επίλυση διαφορών στην ονομασία του υποκειμένου

Ο Π.Υ.Π. πρέπει να προβλέπει στον Κανονισμό Πιστοποίησής του διαδικασία ή τρόπο επίλυσης διαφορών σχετικά με την ονοματοδοσία των υποκειμένων. Αυτό μπορεί να εντάσσεται στα πλαίσια των αρμοδιοτήτων της γενικότερης υπηρεσίας 'Επίλυσης Διαφορών και Παραπόνων' που πρέπει να τηρεί ο Π.Υ.Π. σύμφωνα και με την παρ. 9.1.4 αυτής της Πολιτικής.

4.2 ΕΞΑΚΡΙΒΩΣΗ ΤΗΣ ΤΑΥΤΟΤΗΤΑΣ ΤΟΥ ΥΠΟΚΕΙΜΕΝΟΥ

4.2.1 Στην αρχική εγγραφή

Τόσο η ταυτοποίηση όσο και η γνησιότητα του υποκειμένου που αιτείται την έκδοση προσωπικών πιστοποιητικών SMART-SIGN™, επιτυγχάνεται με την προσκόμιση **επικυρωμένου αντιγράφου** ενός δημόσιου εγγράφου ταυτοποίησης του υποκειμένου, όσο και με την **υποχρεωτική υπογραφή** της σχετικής αίτησής του για την έκδοση των πιστοποιητικών **ενώπιον αρμόδιας δημόσιας αρχής** που θα βεβαιώνει την γνησιότητα της υπογραφής του μετά την εξακρίβωση της φυσικής του ταυτότητας.

Εναλλακτικά, αντί για βεβαίωση της υπογραφής του υποκειμένου από δημόσια αρχή, η εξακρίβωση της ταυτότητας του υποκειμένου **μπορεί να γίνεται και από αρμόδιο υπάλληλο της Τ.Υ.Υ.** στον οποίο θα υποδειχθεί το πρωτότυπο του δημοσίου εγγράφου ταυτοποίησης του υποκειμένου και ο οποίος θα υπογράψει σχετική 'βεβαίωση', μόνο όμως εάν αυτήν την διαδικασία την προβλέπει ρητά ο Κανονισμός Πιστοποίησης του Π.Υ.Π., και εφόσον η Τ.Υ.Υ. έχει ορίσει τους αρμόδιους υπαλλήλους της και έχει προβεί σε ανάληψη της σχετικής ευθύνης απέναντι στον Π.Υ.Π. (ή στην συνεργαζόμενη Υπηρεσία Εγγραφής) στην μεταξύ τους γραπτή σύμβαση.

Το ‘δημόσιο έγγραφο ταυτοποίησης’ που πρέπει να προσκομίσει ο υποψήφιος συνδρομητής, σε επικυρωμένο αντίγραφο μαζί με την αίτησή του, πρέπει να είναι ένα από τα εξής:

- Αστυνομική Ταυτότητα.
- Διαβατήριο.
- Άλλο ισότιμο με τα παραπάνω έγγραφο, που να αποδεικνύει επαρκώς την ταυτότητά του, σύμφωνα με τους ελληνικούς νόμους.

Τα παραπάνω έντυπα, διασταυρώνονται, επιβεβαιώνονται και εγκρίνονται (στην περίπτωση πληρότητας και ορθότητάς τους) από την σχετική Υπηρεσία Εγγραφής του Π.Υ.Π..

4.2.2 Στην τακτική ανανέωση των πιστοποιητικών (πριν λήξουν ή ανακληθούν)

Στην περίπτωση ‘τακτικής ανανέωσης’, στην οποία ο συνδρομητής **έχει ήδη ισχυρό προσωπικό πιστοποιητικό** SMART-SIGN το οποίο δεν έχει ακόμη λήξη ή ανακληθεί, **δεν απαιτείται επανέλεγχος** των στοιχείων της ταυτότητας και της γνησιότητας του συνδρομητή με την παραπάνω διαδικασία.

Τα παραπάνω μπορούν να αντικατασταθούν με την ηλεκτρονική υπογραφή του υποκειμένου (με την χρήση του ‘**αναγνωρισμένου’** πιστοποιητικού του), σε ‘ηλεκτρονική αίτηση ανανέωσης’ που του παρέχει ο Π.Υ.Π. και όπου το υποκείμενο **επιβεβαιώνει** (ή, αν πρέπει, **τροποποιεί**) τα προσωπικά του στοιχεία.

4.2.3 Στην ανανέωση πιστοποιητικών μετά από λήξη ή ανάκλησή τους

Μετά από την λήξη ή την ανάκληση των πιστοποιητικών του, ο ‘υποψήφιος’ πλέον συνδρομητής πρέπει να επαναλάβει την διαδικασία της παρ. 4.2.1, (όπως δηλαδή στην αρχική εγγραφή του), με την διαφορά ότι δεν απαιτείται προσκόμιση καινούργιου επικυρωμένου αντιγράφου ‘δημόσιων εγγράφων ταυτοποίησης, εφόσον το αρχικώς προσκομισμένο έγγραφο δεν έχει λήξει και εφόσον στην αίτησή του ο συνδρομητής αναγράφει τον Π.Κ.Α. που του είχε αποδοθεί κατά την προηγούμενη πιστοποίησή του.

4.2.4 Στην αίτηση αναστολής ή ανάκλησης

Για την εξακρίβωση της ταυτότητας του συνδρομητή κατά την τηλεφωνική ή μέσω διαδικτύου αίτησή του για ‘αναστολή’ (προσωρινή ανάκληση ή παύση) ή ‘οριστική ανάκληση’ των πιστοποιητικών του, μπορεί να χρησιμοποιηθεί ‘Μυστική Φράση’ που θα υποδείξει ο ίδιος ο συνδρομητής προς τον Π.Υ.Π. κατά την αρχική αίτησή του ή μετέπειτα.

Ειδικά για την αίτηση αναστολής (προσωρινή ανάκληση), αυτή -αφού δεν επιφέρει την οριστική ανάκληση των πιστοποιητικών-, μπορεί να γίνει τηλεφωνικά με απλή διασταύρωση κάποιων προσωπικών στοιχείων του αιτούντα με τα στοιχεία του αρχείου του Π.Υ.Π., δηλαδή και χωρίς την χρήση ‘Μυστικής Φράσης’ του υποκειμένου.

Σε κάθε περίπτωση κρίνεται **ικανοποιητική** η ταυτοποίηση του υποκειμένου που ζητά την αναστολή ή ακόμη και την οριστική ανάκληση των πιστοποιητικών εφόσον η αίτηση γίνεται **γραπτώς** (με την ηλεκτρονική ή ιδιόχειρη υπογραφή του αιτούντα) ή αυτοπροσώπως με παράσταση του αιτούντα ενώπιον κάποιας από τις υπηρεσίες του δικτύου του Π.Υ.Π. και την επίδειξη κάποιου εγγράφου ταυτοποίησής του.

4.2.5 Στην αίτηση επαν-ενεργοποίησης (μετά από παύση)

Στην αίτηση επαν-ενεργοποίησης ανασταλθέντων πιστοποιητικών που γίνεται τηλεφωνικά ή μέσω διαδικτύου, απαιτείται η χρήση της ‘Μυστικής Φράσης’, που καθορίστηκε από τον συνδρομητή είτε κατά την αρχική αίτηση, είτε κατά την αίτηση προσωρινής ανάκλησης (αναστολής) του συγκεκριμένου πιστοποιητικού.

Στην περίπτωση που έχει ξεχαστεί η ‘Μυστική Φράση’ από τον συνδρομητή, η αρμόδια υπηρεσία του Π.Υ.Π. μπορεί τηλεφωνικώς, μετά από απλή διασταύρωση κάποιων προσωπικών στοιχείων του αιτούντα με τα στοιχεία του αρχείου της, να του την υπενθυμίσει.

4.3 ΑΠΟΔΕΙΞΗ ΚΑΤΟΧΗΣ ΤΟΥ ΙΔΙΩΤΙΚΟΥ ΚΛΕΙΔΙΟΥ ΑΠΟ ΤΟ ΥΠΟΚΕΙΜΕΝΟ

4.3.1 Δημιουργία των κλειδιών σε εξατομικευμένο φορέα ‘α.δ.δ.υ.’

Τα ζεύγη κρυπτογραφικών κλειδιών των οποίων τα δημόσια κλειδιά θα πιστοποιηθούν σε πιστοποιητικά τύπου SMART-SIGN για ένα υποκείμενο, δημιουργούνται και αποθηκεύονται υποχρεωτικά μέσα σε φορέα 'ασφαλούς διάταξης δημιουργίας υπογραφής' που προετοιμάζει η Υ.Π.Φ.Σ. του Π.Υ.Π., ο οποίος εξατομικεύεται για το υποκείμενο αυτό. Η εξατομίκευση αυτή γίνεται με την αναγραφή του ονόματος ή/και του Κ.Π.Α. του υποκειμένου πάνω στον φορέα και εξασφαλίζει ότι τα συγκεκριμένα κλειδιά που περιέχει ο φορέας θα πιστοποιηθούν στο συγκεκριμένο υποκείμενο-συνδρομητή για το οποίο αυτός έχει εξατομικευτεί.

Στον ίδιο φορέα, πριν τον στείλει στον συνδρομητή, η Υ.Π.Φ.Σ. θα καταχωρήσει και τα σχετικά πιστοποιητικά SMART-SIGN, μόλις αυτά εκδοθούν από τον Εκδότη.

Επιπλέον, αναφορικά με τα αναγνωρισμένα πιστοποιητικά της παρούσας πολιτικής, ο συνδρομητής έχει την δυνατότητα να παράξει τα ζεύγη των κρυπτογραφικών κλειδιών απευθείας στον φορέα που του έχει δοθεί κατά την διαδικασία εγγραφής ή στην κρυπτογραφική μονάδα του ΠΥΠ (cloud HSM). Τα πιστοποιητικά που αποθηκεύονται στην κρυπτογραφική μονάδα του ΠΥΠ βρίσκονται στην αποκλειστική κατοχή του χρήστη (καθώς δεν δύναται η εξαγωγή αυτών από την συσκευή) και είναι προσβάσιμα σε αυτόν μέσω username, password, και κωδικού μιας χρήσης που δημιουργείται σε συσκευή της επιλογής του. Η παραγωγή των κλειδιών πραγματοποιείται μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής στην οποία αποκτά πρόσβαση ο συνδρομητής κατόπιν εγκρίσεως της αίτησής τους.

4.3.2 Αποστολή του φορέα 'α.δ.δ.υ.' και κωδικού ενεργοποίησής του (PIN) στον συνδρομητή

Η Υ.Π.Φ. φροντίζει ώστε ο εξατομικευμένος φορέας και **ο απαραίτητος κωδικός για την ενεργοποίησή του** (PIN), να σταλούν στον συνδρομητή πάντα με ξεχωριστές αποστολές.

Συγκεκριμένα, ο φορέας μπορεί να σταλεί ταχυδρομικώς (στην διεύθυνση που έχει ορίσει στην αίτησή του ο συνδρομητής) ή να του παραδοθεί διαμέσου της σχετικής Τ.Υ.Υ., πάντα με απόδειξη παραλαβής, ενώ ο 'κωδικός ενεργοποίησης' (PIN) του φορέα στέλνεται πάντα με σφραγισμένο και αδιαφανή φάκελο στην διεύθυνση του συνδρομητή.

Επιπλέον στην περίπτωση δημιουργίας του Αναγνωρισμένου Πιστοποιητικού από τον ίδιο τον συνδρομητή, ο κωδικός ενεργοποίησης' (PIN), παράγεται αυτόματα και αποστέλλεται στον συνδρομητή μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής ή τον καθορίζει την στιγμή της δημιουργίας.

4.3.3 Αναστολή των πιστοποιητικών έως την Αρχική Ενεργοποίηση

Τα προσωπικά πιστοποιητικά SMART-SIGN™, **αμέσως μετά την έκδοσή τους** θέτονται, για λόγους ασφαλείας, σε κατάσταση 'Αναστολής' (προσωρινή ανάκληση) μέχρι την 'Αρχική Ενεργοποίησή' τους (βλ. παρ. 5.1.4), η οποία εξασφαλίζει ότι, πριν μπορέσουν να χρησιμοποιηθούν για πρώτη φορά τα πιστοποιητικά SMART-SIGN, ο σχετικός φορέας (και τα εμπεριεχόμενα σ' αυτόν 'δεδομένα δημιουργίας υπογραφής') και ο αντίστοιχος 'κωδικός ενεργοποίησής' του (PIN), βρίσκονται στα χέρια του συνδρομητή.

Επιπλέον στην περίπτωση δημιουργίας των Αναγνωρισμένων Πιστοποιητικών από τον ίδιο τον συνδρομητή η ενεργοποίηση των πιστοποιητικών πραγματοποιείται απευθείας από την ειδικά διαμορφωμένη διαδικτυακή εφαρμογή. Ταυτόχρονα ο 'κωδικός ενεργοποίησης' παρέχεται στον συνδρομητή από την εν λόγω εφαρμογή κατά την διαδικασία παραγωγής των κλειδιών.

5 ΟΡΟΙ ΔΙΑΧΕΙΡΙΣΗΣ ΚΥΚΛΟΥ ΖΩΗΣ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

5.1 ΑΙΤΗΣΗ, ΕΚΔΟΣΗ ΚΑΙ ΕΝΕΡΓΟΠΟΙΗΣΗ

5.1.1 Αίτηση του υποκειμένου και διαδικασία έγκρισης της αίτησης

Η αίτηση του υποψήφιου συνδρομητή για την απόκτηση αναγνωρισμένου πιστοποιητικού, γίνεται μόνο μέσω μιας συμβεβλημένης με τον συμμορφούμενο Π.Υ.Π. 'Τοπικής Υπηρεσίας Υποβολής' (Τ.Υ.Υ.) και πρέπει να περιέχει τα εξής:

- Τα στοιχεία του υποκειμένου που πρόκειται να πιστοποιηθούν (όνομα, επώνυμο, όνομα πατρός, υπηκοότητα και, προαιρετικά, μία διεύθυνση ηλεκτρονικού ταχυδρομείου),
- Το είδος και τα στοιχεία (εκδότης, αριθμός, ημερ/νία έκδοσης, ημερ/νία λήξης) του επισυναπτόμενου σε επικυρωμένο αντίγραφο ισχυρού 'δημόσιου εγγράφου ταυτοποίησης' (βλ. παρ. 4.2.1) που αποδεικνύει τα παραπάνω στοιχεία του υποκειμένου,
- Το τηλέφωνο και την διεύθυνση επικοινωνίας του υποψήφιου συνδρομητή, (στην οποία θα μπορούν να του αποσταλούν ο φορέας, το 'PIN' του και τυχόν φορολογικής φύσης παραστατικά),
- Μία διεύθυνση ηλεκτρονικού ταχυδρομείου (e-mail) -ανεξάρτητα αν αυτή ζητείται να πιστοποιηθεί- ή/και έναν αριθμό τηλεμοιοτυπίας (FAX), όπου θα μπορεί έγκαιρα και έγκυρα ο συνδρομητής να λαμβάνει ενημερωτικά μηνύματα (π.χ. προειδοποίηση λήξης πιστοποιητικού και φόρμα αίτησης ανανέωσής του) από τον Π.Υ.Π.
- Βεβαίωση γνησιότητας της υπογραφής του αιτούντα μετά την εξακρίβωση της φυσικής του ταυτότητας από δημόσια αρχή ή από τον αρμόδιο υπάλληλο της Τ.Υ.Υ. υπό τις προϋποθέσεις που το τελευταίο προβλέπεται (βλ. παρ. 4.2.1).

Ο αρμόδιος υπάλληλος της Τ.Υ.Υ., αφού ελέγξει πρόχειρα την πληρότητά της (σύμφωνα με τα παραπάνω), **συνυπογράφει την αίτηση** και την στέλνει (μαζί με την υπογεγραμμένη από τον υποψήφιο συνδρομητή 'Συνδρομητική Σύμβαση' και τα προσκομιζόμενα από αυτόν δικαιολογητικά), μέσα σε σφραγισμένο φάκελο στην σχετική Υπηρεσία Εγγραφής, **μέσα σε εύλογο χρονικό διάστημα.**.

Η Υπηρεσία Εγγραφής, έχοντας την ευθύνη για τον **τελικό έλεγχο** της αίτησης**,** εγκρίνει **ή** απορρίπτει την αίτηση **ή** ζητά την συμπλήρωση τυχόν ελλείψεων από τον αιτούντα, **εντός το πολύ πέντε (5) εργάσιμων ημερών** από την παραλαβή της αίτησης.

5.1.2 Εξατομίκευση φορέα και δημιουργία ζεύγους κλειδιών

Εφ' όσον η αίτηση του υποψήφιου συνδρομητή γίνει αποδεκτή από την Υπηρεσία Εγγραφής, αυτή δίνει εντολή στην Υ.Π.Φ.Σ. να εξατομικεύσει και να προετοιμάσει έναν φορέα για το υποκείμενο, παρέχοντάς της τα στοιχεία για την εξατομίκευση.

Η Υ.Π.Φ.Σ., αφού εξατομικεύσει τον φορέα και καταγράψει τον κωδικό ενεργοποίησης (PIN) του σε **σφραγισμένο φάκελο** για τον συνδρομητή, ενημερώνει την Υπηρεσία Εγγραφής για τα δημόσια κλειδιά που έχουν δημιουργηθεί στον φορέα αυτό. Τότε η Υπηρεσία Εγγραφής, συνδυάζει τα δημόσια αυτά κλειδιά του υποκειμένου που έλαβε από την Υ.Π.Φ.Σ. με τα στοιχεία του υποκειμένου που πρόκειται να πιστοποιηθούν και στέλνει την σχετική **εντολή** στον Εκδότη των πιστοποιητικών.

Εναλλακτικά, η Υπηρεσία Εγγραφής παραδίδει στον συνδρομητή ένα μη εξατομικευμένο φορέα. Ο συνδρομητής μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής εξατομικεύει τον φορέα (personalization) και παράγει το ζεύγος των κλειδιών απευθείας στον φορέα. Στην περίπτωση χρήσης Remote sign ο συνδρομητής λαμβάνει κωδικούς αρχικοποίησης της εφαρμογής για την παραγωγή του ζεύγους κλειδιών.

5.1.3 Έκδοση των πιστοποιητικών και αποστολή τους στον συνδρομητή

Όταν μια ηλεκτρονικά υπογεγραμμένη εντολή, από την Υπηρεσία Εγγραφής, για την έκδοση πιστοποιητικών φθάσει στον Εκδότη Πιστοποιητικών, ο Εκδότης (μέσω των σχετικών υπο-εκδοτών του, -βλ. παρ. 2.1.1) προχωρεί στην **έκδοση των ηλεκτρονικών πιστοποιητικών SMART-SIGN**™ των οποίων αντίγραφα στέλνει στην Υ.Π.Φ.Σ. για να τα εναποθέσει και αυτά στον σχετικό εξατομικευμένο φορέα που θα σταλεί στον συνδρομητή, σύμφωνα με την παρ. 4.3.2.

Αμέσως μετά την έκδοση των πιστοποιητικών, ο Εκδότης σε συνεργασία με την 'Υπηρεσία Διαχείρισης Ανάκλησης' δημοσιεύει τους σειριακούς αριθμούς τους στην 'Λίστα Ανακληθέντων Πιστοποιητικών' (CRL) ως 'ανασταλθέντα' (προσωρινώς ανακληθέντα), μέχρι να επαν-ενεργοποιηθούν (=ανάκληση της αναστολής τους) με την παρακάτω διαδικασία.

Στις περιπτώσεις που το αναγνωρισμένο πιστοποιητικό έχει εκδοθεί από τον συνδρομητή μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής, η ενημέρωση της 'Λίστας Ανακληθέντων Πιστοποιητικών' πραγματοποιείται αυτόματα από την εν λόγω εφαρμογή χωρίς επέμβαση από την Υ.Π.Φ.Σ.

5.1.4 Αρχική Ενεργοποίηση των πιστοποιητικών

Όταν ο συνδρομητής παραλάβει τον εξατομικευμένο φορέα του (με τα δεδομένα δημιουργίας υπογραφής και τα σχετικά –σε κατάσταση αναστολής- πιστοποιητικά) και τον αντίστοιχο 'κωδικό ενεργοποίησής' του (PIN), **πριν την οποιαδήποτε άλλη χρήση τους** πρέπει να ελέγξει την ορθότητα των περιεχομένων των πιστοποιητικών, και σε θετική περίπτωση να ζητήσει την 'Αρχική Ενεργοποίησή' τους, η οποία θα έχει ως αποτέλεσμα **τη διαγραφή των σειριακών αριθμών των ανασταλθέντων πιστοποιητικών του συνδρομητή από την 'Λίστα Ανακληθέντων Πιστοποιητικών' (Λ.Α.Π. ή CRL)**, ώστε να μπορούν τα πιστοποιητικά αυτά να χρησιμοποιηθούν **εύλογα** και από τρίτους.

Η Αρχική Ενεργοποίηση, γίνεται από την 'Υπηρεσία Διαχείρισης Ανάκλησης' του Π.Υ.Π. εφόσον αυτή λάβει την κατάλληλη ενημέρωση ότι ο φορέας δημιουργίας υπογραφής, τα ιδιωτικά κλειδιά και ο κωδικός ενεργοποίησής τους (PIN) βρίσκονται στα χέρια του συνδρομητή.

Επιπλέον η Αρχική Ενεργοποίηση μπορεί να πραγματοποιηθεί μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής, μέσω της οποίας πραγματοποιείται η διαχείριση του αναγνωρισμένου πιστοποιητικού του υποκειμένου.

Γραπτές οδηγίες για την σημασία και την διαδικασία της αρχικής ενεργοποίησης, πρέπει να συνοδεύουν τον φορέα κατά την παράδοσή του στον συνδρομητή.

5.2 ΙΣΧΥΣ, ΛΗΞΗ ΚΑΙ ΑΝΑΝΕΩΣΗ

5.2.1 Διάρκεια ισχύος των πιστοποιητικών

Τα προσωπικά πιστοποιητικά SMART-SIGN™ εκδίδονται με περίοδο ισχύος **ενός έτους** (με πιθανές αποκλίσεις για διαχειριστικούς λόγους, όπως αυτοί περιγράφονται στον Κανονισμό Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών OID 1.3.6.1.4.1.29402.1.1.1.1, έως +1 μήνα) που ξεκινά από την ημερομηνία έκδοσής τους, εκτός από την περίπτωση τακτικής ανανέωσης (βλ. παρακάτω) όπου η έναρξη ισχύος ορίζεται αμέσως μετά την λήξη του ισχύοντος πιστοποιητικού.

Κατά την διάρκεια ισχύος των πιστοποιητικών ο συνδρομητής τους μπορεί να κάνει **απεριόριστο αριθμό χρήσεών τους**, χωρίς καμιά επιπλέον επιβάρυνση, σύμφωνα με τους όρους του παρόντος.

5.2.2 Λήξη ισχύος των πιστοποιητικών

Οι ημερομηνίες έναρξης και λήξης ισχύος των πιστοποιητικών αναγράφονται ηλεκτρονικά μέσα σ΄ αυτά (όπως επιβάλλει το πρότυπο X.509 - RFC 5280) και μπορούν έτσι να αναγνωριστούν **αυτόματα** από τις περισσότερες εφαρμογές Η/Υ (-οι οποίες δεν θα επιτρέπουν την χρησιμοποίησή τους ή θα προβάλλουν κάποιο χαρακτηριστικό μήνυμα, στην περίπτωση που γίνει προσπάθεια τα πιστοποιητικά να χρησιμοποιηθούν εκτός της διάρκειας της ισχύος τους.) Παρ' όλα αυτά πρέπει να δηλώνεται **ρητά** πως μετά την λήξη του πιστοποιητικού **απαγορεύεται κάθε χρήση** των 'δεδομένων δημιουργίας υπογραφής' που αντιστοιχούν σ' αυτό **από τον συνδρομητή ή οποιονδήποτε άλλον**.

Ο Π.Υ.Π. **δεν θα αναλαμβάνει καμία ευθύνη** έναντι οποιουδήποτε τρίτου που βασίσθηκε σε ένα πιστοποιητικό που είχε λήξει κατά την ημέρα της δημιουργίας της υπογραφής.

5.2.3 Ανανέωση των πιστοποιητικών

Η ανανέωση των προσωπικών πιστοποιητικών SMART-SIGN™ μπορεί να είναι είτε '**τακτική'**, όπου ο συνδρομητής ζητάει την έκδοση νέων πιστοποιητικών από τον Π.Υ.Π. πριν λήξουν ή ανακληθούν τα υπάρχοντα πιστοποιητικά του, συμπληρώνοντας και υπογράφοντας ηλεκτρονικά την αίτηση ανανέωσης, είτε '**έκτακτη'**, (εάν τα πιστοποιητικά του έχουν λήξει ή ανακληθεί) οπότε ο συνδρομητής υποχρεούται να επαναλάβει την διαδικασία αρχικής εγγραφής σύμφωνα με τα οριζόμενα στην παρ 4.2.3.

Για την διευκόλυνση της τακτικής ανανέωσης, ο Π.Υ.Π. ενημερώνει τον συνδρομητή **τουλάχιστον 20 ημέρες πριν την λήξη των πιστοποιητικών** του για την διαδικασία και για την ηλεκτρονική διεύθυνση όπου μπορεί να βρει την ηλεκτρονική φόρμα ανανέωσης, ή, εφόσον ο συνδρομητής έχει δηλώσει ηλεκτρονική διεύθυνση ταχυδρομείου, του στέλνει σε αυτήν ηλεκτρονική ειδοποίηση μαζί με την σχετική φόρμα ανανέωσης για να την συμπληρώσει και να την υπογράψει.

Η ανανέωση του πιστοποιητικού συνίσταται στην έκδοση **νέου αναγνωρισμένου πιστοποιητικού** για το ίδιο φυσικό πρόσωπο και το οποίο θα έχει ημερομηνία έναρξης της ισχύος του την ημερομηνία λήξης του προηγούμενου πιστοποιητικού που ανανεώνεται.

Η ανανέωση απαιτεί την δημιουργία **νέων δεδομένων δημιουργίας υπογραφής** σε νέο ή ακόμη και στον ίδιο φορέα 'α.δ.δ.υ.' ανάλογα με το τι προβλέπει ο Κανονισμός Πιστοποίησης του Π.Υ.Π. (και εφόσον η τεχνολογία του φορέα επιτρέπει την δημιουργία νέων κλειδιών σ' αυτόν).

Ο Π.Υ.Π. μπορεί να ορίζει στον Κανονισμό του ή στην Συνδρομητική Σύμβαση και επιπλέον προϋποθέσεις για να κάνει δεκτή την αίτηση ανανέωσης πιστοποιητικών από τον συνδρομητή, όπως π.χ. να απαιτεί έγκριση της ανανέωσης από την Τ.Υ.Υ. που συνυπόγραψε την αρχική αίτηση του συνδρομητή, ιδίως εάν προβλέπεται ότι ο τυχόν νέος φορέας που θα χρησιμοποιηθεί θα πρέπει να προέρχεται από την Τ.Υ.Υ..

Η ανανέωση των πιστοποιητικών SMART-SIGN συνίσταται σε έκδοση νέων πιστοποιητικών που υπόκεινται στις ίδιες τις παρούσες πολιτικές ή **σε τυχόν νεώτερες αναθεωρημένες εκδόσεις του**ς, (βλ. σχετικά υποκεφάλαιο 10.2) με την προϋπόθεση ότι έχει ενημερωθεί σχετικά ο συνδρομητής. Με την έγκριση της σχετικής Τ.Υ.Υ., ή χωρίς αυτήν αν δεν την απαιτεί ο Π.Υ.Π., ο συνδρομητής μπορεί να ζητήσει κατά την ανανέωση, την **αντικατάσταση** των πιστοποιητικών SMART-SIGN™ –Κλάσης 2ης **με πιστοποιητικά SMART-SIGN™ άλλης κλάσης**, -εφόσον παρέχονται εκείνη την περίοδο από το συγκεκριμένο Π.Υ.Π..

Επιπλέον ο συνδρομητής μπορεί να πραγματοποιήσει την ανανέωση του αναγνωρισμένου πιστοποιητικού του μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής.

5.3 ΑΝΑΣΤΟΛΗ, ΑΝΑΚΛΗΣΗ ΚΑΙ (ΕΠΑΝ-)ΕΝΕΡΓΟΠΟΙΗΣΗ

5.3.1 Αναστολή και ανάκληση του πιστοποιητικού

Η '**αναστολή'** (προσωρινή ανάκληση) και η (οριστική) '**ανάκληση'** των προσωπικών πιστοποιητικών SMART-SIGN γίνεται με την δημοσίευση των σειριακών αριθμών των συγκεκριμένων πιστοποιητικών στην σχετική 'Λίστα Ανακληθέντων Πιστοποιητικών' (CRL) του Π.Υ.Π..

Η αναστολή των πιστοποιητικών **επιβάλλεται** να προκληθεί από τον συνδρομητή-κάτοχο των πιστοποιητικών ή από τον ίδιο τον Π.Υ.Π. στην περίπτωση ύπαρξης έστω και 'αμυδράς υποψίας' για έκθεση των σχετικών δεδομένων δημιουργίας υπογραφής προς οποιονδήποτε τρίτο, ενώ η ανάκλησή τους στην αντίστοιχη περίπτωση της σοβαρής υποψίας ή της βεβαιότητας για κάποιο παρόμοιο τέτοιο γεγονός. Την **ανάκληση** των πιστοποιητικών του είναι επίσης **υποχρεωμένος** να ζητήσει ο συνδρομητής στην περίπτωση που απολέσει τον έλεγχο των σχετικών δεδομένων δημιουργίας υπογραφής τους ή εάν διαπιστώσει ότι δεν αληθεύει κάποιο από τα περιεχόμενα στο πιστοποιητικό στοιχεία του.

Ο Π.Υ.Π. μπορεί να προβεί στην αναστολή ή στην ανάκληση των πιστοποιητικών οποτεδήποτε κρίνει ότι έτσι προστατεύεται η ασφάλεια της υποδομής του ή σε οποιαδήποτε άλλη περίπτωση προβλέπεται σχετικά από τον Κανονισμό Πιστοποίησής του, ενημερώνοντας σχετικά τον συνδρομητή. Σε περίπτωση ανάκλησης των πιστοποιητικών χωρίς την ύπαρξη ευθύνης εκ μέρους του συνδρομητή, ο Π.Υ.Π. υποχρεούται να τον

αποζημιώσει για το υπόλοιπο χρονικό διάστημα κανονικής ισχύος των πιστοποιητικών του (βλ. σχετικά παρ. 9.2.2).

Τα πιστοποιητικά 'SMART-SIGN' **δεν επιτρέπεται** να μείνουν σε κατάσταση αναστολής για συνεχόμενο χρονικό διάστημα άνω της μίας εβδομάδας˙ εάν έως το πέρας αυτής της περιόδου δεν διευθετηθούν οι αιτίες για τις οποίες τα πιστοποιητικά τέθηκαν σε αναστολή ώστε αυτά να (επαν-) ενεργοποιηθούν, τότε **αυτομάτως** πρέπει να θέτονται σε κατάσταση οριστικής ανάκλησης!

Τέλος ο συνδρομητής δύναται να αναστείλει ή να ανακαλέσει το αναγνωρισμένο πιστοποιητικό του μέσω της ειδικά διαμορφωμένης διαδικτυακής εφαρμογής. Η δημοσίευση των σειριακών αριθμών των συγκεκριμένων πιστοποιητικών στην σχετική 'Λίστα Ανακληθέντων Πιστοποιητικών' (CRL) του Π.Υ.Π. πραγματοποιείται αυτόματα από την εφαρμογή.

5.3.2 Ενεργοποίηση μετά από αναστολή

Η (επαν-)ενεργοποίηση των πιστοποιητικών μετά από την θέση τους στην 'προσωρινή' κατάσταση αναστολής' συνίσταται στην διαγραφή των σειριακών αριθμών τους από την 'Λίστα Ανακληθέντων Πιστοποιητικών' (CRL) στην οποία είχαν καταγραφεί με την διαδικασία της 'αναστολής' τους.

Η ενεργοποίηση των πιστοποιητικών απαιτεί σχετική αίτηση από τον συνδρομητή-κάτοχο των πιστοποιητικών, ο οποίος, με την πράξη του αυτή, **αναλαμβάνει πλήρως την ευθύνη** για την μη ύπαρξη λόγων που θα επέβαλαν την οριστική ανάκληση των πιστοποιητικών. Ο Π.Υ.Π. όμως, εφόσον επικαλεστεί λόγους ασφάλειας της υποδομής του ή άλλους λόγους που προβλέπονται από τον Κανονισμό του, **μπορεί να αρνηθεί το αίτημα** της (επαν-)ενεργοποίησης των πιστοποιητικών από τον συνδρομητή και να προβεί έτσι στην οριστική ανάκλησή τους.

Επιπλέον, η ενεργοποίηση του αναγνωρισμένου πιστοποιητικού του συνδρομητή μπορεί να πραγματοποιηθεί από την ειδικά διαμορφωμένη διαδικτυακή εφαρμογή διαχείρισης πιστοποιητικών. Κατά την διαδικασία αυτή η διαγραφή των σειριακών αριθμών από λίστα 'Λίστα Ανακληθέντων Πιστοποιητικών' (CRL) στην οποία είχαν καταγραφεί κατά την διαδικασία 'αναστολής' τους πραγματοποιείται αυτόματα από την εν λόγω διαδικτυακή εφαρμογή.

Η (επαν-) ενεργοποίηση πιστοποιητικών που είχαν 'ανακληθεί' οριστικά δεν επιτρέπεται σε καμιά περίπτωση!

5.4 ΥΠΗΡΕΣΙΕΣ ΔΗΜΟΣΙΕΥΣΗΣ ΚΑΤΑΣΤΑΣΗΣ ΤΩΝ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

5.4.1 Υπηρεσία Καταλόγου εκδοθέντων πιστοποιητικών

Ο Π.Υ.Π. που εκδίδει πιστοποιητικά SMART-SIGN **οφείλει** να παρέχει σε συγκεκριμένη και γνωστή ηλεκτρονική διεύθυνση 'υπηρεσία καταλόγου εκδοθέντων πιστοποιητικών' (Directory) στην οποία θα δημοσιεύει και θα καθιστά προσβάσιμα σε οποιονδήποτε ενδιαφερόμενο τρίτο όλα τα προσωπικά πιστοποιητικά SMART-SIGN που έχει εκδώσει (είτε 'αναγνωρισμένα' είτε 'ταυτοποίησης') για λόγους επαλήθευσής τους, **με την προϋπόθεση** ότι δεν έχει αντιταχθεί στην δημοσίευσή τους ο κάτοχός τους-συνδρομητής του Π.Υ.Π. κατά την αίτησή του για την έκδοσή τους ή και αργότερα *(βλ. σχετικά παρ. 9.1.3: 'Προστασία δεδομένων προσωπικού χαρακτήρα')*.

Η δημοσίευση μπορεί να γίνεται με την τεχνολογία 'LDAP' ή 'HTTP' και θα επιτρέπει την αναζήτηση συγκεκριμένων πιστοποιητικών βάσει των περιεχόμενων στο πιστοποιητικό στοιχείων του υποκειμένου ή τον σειριακό αριθμό των πιστοποιητικών. Είναι επιτρεπτό να παρέχονται από τον ίδιο κατάλογο και άλλα πιστοποιητικά SMART-SIGN που δεν είναι ενεργά εκείνη την στιγμή (λόγω π.χ. λήξης ή ανάκλησή τους), αλλά θα πρέπει σ' αυτήν την περίπτωση να παρέχεται σαφής ένδειξη κατά την εμφάνιση των πιστοποιητικών σχετικά με την κατάσταση ισχύος τους.

Η υπηρεσία αυτή **πρέπει** (στο βαθμό που η ύπαρξη δεύτερου εφεδρικού συστήματος το εξασφαλίζει) να είναι διαθέσιμη 24 ώρες το 24ωρο, όλο το χρόνο, να ενημερώνεται άμεσα (εντός το πολύ 24 ωρών) μετά από κάθε έκδοση, ανάκληση ή/και ενεργοποίηση και να παρέχεται από τον Π.Υ.Π. **δωρεάν**.

5.4.2 Υπηρεσία καταλόγου ανασταλθέντων και ανακληθέντων πιστοποιητικών (CRL)

Ο κατάλογος (λίστα) με τα ανασταλθέντα και τα ανακληθέντα πιστοποιητικά SMART-SIGN που έχει εκδώσει ο Π.Υ.Π. ('Λίστα Ανακληθέντων Πιστοποιητικών' – ΛΑΠ ή CRL) πρέπει να είναι διαθέσιμη και να παρέχεται δωρεάν 24 ώρες το 24ωρο, όλο το χρόνο, (στο βαθμό που η ύπαρξη δεύτερου εφεδρικού συστήματος το εξασφαλίζει) **στην ηλεκτρονική διεύθυνση του Π.Υ.Π. που αυτός αναγράφει μέσα στα ίδια τα πιστοποιητικά SMART-SIGN όταν τα εκδίδει** (στο υποχρεωτικό πεδίο τους 'CRLDistributionPoint').

Η τεχνολογία παρουσίασης (πρωτόκολλο) του καταλόγου CRL πρέπει να είναι τύπου 'LDAP' (σύμφωνα με τα οριζόμενα στο υποκεφάλαιο 8.2 σχετικά με το 'Profile' του CRL), και πρέπει να περιλαμβάνει στα πεδία του τουλάχιστον τον σειριακό αριθμό του πιστοποιητικού στο οποίο αναφέρεται, σχετικούς 'δείκτες' για την αιτία της εγγραφής του πιστοποιητικού στην λίστα (π.χ. 'αναστολή' ή οριστική 'ανάκληση' κ.λ.π.) και την ακριβή ώρα που συνέβηκε η εγγραφή σ' αυτόν, ενώ όλα τα δεδομένα του θα πρέπει να εξασφαλίζονται από αλλοίωση με την **ηλεκτρονική υπογραφή του** από τον εκδότη, από τα ίδια τα ίδια κλειδιά που χρησιμοποίησε για την έκδοση των -εμπεριεχόμενων σ' αυτόν τον κατάλογο- πιστοποιητικών!

Η **συχνότητα της ανανέωσης** του καταλόγου (με την έκδοση νέου χρονοσημασμένου καταλόγου ο οποίος θα περιλαμβάνει και ένδειξη για την ακριβή ώρα της επόμενης τακτικής έκδοσης) **δεν πρέπει να υπερβαίνει τις 24 ώρες,** ενώ ο Π.Υ.Π. μπορεί να προβλέπει στον Κανονισμό του και περιπτώσεις στις οποίες θα εκδίδει και 'έκτακτες εκδόσεις' του καταλόγου CRL.

Άλλοι τρόποι δημοσίευσης της κατάστασης των πιστοποιητικών, όπως η υπηρεσία 'On-line Certificate Status Protocol' (OCSP) ή η έκδοση τμηματικών καταλόγων (dCRLs), επιτρέπονται μόνο εφόσον προβλέπονται ρητά από τον Κανονισμό Πιστοποίησης του Π.Υ.Π..

6 ΕΓΚΥΡΟΤΗΤΑ ΚΑΙ ΑΠΟΔΕΙΚΤΙΚΗ ΙΚΑΝΟΤΗΤΑ

6.1 ΕΛΕΓΧΟΣ ΕΓΚΥΡΟΤΗΤΑΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ & ΥΠΟΓΕΓΡΑΜΜΕΝΩΝ ΕΓΓΡΑΦΩΝ

6.1.1 Έλεγχος εγκυρότητας των προσωπικών πιστοποιητικών SMART-SIGN™

Για να χρησιμοποιήσει ή να βασισθεί εύλογα κάποιος στα περιεχόμενα των πιστοποιητικών SMART-SIGN, θα πρέπει **πρώτα** να ελέγξει και να επιβεβαιώσει την **εγκυρότητά** τους.

Έγκυρα θεωρούνται τα πιστοποιητικά SMART-SIGN που δεν έχει παρέλθει η ημερομηνία λήξης τους και που δεν έχουν ανακληθεί οριστικά ή 'προσωρινά' (=αναστολή).

Ο έλεγχος της τυχόν ανάκλησης των πιστοποιητικών SMART-SIGN γίνεται με την **αντιπαραβολή** του 'σειριακού αριθμού έκδοσής' τους (serial number) -που τα χαρακτηρίζει μοναδικά και εμπεριέχεται ως πεδίο μέσα στα ίδια τα πιστοποιητικά-, με τους 'σειριακούς αριθμούς' των πιστοποιητικών που περιλαμβάνονται στην σχετική 'Λίστα Ανακληθέντων Πιστοποιητικών' (CRL) που δημοσιεύει ο Εκδότης τους, σύμφωνα με την παρ. 5.4.2 αυτής της πολιτικής.

Ο έλεγχος αυτός, μπορεί να γίνει **είτε** άμεσα από τον ενδιαφερόμενο, με την ανάγνωση της λίστας 'CRL' από αυτόν και την εφαρμογή της παραπάνω μεθόδου αντιπαραβολής των σειριακών αριθμών, **είτε** με την χρήση ειδικού λογισμικού ελέγχου της εγκυρότητας των πιστοποιητικών (το οποίο είναι ικανό να ελέγχει τέτοιες λίστες) και το οποίο **ο χρήστης εμπιστεύεται**.

6.1.2 Εγκατάσταση και έλεγχος εγκυρότητας της αλυσίδας των ιεραρχικά ανώτερων πιστοποιητικών

Τα πιστοποιητικά SMART-SIGN προϋποθέτουν την έγκυρη υπογραφή τους από έναν 'Υπο-εκδότη' (βλ. παρ. 2.2.1) ο οποίος πρέπει με την σειρά του να φέρει πιστοποιητικό υπογεγραμμένο από τον 'κυρίως' Εκδότη -που εκπροσωπεί τον Π.Υ.Π..

Έτσι, εκτός από τον παραπάνω έλεγχο εγκυρότητας των πιστοποιητικών SMART-SIGN, ο βασιζόμενος σ' αυτά τρίτος θα πρέπει να εγκαταστήσει στον υπολογιστή του και να ελέγξει τόσο τα πιστοποιητικά του Υπο-εκδότη όσο και του 'κυρίως' Εκδότη τους **ώστε να αποκλείσει την περίπτωση πλαστότητάς τους**.

Η 'αλυσίδα' των πιστοποιητικών που πρέπει να ελεγχθεί σταματάει με ένα **αυτοϋπογραφόμενο** (self-signed) πιστοποιητικό (στο οποίο δηλαδή το πεδίο 'Issuer' *(εκδότης)* και 'Subject' *(υποκείμενο)* είναι ακριβώς τα ίδια) και το οποίο θα **πρέπει να αποδεχθεί και να εγκαταστήσει** ως αξιόπιστο 'Θεμελιώδη Εκδότη Πιστοποιητικών' (Θ.Ε.Π. ή 'Root-CA') στον υπολογιστή του ο χρήστης.

Ο Π.Υ.Π., **πρέπει** να παρέχει μέσα από τις ηλεκτρονικές σελίδες του **όλα αυτά τα πιστοποιητικά** που είναι απαραίτητα για τον έλεγχο της 'αλυσίδας εμπιστοσύνης' των πιστοποιητικών (από τον Θεμελιώδη Εκδότη έως τα τελικά πιστοποιητικά SMART-SIGN).

6.1.3 Μακροχρόνιος έλεγχος υπογεγραμμένων εγγράφων -Χρονοσήμανση (time stamping)

Για να μπορεί να αποδειχθεί με ασφάλεια η εγκυρότητα ενός εγγράφου που έχει υπογραφθεί με την χρήση ενός ισχυρού -κατά την υπογραφή- πιστοποιητικού SMART-SIGN **μετά την λήξη ή ανάκληση του πιστοποιητικού αυτού** (μακροχρόνιος έλεγχος), απαιτείται επιπλέον η προσθήκη '**χρονοσήμανσης**' (time-stamps) στο έγγραφο αυτό και μάλιστα **πριν** την λήξη ή ανάκληση του χρησιμοποιούμενου πιστοποιητικού.

Μόνο έτσι εξασφαλίζεται ότι το έγγραφο 'δεν υπογράφθηκε πλαστώς' από κάποιον τρίτο στον οποίον εκτέθηκαν τα συγκεκριμένα 'δεδομένα δημιουργίας υπογραφής' **μετά** την ανισχυροποίηση του σχετικού πιστοποιητικού (η οποία μπορεί και να έγινε με ανάκληση ακριβώς εξαιτίας της έκθεσης αυτής!).

Οι υπηρεσίες χρονοσήμανσης –που δεν αποτελούν αντικείμενο αυτής της πολιτικής- μπορούν να παρέχονται από τον ίδιο τον συμμορφούμενο με την παρούσα πολιτική Π.Υ.Π. που εκδίδει πιστοποιητικά SMART-SIGN, είτε από οποιονδήποτε άλλον Π.Υ.Π.

6.2 ΣΤΟΙΧΕΙΑ ΠΟΥ ΚΑΤΑΧΩΡΟΥΝΤΑΙ – ΠΡΟΣΒΑΣΗ - ΧΡΟΝΟΣ ΑΡΧΕΙΟΘΕΤΗΣΗΣ

6.2.1 Αποδεικτικά στοιχεία που καταχωρούνται κατά τη διαχείριση των πιστοποιητικών

Ο Π.Υ.Π. που εκδίδει πιστοποιητικά SMART-SIGN **οφείλει** να διατηρεί 'προσωπικό φάκελο' για κάθε συνδρομητή του, ο οποίος περιλαμβάνει τουλάχιστον:

α) την αρχική αίτηση μαζί με την υπογεγραμμένη σύμβαση και τα επισυναπτόμενα δικαιολογητικά,

β) πρωτόκολλο έγκρισης της αίτησης του συνδρομητή, υπογεγραμμένο από τον υπεύθυνο υπάλληλο της Υπηρεσίας Εγγραφής, ή άλλη σχετική απόδειξη,

γ) πρωτόκολλο προετοιμασίας και αποστολής του φορέα 'α.δ.δ.υ.', με τα στοιχεία του εξατομικευμένου φορέα του συνδρομητή και τα σχετικά αποδεικτικά αποστολής και παραλαβής του φορέα, υπογεγραμμένο από τον υπεύθυνο της Υπηρεσίας Προετοιμασίας Φορέα Συνδρομητών, ή άλλη σχετική απόδειξη,

δ) πρωτόκολλο για την έκδοση των πιστοποιητικών SMART-SIGN με τους σειριακούς αριθμούς αυτών, την ακριβή ώρα της έκδοσής τους και τα πιστοποιούμενα δημόσια κλειδιά, καθώς και αναφορά της πράξης και την ακριβή ώρα την οποία αυτά τέθηκαν σε αρχική 'αναστολή', υπογεγραμμένο από τον υπεύθυνο της 'υπηρεσίας' Έκδοσης πιστοποιητικών, ή άλλη σχετική απόδειξη,

ε) Πληροφορίες και αποδεικτικά στοιχεία για κάθε αίτημα αλλαγής κατάστασης των πιστοποιητικών του συνδρομητή, (όπως αρχική ενεργοποίηση, αναστολή, ενεργοποίηση ή ανάκληση) με σαφείς καταγραφές για το από ποιόν, πώς, πότε έγιναν τα αιτήματα αυτά και αν και πότε ακριβώς ικανοποιήθηκαν,

στ) Πρωτόκολλα για κάθε τακτική ανανέωση των πιστοποιητικών του με μνεία της σχετικά υπογεγραμμένης εντολής ανανέωσης του συνδρομητή, ή εκ νέου τα στοιχεία υπό α΄, β΄, γ΄ και δ΄ για κάθε 'μή τακτική' ανανέωση.

ζ) Στοιχεία και τυχόν αντίγραφα εγγράφων για κάθε παράπονο ή αίτημα για επίλυση διαφοράς που προέρχεται ή σχετίζεται με τον συνδρομητή, καθώς και στοιχεία για την πορεία της διευθέτησης αυτής.

Μέρος των παραπάνω στοιχείων, ο Π.Υ.Π. **μπορεί**, εφόσον εξασφαλίζει την ακεραιότητα και την διαθεσιμότητά τους, να διατηρεί σε **ηλεκτρονική μορφή** (logs), με την προϋπόθεση όμως ότι αυτά θα μπορούν να εκτυπωθούν άμεσα σε κατανοητή γλώσσα σε χαρτί, να επικυρωθούν από τον Π.Υ.Π. και να διατεθούν σε αποδεικτικές διαδικασίες **οποιαδήποτε στιγμή αυτό απαιτηθεί**.

Πέρα από τα στοιχεία σχετικά με τον συνδρομητή, ο Π.Υ.Π. θα πρέπει να καταγράφει και να είναι σε θέσει να αποδείξει τις ακριβείς ώρες και τα περιεχόμενα όλων των εκδόσεων καταλόγων CRL που έχει εκδώσει.

6.2.2 Περίοδος αρχειοθέτησης

Όλα τα παραπάνω στοιχεία που σχετίζονται με την ύπαρξη και τη εγκυρότητα ενός Πιστοποιητικού SMART-SIGN™ **διατηρούνται αναλλοίωτα για μια περίοδο 30 ετών** από την λήξη ισχύος του πιστοποιητικού ώστε να είναι διαθέσιμα για την διαδικασία 'Επίλυσης Διαφορών' που παρέχει ο Π.Υ.Π. (βλ. παρ. 9.1.4) και για την παροχή αποδεικτικών στοιχείων σε τυχόν άλλες νομικές ή διοικητικές διαδικασίες.

Καμία εγγύηση για την παραπάνω δυνατότητα **δεν δίνεται** στον συνδρομητή-πιστοποιούμενο ή στον οποιοδήποτε τρίτο που βασίσθηκε σε ένα πιστοποιητικό **μετά από αυτήν την περίοδο.**

6.2.3 Πρόσβαση στα αποδεικτικά στοιχεία

Πρόσβαση στις πληροφορίες του φακέλου του μπορεί να έχει **άμεσα** ο συνδρομητής και **έμμεσα** (διαμέσου μιας 'Επιτροπής Επίλυσης Διαφορών'), οποιοδήποτε τρίτος αποδείξει ότι έχει έννομο συμφέρον που σχετίζεται με συγκεκριμένο πιστοποιητικό του συνδρομητή.

Αν η διαδικασία Επίλυσης Διαφορών ή Διευθέτησης Παραπόνων που **υποχρεωτικά** (-σύμφωνα με την παρούσα πολιτική) **προβλέπει και παρέχει ο Π.Υ.Π.** προς τους τρίτους ή τους συνδρομητές του, δεν ικανοποιήσει τον ενδιαφερόμενο, ο Π.Υ.Π. είναι υποχρεωμένος να παράσχει τα παραπάνω αποδεικτικά στοιχεία ενώπιον οποιασδήποτε δικαστικής ή διοικητικής αρχής επιληφθεί του θέματος της διαφοράς μετά από σχετικό αίτημα της,

7 ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ & ΑΞΙΟΠΙΣΤΙΑΣ

7.1 ΤΕΧΝΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ

7.1.1 Κρυπτογραφικά κλειδιά του Εκδότη των πιστοποιητικών

Η δημιουργία και αποθήκευση των κρυπτογραφικών κλειδιών του Θεμελιώδη Εκδότη και των Υπο-Εκδοτών του (που υπογράφουν τα πιστοποιητικά SMART-SIGN™), πρέπει να γίνεται με ειδική '**ασφαλή μονάδα υλικού**' (*Hardware Security Module*) η λειτουργία της οποίας θα είναι πιστοποιημένη βάσει του προτύπου [FIPS 140-2 level 3].

Η δημιουργία, η χρήση, η αντιγραφή, η αποθήκευση και η επανάκτηση των παραπάνω κλειδιών πρέπει να απαιτούν την σύμπραξη τουλάχιστον δύο (2) διαπιστευμένων ατόμων.

Το μέγεθος των κλειδιών του Εκδότη (CA) πρέπει να έχουν ελάχιστο μέγεθος **4098 Bits** και των Υπο-Εκδοτών του (Subordinate CAs) πρέπει να έχουν ελάχιστο μέγεθος **2048 Bits,** και να χρησιμοποιούν τον αλγόριθμο [Rivest - Shimar - Adleman Algorithm] **(RSA)** για την δημιουργία τους και τον αλγόριθμο [Secure Hashing Algorithm – 1] **(SHA-1)** για τον 'κατακερματισμό' (Hashing) κατά την υπογραφή.

Η χρήση των κλειδιών των Υπο-Εκδοτών του -σύμμορφου με την παρούσα πολιτική- Π.Υ.Π., πρέπει να περιορίζεται **αποκλειστικά** στην υπογραφή 'Πιστοποιητικών' και 'Λιστών Ανακληθέντων Πιστοποιητικών' (ΛΑΠ) χωρίς να επιτρέπεται η χρησιμοποίησή τους για κανέναν άλλον σκοπό ή χρήση.

Τα κρυπτογραφικά κλειδιά του Εκδότη (και των Υπο-Εκδοτών του σε πιο συχνή βάση) πρέπει να έχουν περιορισμένη χρονική διάρκεια ισχύος (το πολύ 20 έτη για τον Εκδότη και το πολύ 10 έτη για τους Υπο-Εκδότες), οπότε, με την λήξη τους (ή ακόμη και με την ανάκλησή τους), να καταστρέφονται αφού πρώτα έχουν εκδοθεί νέα κλειδιά που τα αντικαθιστούν.

7.1.2 Κρυπτογραφικά κλειδιά και Φορέας 'α.δ.δ.υ.' των ιδιωτικών κλειδιών των συνδρομητών.

Τα κλειδιά των συνδρομητών δημιουργούνται υποχρεωτικά από την Υ.Π.Φ.Σ. του Π.Υ.Π. και κατά την δημιουργία τους λαμβάνονται ανάλογα επίπεδα ασφαλείας με τα κλειδιά των Εκδοτών. Το μέγεθος των δημόσιων κλειδιών που παράγονται για τον συνδρομητή από την Υ.Π.Φ.Σ. για να πιστοποιηθούν με πιστοποιητικά SMART-SIGN™, πρέπει να έχουν μέγεθος **τουλάχιστον 2048Bits** και να χρησιμοποιούν τους ίδιους αλγόριθμους για την δημιουργία τους, την δημιουργία υπογραφής και τον κατακερματισμό (RSA και SHA-1 αντίστοιχα).

Ο εξατομικευμένος φορέας 'ασφαλούς διάταξης δημιουργίας υπογραφής' (π.χ. smart card) που παρέχεται υποχρεωτικά στον συνδρομητή των πιστοποιητικών SMART-SIGN™ μέσω της Υ.Π.Φ.Σ. του Π.Υ.Π., πρέπει να συμμορφώνεται στις απαιτήσεις ασφαλείας με τα εκάστοτε ισχύοντα πρότυπα και να απαιτεί την χρήση μυστικού '**Κωδικού Ενεργοποίησης**' (PIN) για τη χρήση των περιεχόμενων σ' αυτόν ιδιωτικών κλειδιών, που ο ΠΥΠ εξασφαλίζει ότι γνωστοποιείται μόνο στον συνδρομητή.

7.1.3 Απαγόρευση επιμερισμού (escrow) ή άλλης διαδικασίας ανάκτησης των ιδιωτικών κλειδιών

Τα 'δεδομένα δημιουργίας υπογραφής' (*ιδιωτικά κλειδιά*) που δημιουργεί η ΥΠΦΣ του Π.Υ.Π. για τον συνδρομητή των οποίων τα 'δεδομένα επαλήθευσης υπογραφής' (*δημόσια κλειδιά*) θα πιστοποιηθούν με πιστοποιητικά SMART-SIGN, καθώς και το ιδιωτικό κλειδί του Παρόχου Υπηρεσιών Πιστοποίησης **δεν επιτρέπεται** να εξαχθούν από τον εξατομικευμένο φορέα του συνδρομητή ή να αντιγραφούν σε οποιοδήποτε αρχείο του Π.Υ.Π., **ούτε** να τύχουν οποιασδήποτε άλλης μεθόδου που να επιτρέπει την, έστω υπό όρους, **επανάκτησή** τους, όπως ο 'επιμερισμός' (γνωστός και ως 'key escrow').

7.2 ΑΛΛΕΣ ΑΠΑΙΤΗΣΕΙΣ ΑΣΦΑΛΕΙΑΣ ΚΑΙ ΑΞΙΟΠΙΣΤΙΑΣ ΤΟΥ Π.Υ.Π.

7.2.1 Αξιοπιστία συστήματος του Π.Υ.Π. – Συμμόρφωση με διεθνή πρότυπα ασφάλειας

Ο Πάροχος Υπηρεσιών Πιστοποίησης (Π.Υ.Π.) που εκδίδει πιστοποιητικά τύπου SMART-SIGN™ σύμφωνα με την παρούσα πολιτική, πρέπει να έχει εξασφαλίσει ένα 'αξιόπιστο σύστημα' για την παροχή των υπηρεσιών του, το οποίο να καλύπτει πλήρως τις σχετικές του Κανονισμού (ΕΕ) αριθ. 910/2014 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου της 23ης Ιουλίου 2014. Επιπλέον, πρέπει να έχει εξασφαλίσει

ένα 'αξιόπιστο σύστημα' για την παροχή υπηρεσιών το οποίο να ακολουθεί τις υποδείξεις των προτύπων *IETF RFC 5280 (2006): 'Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile'* και *"CWA 14167-1: Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures"* του ευρωπαϊκού οργανισμού τυποποίησης CEN.

Παράλληλα, ο συμμορφούμενος με τις παρούσες πολιτικές Π.Υ.Π., πρέπει να υιοθετεί στον 'Κανονισμό Πιστοποίησής Αναγνωρισμένων Πιστοποιητικών' του (C.P.S.) τις τεχνικές, λειτουργικές και διαχειριστικές απαιτήσεις που ορίζονται για την πολιτική **QCP-n-qscd** στο κεφάλαιο 5 του 'προτύπου' **ETSI EN 319 411-2 (2016-02): Policy requirements for certification authorities issuing qualified certificates** *"* του ευρωπαϊκού οργανισμού τυποποίησης ETSI **.**

7.2.2 Φυσική ασφάλεια, Ασφάλεια διαδικασιών, Εκπαίδευση και έλεγχος αξιοπιστίας προσωπικού

Ο Π.Υ.Π. πρέπει να λαμβάνει όλα τα απαραίτητα μέτρα που εξασφαλίζουν την φυσική ασφάλεια των συστημάτων λειτουργίας του, όπως πρόβλεψη για τον κλιματισμό, την συνεχή παροχή ρεύματος, την έλλειψη διαρροών, την πυροπροστασία και την απαγόρευση της φυσικής πρόσβασης μη εξουσιοδοτημένων ατόμων στον χώρο κύριας λειτουργία του συστήματός του.

Παράλληλα θα πρέπει να έχει ορίσει με σαφήνεια στον Κανονισμό Πιστοποίησής του τις διαδικασίες εκείνες που εξασφαλίζουν την διεκπεραίωση των λειτουργιών του συστήματός της από εξουσιοδοτημένα άτομα με συγκεκριμένους ρόλους και δικαιώματα πρόσβασης, απαιτώντας την σύμπραξη δύο χρηστών στις κρίσιμες λειτουργίες.

Τέλος θα πρέπει να προβλέπει την συνεχή εκπαίδευση και την ενημέρωση του προσωπικού, και να εξασφαλίζει μέσα από συμβατικές δεσμεύσεις και ελέγχους την εχεμύθειά και την μη διάδοση ευαίσθητων πληροφοριών ασφάλειας του συστήματος και προσωπικών δεδομένων των συνδρομητών.

7.2.3 Οικονομική αξιοπιστία και επιβιωσιμότητα του Π.Υ.Π.

Ο Π.Υ.Π. που εκδίδει πιστοποιητικά SMART-SIGN™ **πρέπει να είναι νομικό πρόσωπο** (ιδιωτικού ή δημοσίου δικαίου) και να επιδεικνύει τα κατάλληλα 'εχέγγυα' για την οικονομική ικανότητα και την επιβιωσιμότητα του η οποία είναι αναγκαία για την μακροχρόνια άσκηση των δραστηριοτήτων ψηφιακής πιστοποίησης. Σε κάθε περίπτωση ο συμμορφούμενος με την παρούσα πολιτική Π.Υ.Π. **θα πρέπει να προβλέπει στον Κανονισμό Πιστοποίησής του** τις ενέργειες που θα πρέπει να γίνουν καθώς και τον τρόπο διευθέτησης των αρχείων του και των ενεργών πιστοποιητικών του στην περίπτωση παύσης ή τερματισμού των λειτουργιών του.

7.2.4 Λειτουργική αυτοτέλεια

Αν η δραστηριότητα της 'παροχής υπηρεσιών ψηφιακής πιστοποίησης' αποτελεί μέρος μόνο των συνολικών δραστηριοτήτων του νομικού προσώπου του Π.Υ.Π., το τμήμα που θα ασχολείται με τις δραστηριότητες αυτές **θα πρέπει να έχει απόλυτη λειτουργική αυτοτέλεια και αυτόνομες υποδομές και εγκαταστάσεις** σε σχέση με τα υπόλοιπα τμήματα του νομικού προσώπου.

8 ΠΕΡΙΓΡΑΦΗ (PROFILE) ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ & Λ.Α.Π. (C.R.L.)

8.1 ΠΕΡΙΓΡΑΦΗ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ

8.1.1 Τύπος και αριθμός έκδοσης

Τα προσωπικά πιστοποιητικά Smart-Sign™ του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ είναι 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.

8.1.2 Περιεχόμενο και σημασία των πεδίων των πιστοποιητικών

Τα αναγνωρισμένα πιστοποιητικά Smart-Sign™, περιέχουν τουλάχιστον τα εξής βασικά και εκτεταμένα πεδία του τύπου X.509 V3:

Όνομα πεδίου (*)	Περιεχόμενο	Παρατηρήσεις
Έκδοση ***Version***	"V3"	*Έκδοση '3' του προτύπου ηλεκ. πιστοποιητικών 'X.509 - RFC 5280' που υποστηρίζει εκτεταμένα πεδία.*
Σειριακός Αριθμός ***Serial Number***	[Ακέραιος αριθμός]	*Μοναδικός αριθμός του εκδιδόμενου πιστοποιητικού από τον συγκεκριμένο εκδότη*
Αλγόριθμος Υπογραφής ***Signature Algorithm***	[Προσδιοριστικό]	*Προσδιορίζει τον αλγόριθμο που χρησιμοποιήθηκε για τον κατακερματισμό (Hash) και την υπογραφή του πιστοποιητικού*
Εκδότης ***Issuer***	(**Διακεκριμένο Όνομα (DN)** τύπου 'X.501' για τον Εκδότη)	*Το όνομα του εκδότη, αναλυμένο σε υπο-πεδία. Δες ανάλυση στην παρακάτω παράγραφο 8.1.4*
Ισχύει από ***Valid From***	[Ημερομηνία]	*Η ημερομηνία έκδοσης του πιστοποιητικού.*
Ισχύει μέχρι ***Valid To***	[Ημερομηνία]	*Η ημερομηνία λήξης της ισχύος του πιστοποιητικού.*
Θέμα (Υποκείμενο) ***Subject***	(**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. Επιπλέον στο Θέμα αναγράφεται εμφανώς και το είδος του πιστοποιητικού, ήτοι* ***Qualified****.* *Τα χρησιμοποιούμενα υποπεδία και το περιεχόμενό τους αναλύεται στην παρακάτω παράγραφο 8.1.5*
Δημόσιο Κλειδί ***Public Key***	[Δεκαεξαδικός αριθμός 2048 bit]	*Το πιστοποιούμενο 'Δημόσιο Κλειδί' του Συνδρομητή ('θέματος')*
Σημεία Διανομής Λ.Α.Π. ***CRL Distribution Points***	*(Στο υποπεδίο 'Distribution Point Name:/Full Name:=')* [Διεύθυνση τύπου 'URI']	*Η ηλεκτρονική διεύθυνση όπου δημοσιεύεται η πρόσφατη 'Λίστα Ανακληθέντων Πιστοποιητικών' ('Λ.Α.Π.' ή 'CRL') του Π.Υ.Π..*
Πολιτικές Πιστοποιητικού ***Certificate Policies***	"1.3.6.1.4.1.29402.1.2.1.1.1.1" (& στο υποπεδίο 'Qualifier: CPSUri:=') [Διεύθυνση τύπου 'URI']	*Περιέχει τον αριθμό αναγνώρισης (OID) που αντιστοιχεί στην πολιτική αναγνωρισμένου πιστοποιητικού και την ηλεκτρονική διεύθυνση που βρίσκεται ο Κανονισμός Πιστοποίησης Αναγνωρισμένων Πιστοποιητικών (CPS Q.C.) του Εκδότη.*
Χρήσεις Κλειδιού ***Key Usage***	Non - Repudiation	*Προσδιορίζει τις επιτρεπόμενες χρήσεις του ιδιωτικού κλειδιού του συνδρομητή ανάλογα με το είδος του συγκεκριμένου πιστοποιητικού*

QC Statements	id-etsi-qcs-Qccompliance (esi4-qcStatement-1) id-etsi-qcs-QcSSCD (esi4-qcStatement-4) Id-etsi-qcs-QcPDS (esi4-qcStatement-5)	*Ενδειξη ότι το πιστοποιητιό εκδόθηκε βάση του Κανονισμού Νο 910/2014 και αποθηκεύεται σε Α.Δ.Δ.Υ*

(ΣΗΜΕΙΟ 5)

(*) = *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).*

Επίσης, στα πιστοποιητικά Smart-Sign, μπορούν να υπάρχουν (προαιρετικά) και επιπλέον πεδία που παρέχουν περισσότερες πληροφορίες π.χ. κείμενο-δηλώσεις σχετικά με τους ιδιαίτερους όρους χρήσης (π.χ. ανώτατο όριο επιτρεπόμενων συναλλαγών) του πιστοποιητικού ή προσδιοριστικά των χρησιμοποιούμενων κλειδιών.

8.1.3 Τύπος και περιεχόμενο των διακεκριμένων ονομάτων (dn)

Τα διακεκριμένα ονόματα (Distinguished Names –'DN') που περιέχονται στα πεδία του 'Εκδότη' (Issuer) και του 'Θέματος' (Subject) των πιστοποιητικών Smart-Sign™ είναι της μορφής 'ITU-T Recommendation X.501 -Name' που περιλαμβάνει υποπεδία με συγκεκριμένες ιδιότητες. Οι ιδιότητες αυτές (όπως Όνομα, Επίθετο, Χώρα κ.λ.π.) προσδιορίζονται αναλυτικά στο 'ITU-T Recommendation X.520'.

Τα περιεχόμενα των υπο-πεδίων αυτών αναγράφονται με λατινικούς χαρακτήρες, είτε με την πιστή μετάφραση του περιεχομένου τους στα Αγγλικά, είτε με 'μεταγραφή' (transcription) των ελληνικών χαρακτήρων σε λατινικούς σύμφωνα με το πρότυπο [ΕΛΟΤ 743] (βλ. και παράγραφο 4.1.3), για λόγους διεθνούς συμβατότητας.

8.1.4 Διακεκριμένο όνομα (DN) του 'Εκδότη Πιστοποιητικών' (Issuer)

Το διακεκριμένο όνομα (DN) που καταγράφεται στο πεδίο 'Εκδότης' (Issuer) στα πιστοποιητικά Smart-Sign, το οποίο προσδιορίζει τον Εκδότη του πιστοποιητικού, πρέπει να έχει το εξής περιεχόμενο:

Υποπεδίο	Επεξήγηση	Περιεχόμενο
O=	Οργανισμός ***(Organization)***	Ονομασία του υπεύθυνου Εκδότη (Π.Υ.Π.)
OU=	Τμήμα Οργανισμού ***(Organization Unit)***	Ονομασία του σχετικού υπό-Εκδότη *(με μνεία αν προορίζεται για έκδοση αναγνωρισμένων πιστοποιητικών ή όχι)*
[… OU=]	Τμήμα Οργανισμού *[επιπλέον]* ***(Organization Unit)***	Επιπλέον προσδιορισμοί του Εκδότη *[Προαιρετικά]*
CN=	Κοινό Όνομα ***(Common Name)***	Συνδυασμός ονομασίας Εκδότη-ΥποΕκδότη
C=	Χώρα ***(Country)***	Κωδικός χώρας του Εκδότη *(2 γράμματα)*

8.1.5 Διακεκριμένο όνομα (DN) του 'Συνδρομητών' ('Θέμα' ή 'Subject')

Το διακεκριμένο όνομα (DN) που καταγράφεται στο πεδίο 'Συνδρομητής' ('Θέμα' ή 'Subject') στα πιστοποιητικά Smart-Sign™, (βλ. και παραγράφους 4.1.1 - 4.1.3), πρέπει να έχει το εξής περιεχόμενο:

Υποπεδίο	Επεξήγηση	Περιεχόμενο
GN=	Όνομα ***(Given Name)***	Όνομα του Συνδρομητή *(Ολόκληρο ή τα αρχικά του)*
S=	Επίθετο ***(Surname)***	Επίθετο του Συνδρομητή
I=	Αρχικά (Πατρώνυμο)	Πατρώνυμο του Συνδρομητή *(1-3 πρώτα γράμματα)*

	(Initials)	
CN=	Κοινό Όνομα ***(Common Name)***	Συνδυασμός Ονόματος-Πατρώνυμου-Επιθέτου
SN=	Σειριακός Αριθμός ***(Serial Number)***	Προσωπικός Κωδικός Αναγνώρισης του Συνδρομητή *(Μοναδικός κωδικός του Συνδρομητή στον Εκδότη)*
E=	Διεύθυνση ηλεκ. ταχυδρομείου ***(E-Mail)***	Διεύθυνση E-Mail του Συνδρομητή *(σε μορφή RFC 822 Name) - [Προαιρετικά]*
C=	Χώρα ***(Country)***	Κωδικός χώρας ιθαγένειας του Συνδρομητή *(2 γράμματα)*

8.1.6 Πεδία που χαρακτηρίζονται 'Κρίσιμα' (Critical)

Ως **'κρίσιμο πεδίο'** στα πιστοποιητικά Smart-Sign™, το οποίο δηλαδή πρέπει να αναγνωρίζεται και να ερμηνεύεται υποχρεωτικά από οποιαδήποτε εφαρμογή πριν την αποδοχή και την χρήση των περιεχομένων του πιστοποιητικού, ορίζεται **μόνο το πεδίο 'Key Usage'** (χρήσεις κλειδιών) το οποίο, με το κωδικοποιημένο περιεχόμενό του, προσδιορίζει τον τύπο και τις γενικές χρήσεις του πιστοποιητικού.

Ο ορισμός αυτός γίνεται με την τοποθέτηση της τιμής '*True*' στο σχετικό υπο-πεδίο (*Critical Flag*) του πεδίου αυτού.

8.2 ΔΙΑΡΘΡΩΣΗ (PROFILE) ΛΙΣΤΑΣ ΑΝΑΚΛΗΣΗΣ ΠΙΣΤΟΠΟΙΗΤΙΚΩΝ (ΛΑΠ ή CRL)

8.2.1 Τύπος και αριθμός έκδοσης

Οι συμμορφούμενοι με τις παρούσες Πολιτικές Π.Υ.Π. πρέπει να εκδίδουν ΛΑΠ της μορφής 'X.509, CRL Version 2' (Έκδοση 2η) η οποία υποστηρίζει την χρήση εκτεταμένων πεδίων (*extensions*). Ο αριθμός της έκδοσης πρέπει να αναφέρεται στο σχετικό πεδίο του πιστοποιητικού.

8.2.2 Περιεχόμενο και σημασία των πεδίων της ΛΑΠ

Οι 'Λίστες Ανακληθέντων Πιστοποιητικών' (ΛΑΠ) που εκδίδονται από έναν Π.Υ.Π. σχετικά με τα πιστοποιητικά Smart-Sign™ που εξέδωσαν οι Υπο-εκδότες του, πρέπει να περιέχουν υποχρεωτικά τα παρακάτω πεδία:

Όνομα πεδίου	Υποχρεωτικό	Περιεχόμενο	Παρατηρήσεις
Έκδοση ***Version***	ΝΑΙ	"V2"	*Έκδοση '2' του προτύπου 'X.509 - RFC 5280 CRL' που υποστηρίζει εκτεταμένα πεδία.*
Αύξων Αριθμός ΛΑΠ ***CRL Number***	ΝΑΙ	[Ακέραιος αριθμός]	*Μοναδικός αύξων αριθμός που χαρακτηρίζει την συγκεκριμένη ΛΑΠ στα πλαίσια του συγκεκριμένου Υπο-Εκδότη..*
Αλγόριθμος Υπογραφής ***Signature Algorithm***	ΝΑΙ	[Προσδιοριστικό]	*Προσδιορίζει τον αλγόριθμο που χρησιμοποιείται για τον κατακερματισμό (Hash) και την υπογραφή της λίστας.*
Εκδότης ***Issuer***	ΝΑΙ	(Διακεκριμένο Όνομα (DN) τύπου 'X.501' για τον Εκδότη)	*Το όνομα τουΥπο-εκδότη (που υπογράφει την ΛΑΠ), αναλυμένο σε υπο-πεδία. Δες παράγραφο 8.1.4*
Παρούσα Έκδοση ***This Update***	ΝΑΙ	[Ημερομηνία]	*Η ημερομηνία και ώρα έκδοσης της συγκεκριμένης τρέχουσας ΛΑΠ.*
Επόμενη Έκδοση ***Next Update***	ΝΑΙ	[Ημερομηνία]	*Η ημερομηνία και ώρα της επόμενης προγραμματισμένης έκδοσης ΛΑΠ.*
Προσδιοριστικό Κλειδιού Εκδότη ***Authority Key Identifier***	ΟΧΙ	[Ακέραιος αριθμός]	*Προσδιορίζει σε ποιο ζεύγος κλειδιών του Εκδότη αντιστοιχεί η συγκεκριμένη ΛΑΠ (από το οποίο και υπογράφθηκε).*
Ανακληθέντα Πιστοποιητικά ***Revoked Certificates***	ΝΑΙ	[Λίστα Πιστοποιητικών]	*Η ενημερωμένη κύρια λίστα με πληροφορίες για τα –έως την έκδοση της ΛΑΠ- ανακληθέντα πιστοποιητικά. Smart-Sign (Δες επόμενο πίνακα).*

Στο πεδίο ‘Ανακληθέντα Πιστοποιητικά’ (με την κυρίως λίστα των πιστοποιητικών Smart-Sign™ 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 ***User Certificate***	ΝΑΙ	[Ακέραιος αριθμός]	*Ο μοναδικός ‘σειριακός αριθμός’ του πιστοποιητικού Smart-*Sign που *ανακαλείται*
Ημερομηνία Ανάκλησης ***Revocation Date***	ΝΑΙ	[Ημερομηνία]	*Η ημερομηνία και ώρα της έκδοσης της ΛΑΠ με την οποία ανακλήθηκε το συγκεκριμένο πιστοποιητικό.*
Κωδικός Αιτίας ***Reason Code***	ΝΑΙ	(Byte με ενδείξεις για τον λόγο που ανακλήθηκε το πιστοποιητικό αυτό – σύμφωνα με το RFC 5280 ή τα εκάστοτε ισχύοντα πρότυπα)	*Προσδιορίζει τον λόγο ανάκλησης του πιστοποιητικού π.χ. ανάκληση λόγω έκθεσης κλειδιών ή απλή παύση (προσωρινή ανάκληση)*
Ημερομηνία Απώλειας Ισχύος ***Invalidity Date***	Προαιρετικό	[Ημερομηνία]	*Η ημερομηνία και ώρα της αίτησης για την ανάκληση του πιστοποιητικού αυτού.*

8.2.3 Πεδία που χαρακτηρίζονται ‘Κρίσιμα’ (Critical)

Στις ΛΑΠ που εκδίδονται για τα πιστοποιητικά Smart-Sign™ δεν απαιτείται να είναι χαρακτηρισμένο ως ‘critical’ κάποιο πεδίο.

9 ΑΛΛΟΙ ΓΕΝΙΚΟΙ ΟΡΟΙ

9.1 ΔΙΚΑΙΩΜΑΤΑ ΚΑΙ ΠΡΟΣΤΑΣΙΑ

9.1.1 Δικαιώματα πνευματικής ιδιοκτησίας

Το 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.

9.1.2 Εμπορικά σήματα και άλλες ιδιοκτησίες

Το σήμα '**SMART-SIGN™**' αποτελεί κατατεθέν εμπορικό σήμα του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ Α.Ε. και ως τέτοιο απαγορεύεται αυστηρά η χρήση του για σχετικά προϊόντα ή υπηρεσίες από οποιονδήποτε τρίτο.

Δικαίωμα 'επίκλησης συμβατότητας' των παρεχόμενων υπηρεσιών πιστοποίησής τους με τα οριζόμενα στις παρούσες «Πολιτικές Προσωπικών Πιστοποιητικών τύπου 'SMART-SIGN™' έχουν -κατ' εξαίρεση- **μόνο** οι 'Πάροχοι Υπηρεσιών Πιστοποίησης' (Π.Υ.Π.) που έχουν εγκριθεί από την 'Επιτροπή Διαχείρισης Πολιτικής' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ σύμφωνα με την παρ. 10.3.3. και έχουν αποκτήσει **γραπτή άδεια** για αυτό.

9.1.3 Προστασία δεδομένων προσωπικού χαρακτήρα

Η παροχή υπηρεσιών ψηφιακής πιστοποίησης, εκ του αντικειμένου της, σχετίζεται άμεσα με την επεξεργασία και την διάδοση των προσωπικών δεδομένων των υποκειμένων που πιστοποιούνται.

Ως εκ τούτου, η παρούσα πολιτική επιβάλει στους Π.Υ.Π. που εκδίδουν πιστοποιητικά τύπου 'SMART-SIGN™', την τήρηση του ν. 2472/97 '*για την προστασία του ατόμου από την επεξεργασία των δεδομένων προσωπικού χαρακτήρα*', όπως ισχύει και τις εξής πρόσθετες δεσμεύσεις:

α) τη **μη δημοσίευση** στον δημόσιο κατάλογο των πιστοποιητικών, άλλων προσωπικών στοιχείων του συνδρομητή που τυχόν διαθέτει ο Π.Υ.Π., πλην των στοιχείων του συνδρομητή που πιστοποιούνται (βάσει της εγκεκριμένης αίτησης-σύμβασης) και αυτών που αναγράφονται στο πιστοποιητικό.

β) την **παροχή της δυνατότητας** στον συνδρομητή, -τόσο κατά την αίτησή του για την αρχική έκδοση των πιστοποιητικών όσο και σε οποιοδήποτε μεταγενέστερη στιγμή το αποφασίσει, **να ζητήσει τη μη δημοσίευση** του πιστοποιητικού του στον 'δημόσιο κατάλογο ενεργών πιστοποιητικών' που διατηρεί ο Π.Υ.Π.

γ) Η διάδοση των λοιπών προσωπικών δεδομένων των υποκειμένων των πιστοποιητικών SMART-SIGN™ σε τρίτους, να ενεργείται μόνο σε περιπτώσεις '**επίλυσης διαφορών**' που προέρχονται από την χρήση του συγκεκριμένου πιστοποιητικού, εκτός και αν υπάρχει ρητή συγκατάθεση του υποκειμένου για το αντίθετο.

9.1.4 Πολιτική επίλυσης διαφορών και παραπόνων

Ο Πάροχος Υπηρεσιών Πιστοποίησης που εκδίδει πιστοποιητικά τύπου SMART-SIGN™ πρέπει να έχει εξασφαλίσει μια 'διαδικασία επίλυσης διαφορών και παραπόνων' για τους συνδρομητές και τους αποδέκτες των πιστοποιητικών του οι οποίοι επιθυμούν μια εξώδικη λύση ή διευθέτηση διαφορών ή/και παραπόνων τους από αυτόν.

Η διαδικασία πρέπει να ορίζει ένα χρονικό περιθώριο **έως το πολύ ένα (1) μήνα** από την έγγραφη αίτηση του ενδιαφερόμενου μέσα στον οποίο οφείλει να έχει ανταποκριθεί σχετικά η αρμόδια επιτροπή του Π.Υ.Π.. Η επιτροπή αυτή πρέπει να είναι τουλάχιστον τριμελής και να περιλαμβάνει στην σύνθεσή της ένα διοικητικό στέλεχος, έναν τεχνικό ασφαλείας συστημάτων και έναν νομικό σύμβουλο της εταιρίας.

Οι σχετικές υπηρεσίες **πρέπει να παρέχονται χωρίς επιβάρυνση προς τον ενδιαφερόμενο**, τουλάχιστον για την περίπτωση που αυτός δεν προσφύγει σε αίτημα για δικαστική διευθέτηση κατά το

διάστημα αυτό.

9.2 ΤΙΜΟΛΟΓΙΑΚΗ ΠΟΛΙΤΙΚΗ

9.2.1 Δημοσίευση τιμολογιακής πολιτικής

Ο συμμορφούμενος Π.Υ.Π. μπορεί, αν θέλει, να ορίζει και να δημοσιεύει την 'Τιμολογιακή Πολιτική' του για τα πιστοποιητικά τύπου SMART-SIGN™ που παρέχει, **δεσμεύοντας έτσι ως προς το ανώτερο όριο** την τιμολογιακή πολιτική των συνεργαζόμενων με το δίκτυό του 'Τοπικών Υπηρεσιών Υποβολής'. Κατά τα άλλα οι 'Τ.Υ.Υ.' μπορούν να ασκούν ανεξάρτητη τιμολογιακή πολιτική για τις υπηρεσίες του Π.Υ.Π. προς τους συνδρομητές τους.

Η τιμολογιακή πολιτική πρέπει να ορίζει τον τρόπο τιμολόγησης για τα τέλη εγγραφής και τα τέλη έκδοσης και ανανέωσης των πιστοποιητικών SMART-SIGN™ καθώς και για τους προσφερόμενους φορείς 'α.δ.δ.υ.' και τους τυχόν 'αναγνώστες' τους (readers) που παρέχονται προς τους συνδρομητές.

Οι υπηρεσίες κοινόχρηστου Καταλόγου εκδοθέντων πιστοποιητικών Smart-Sign™ και οι υπηρεσίες δημοσίευσης των 'Λιστών Ανακληθέντων Πιστοποιητικών' (CRLs), καθώς και οι λειτουργίες ανάκλησης, αναστολής και ενεργοποίησης των πιστοποιητικών SMART-SIGN™ **πρέπει να προσφέρονται δωρεάν.**

9.2.2 Περιπτώσεις επιστροφής της καταβληθείσας συνδρομής

Τα τέλη εγγραφής και έκδοσης των πιστοποιητικών SMART-SIGN™ που τυχόν καταβλήθηκαν από τον υποψήφιο συνδρομητή κατά την υποβολή της σχετικής αίτησής του, **πρέπει να επιστρέφονται αυτούσια** (από αυτόν που τα παρέλαβε) στον αιτούντα εάν, τελικά, δεν εγκριθεί η αίτησή του από την Υπηρεσία Εγγραφής.

Επίσης, μερική επιστροφή των τελών έκδοσης από τον Π.Υ.Π. προς τον συνδρομητή (όχι όμως και των τελών εγγραφής) πρέπει να προβλέπεται στην περίπτωση ανάκλησης των πιστοποιητικών του συνδρομητή από τον Π.Υ.Π. για λόγους που δεν έχει ευθύνη ο συνδρομητής. Σ' αυτήν την περίπτωση θα πρέπει να επιστρέφεται το ποσό των τελών έκδοσης των πιστοποιητικών που ανακλήθηκαν το οποίο θα αναλογεί στο εναπομείναντα έως την κανονική λήξη των πιστοποιητικών χρόνο.

9.3 ΕΡΜΗΝΕΙΑ ΚΑΙ ΕΚΤΕΛΕΣΤΟΤΗΤΑ

9.3.1 Αυθεντική ερμηνεία των όρων του παρόντος στις συγκριτικές αξιολογήσεις

Στις περιπτώσεις 'συγκριτικής αξιολόγησης' των παρόντων πολιτικών (*με Κανονισμούς Πιστοποίησης για την διαπίστωση συμμόρφωσή τους ή με άλλες Πολιτικές Πιστοποιητικών για την διαπίστωση της τυχόν ισοδυναμίας τους ή συμβατότητάς τους που γίνονται σύμφωνα με τις παρ. 10.3.1 και 10.3.2 της παρούσας πολιτικής*) με σκοπό τις εμπορικές συνεργασίες στην 'αγορά παροχής υπηρεσιών δημοσίας πιστοποίησης', η «Επιτροπή Διαχείρισης Πολιτικών» του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ **είναι η μόνη αρμόδια** για να ερμηνεύσει 'αυθεντικά' τους όρους της παρούσας πολιτικής και να προβεί έτσι ή όχι στις σχετικές διαπιστώσεις που αφορούν την παρούσα πολιτική σε σχέση της με άλλα κείμενα.

9.3.2 Εκτελεστότητα - Διατηρησιμότητα των μη άκυρων όρων

Η παρούσα πολιτική, ισχύουσα για τα '**αναγνωρισμένα προσωπικά πιστοποιητικά**' τύπου **SMART-SIGN™ –Κλάσης 2ης**, δεσμεύει τα μέρη της κοινότητας των πιστοποιητικών SMART-SIGN™ (Π.Υ.Π. και συνεργαζόμενους στην παροχή των υπηρεσιών του τρίτους, συνδρομητές και αποδέκτες) τα οποία και την ενσωματώνουν στις μεταξύ τους συμβάσεις, με μόνη την αναφορά στο σύνολό της**.**

Σε περίπτωση ασυμφωνίας της παρούσας με κάποιον όρο των παραπάνω συμβάσεων, **υπερισχύει η παρούσα πολιτική**.

Η **μη εφαρμοσιμότητα** ή η **ακυρότητα** οποιασδήποτε διάταξης ή παραγράφου του παρόντος κειμένου δεν καθιστά ανεφάρμοστο το σύνολο ή άλλο τμήμα της πολιτικής αυτής των προσωπικών πιστοποιητικών SMART-SIGN™ –Κλάσης 2ης, και η παρούσα πολιτική θεωρείται ως τροποποιημένη με την διαγραφή ή μεταβολή της διάταξης αυτής ώστε να καταστεί **έγκυρη και εφαρμόσιμη και**, στο βαθμό που είναι δυνατό, **σύμφωνη με τον αρχικό σκοπό της**.

9.3.3 Εφαρμοστέο δίκαιο και αρμόδια δικαστήρια

Η παρούσα πολιτική **διέπεται από το Ελληνικό Δίκαιο** και για κάθε αγωγή, αμφισβήτηση ή διαφορά σε σχέση με αυτήν **αρμόδια θα είναι τα δικαστήρια της πόλης των Αθηνών**, στην συντρέχουσα δωσιδικία των οποίων υποβάλλονται με την παρούσα τα συμβαλλόμενα μέρη τα οποία ενσωματώνουν 'με αναφορά' το σύνολο της παρούσας πολιτικής στην μεταξύ τους σύμβαση.

10 ΔΙΑΧΕΙΡΙΣΗ ΚΑΙ ΑΝΑΘΕΩΡΗΣΗ ΤΗΣ ΠΟΛΙΤΙΚΗΣ

10.1 ΥΠΕΥΘΥΝΟΣ ΕΚΔΟΣΗΣ ΚΑΙ ΔΙΑΧΕΙΡΙΣΗΣ

10.1.1 Ονομασία – Αρμοδιότητες –Υποχρεώσεις

Υπεύθυνος για την έκδοση και την διαχείριση της παρούσας πολιτικής προσωπικών πιστοποιητικών SMART-SIGN™ είναι η «**Επιτροπή Διαχείρισης Πολιτικών**» του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΏΝ Α.Ε..

Η επιτροπή αυτή αποτελεί το **ανώτερο όργανο** των 'Υπηρεσιών Ψηφιακής Πιστοποίησης' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΏΝ σε θέματα διαμόρφωσης πολιτικών και επιπέδων ασφαλείας για τα εκδιδόμενα πιστοποιητικά καθώς και στην διαμόρφωση στρατηγικής για την εναρμόνιση των υπηρεσιών πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΏΝ με τις απαιτούμενες νομικές και τεχνικές προδιαγραφές και τις διαμορφούμενες τάσεις της αγοράς. Η **συγκρότησή** της γίνεται με ευθύνη των 'Υπηρεσιών Ψηφιακής Πιστοποίησης' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΏΝ και στην **σύνθεσή** της περιλαμβάνει ανώτερα διοικητικά στελέχη, τεχνικούς και υπεύθυνους ασφαλείας καθώς και νομικούς συμβούλους του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΏΝ .

Αρμοδιότητες της «Επιτροπής Διαχείρισης Πολιτικών» είναι **η έκδοση, η δημοσίευση και η αναθεώρηση** των Πολιτικών των Πιστοποιητικών (Certificate Policies) που εκδίδουν οι 'Υπηρεσίες Ψηφιακής Πιστοποίησης' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΏΝ και **η έγκριση** του 'Κανονισμού Πιστοποίησης' (Certification Practice Statement) της, ως συμμορφούμενου με τις απαιτήσεις και τις προδιαγραφές που ορίζουν οι Πολιτικές της.

Επίσης, η επιτροπή αυτή, είναι η μόνη αρμόδια για την νομικοτεχνική επεξεργασία και την **έγκριση (***μετά από 'συγκριτική αξιολόγηση' σε σχέση με τις Πολιτικές που αυτή εκδίδει –βλ. υποκεφάλαιο 10.3*) άλλων 'Πολιτικών Πιστοποιητικών' και 'Κανονισμών Πιστοποίησης' στις περιπτώσεις συνεργασίας των 'Υπηρεσιών Ψηφιακής Πιστοποίησης' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΏΝ **με άλλους παρόχους υπηρεσιών πιστοποίησης ή αρχές έκδοσης πολιτικών**. (π.χ. 'αλληλο-πιστοποίηση' *(cross-certifying),* 'υιοθέτηση' ή 'κήρυξη ισοδυναμίας πολιτικών' *(policy-mapping)*).

Η επιτροπή 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)

10.1.2 Στοιχεία Επικοινωνίας

Η «Επιτροπή Διαχείρισης Πολιτικών» στεγάζεται στην έδρα του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΏΝ Α.Ε. και οποιεσδήποτε ερωτήσεις, παρατηρήσεις ή σχόλια προς την επιτροπή πρέπει να απευθύνονται προς:

ΕΛΛΗΝΙΚΑ ΧΡΗΜΑΤΙΣΤΗΡΙΑ- ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΏΝ ΑΝΩΝΥΜΗ ΕΤΑΙΡΕΙΑ ΣΥΜΜΕΤΟΧΩΝ

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/el/web/guest/digital-certificates

10.2 ΑΝΑΘΕΩΡΗΣΗ ΤΩΝ ΠΟΛΙΤΙΚΩΝ

10.2.1 Υποβολή, έγκριση και δημοσίευση των αναθεωρημένων εκδόσεων

Η 'Επιτροπή Διαχείρισης Πολιτικών' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ αποφαίνεται για την ανάγκη αναθεώρησης ή όχι των παρόντων πολιτικών των πιστοποιητικών SMART-SIGN™ **είτε** με δική της πρωτοβουλία μετά από τυχόν τροποποιήσεις της ισχύουσας νομοθεσίας ή των τεχνικών προτύπων για τις ηλεκτρονικές υπογραφές **είτε** κατόπιν ερωτήματος ή σχετικού αιτήματος από τις Υπηρεσίες Ψηφιακής Πιστοποίησης του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ και των τυχόν συνεργατών της που υπόκεινται στις παρούσες πολιτικές.

Οι αναγκαίες αναθεωρήσεις των παρόντων πολιτικών συντάσσονται από μέλη της Επιτροπής και συντελούνται **μόνο με την έγκριση** του νέου κειμένου από την ολομέλεια της Επιτροπής **και τη δημοσίευση** του στην σχετική ηλεκτρονική σελίδα των 'Υπηρεσιών Ψηφιακής Πιστοποίησης' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ (http://www.athexgroup.gr/el/web/guest/digital-certificates-pki-regulations) **σαράντε πέντε (45) τουλάχιστον ημέρες πριν την θέση τους σε ισχύ**.

Κάθε εγκεκριμένη αναθεώρηση πρέπει να περιλαμβάνει 'εισαγωγικό κεφάλαιο' με περίληψη των τροποποιήσεων που έχουν υποστεί οι πολιτικές από την αρχική τους έκδοση, ενώ οι προηγούμενες εκδόσεις **πρέπει να συνεχίσουν να δημοσιεύονται** -ως τέτοιες- στην ίδια ηλεκτρονική διεύθυνση.

10.2.2 Κρισιμότητα των αναθεωρήσεων και σχετική αριθμοδότηση

Ως '**κρίσιμες**' θεωρούνται οι αναθεωρήσεις της παρούσας πολιτικής οι οποίες αλλοιώνουν ή επηρεάζουν ουσιαστικά τις σχέσεις (δικαιώματα και υποχρεώσεις) μεταξύ των μερών της κοινότητας των πιστοποιητικών SMART-SIGN™ ή που τροποποιούν βασικές ιδιότητες και χαρακτηριστικά ή το επίπεδο της προσφερόμενης ασφάλειας των πιστοποιητικών αυτών.

Δεν θεωρούνται ως 'κρίσιμες' οι αναθεωρήσεις οι οποίες έχουν ως αποτέλεσμα να:

- Προσθέτουν την περιγραφή και άλλων κλάσεων προσωπικών πιστοποιητικών SMART-SIGN™ στο ενιαίο κείμενο χωρίς να αλλοιώνουν τους όρους και τις προϋποθέσεις των προηγούμενων.
- Προβλέπουν κάποιες πρόσθετες εναλλακτικές ιδιότητες ή χαρακτηριστικά στις προσφερόμενες υπηρεσίες του συμμορφούμενου Π.Υ.Π., χωρίς να μειώνουν τα υπάρχοντα δικαιώματα του αποδέκτη τους,
- Διευκρινίζουν καλύτερα κάποιες από τις αναφερόμενες -στην προηγούμενη έκδοση της πολιτικής- διαδικασίες, χωρίς να αλλοιώνουν την ουσία στις τυχόν σχέσεις που εξυπηρετεί η διαδικασία αυτή.

Κάθε **'κρίσιμη' αναθεώρηση** εκφράζεται με την μεταβολή (αύξηση) του πρώτου ψηφίου του αποδιδόμενου 'αριθμού έκδοσης' στην προκύπτουσα νέα πολιτική, ενώ οι **'μη κρίσιμες' αναθεωρήσεις** μεταβάλλουν (αυξάνοντας) το δεύτερο ψηφίο του 'αριθμού έκδοσής' της, σε σχέση πάντα με τον αριθμό έκδοσης της προηγούμενης ισχύουσας πολιτικής.

Οι νέες εκδόσεις των πολιτικών που προκύπτουν από την διαδικασία αναθεώρησής τους λαμβάνουν αντίστοιχα **νέο μοναδικό αριθμό OID** από το ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ, ο οποίος διαμορφώνεται ανάλογα με την **σύνθεση** των ισχύοντων αριθμών OIDs (που αναλύονται στην παρ. 1.2.3), την **κλάση** και τον νέο '**αριθμό έκδοσης**' των προκυπτουσών πολιτικών.

10.2.3 Αναδρομικότητα ισχύος της αναθεωρημένης έκδοσης

Όλες οι αναθεωρήσεις των παρόντων πολιτικών **ισχύουν** ως προς την εφαρμογή τους **μόνο μετά από δέκα (10) ημέρες από την ημερομηνία της δημοσίευσής τους** (σύμφωνα με την παρ. 10.2.1) και διέπουν όλα τα νέα πιστοποιητικά που εκδίδονται μετά από αυτήν την ημερομηνία και τα οποία **πρέπει να αναγράφουν τον καινούργιο αριθμό OID** της πολιτικής που τους αντιστοιχεί.

Οι εκδότες, οι κάτοχοι-συνδρομητές και τα βασιζόμενα μέρη πιστοποιητικών SMART-SIGN™ που έχουν εκδοθεί με ισχύουσα προηγούμενη της αναθεώρησης έκδοση της παρούσας πολιτικής (δηλαδή στα πιστοποιητικά στα οποία αναγράφεται ο OID προηγούμενης από την ισχύουσα πολιτική) εξακολουθούν να διέπονται από τους όρους εκείνης της πολιτικής, **με εξαίρεση** τις τυχόν 'μη κρίσιμες' αναθεωρήσεις εκείνης της πολιτικής που στο μεταξύ δημοσιεύτηκαν και τέθηκαν σε ισχύ, **οι οποίες**, κατά ρητή πρόβλεψη της

παρούσας πολιτικής, **θα αντικαθιστούν τις προηγούμενες και θα διέπουν στο εξής τις σχέσεις όλων των εμπλεκόμενων μερών**.

Οι εγκρίσεις Κανονισμών Πιστοποίησης και οι σχετικές άδειες για επίκληση συμβατότητας ή ισοδυναμίας άλλων Πολιτικών με την παρούσα πολιτική των προσωπικών πιστοποιητικών SMART-SIGN™ που έχουν δοθεί από την 'Επιτροπή Διαχείρισης Πολιτικών' (σύμφωνα με το παρακάτω υποκεφάλαιο) **θα παραμένουν ισχυρές και θα καλύπτουν και τις νέες εκδόσεις** της παρούσας πολιτικής στις περιπτώσεις των **'μη κρίσιμων' αναθεωρήσεων** αυτής (δηλαδή στις εκδόσεις της στις οποίες δεν έχει αλλάξει το πρώτο ψηφίο του 'αριθμού έκδοσης', σύμφωνα με τα παραπάνω). Για την συγκριτική αξιολόγηση των παραπάνω κειμένων με νέες πολιτικές των πιστοποιητικών SMART-SIGN™ **που έχουν προκύψει από 'κρίσιμη' αναθεώρηση** απαιτείται **νέα έγκριση** από την Επιτροπή, με επανάληψη των παρακάτω διαδικασιών.

10.3 ΣΥΓΚΡΙΤΙΚΕΣ ΑΞΙΟΛΟΓΗΣΕΙΣ ΣΧΕΤΙΚΑ ΜΕ ΤΙΣ ΠΑΡΟΥΣΕΣ ΠΟΛΙΤΙΚΕΣ

10.3.1 Απόδοση ισοδυναμίας με άλλες πολιτικές πιστοποιητικών (policy mapping)

Στις περιπτώσεις που απαιτείται 'δια-λειτουργικότητα' (interoperability) στις εφαρμογές των προσωπικών πιστοποιητικών SMART-SIGN™ με την μονόδρομη ή αμφιμερή 'απόδοση ισοδυναμίας' (policy mapping) των παρόντων πολιτικών με άλλες πολιτικές προσωπικών πιστοποιητικών (εκδιδομένες από άλλον Π.Υ.Π. ή σχετική 'Αρχή') θα πρέπει οι συγκρινόμενες με την παρούσα πολιτική άλλες πολιτικές να αξιολογηθούν σχετικά από την αρμόδια 'Επιτροπή της Διαχείρισης Πολιτικής' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

Ειδικότερα για την περίπτωση **αμφίδρομης** και αμοιβαίας 'απόδοσης ισοδυναμίας' πολιτικών ή στην **μονόδρομη** 'απόδοση ισοδυναμίας' όπου αποδέκτης του τίτλου 'συμβατότητας ή ισοδυναμίας' είναι η παρούσα πολιτική, η παραπάνω επιτροπή του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ -ως διαχειριστής της παρούσας πολιτικής-, μετά από τον κατάλληλο νομοτεχνικό έλεγχο του συγκρινόμενου μοντέλου με την παρούσα πολιτική **αποφαίνεται δεσμευτικά** για τις 'Υπηρεσίες Ψηφιακής Πιστοποίησης' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ και τους τυχόν άλλους συμμορφούμενους με την παρούσα πολιτική Π.Υ.Π. (οι οποίοι έχουν λάβει την έγκρισή της και χρησιμοποιούν τις παρούσα πολιτική) για την υπάρχουσα ή όχι συμβατότητα και τις τυχόν απαιτούμενες αναθεωρήσεις των κειμένων που επιβάλλεται να γίνουν ώστε να επιτευχθεί η συμβατότητα αυτή.

Στην περίπτωση **μονόδρομης** απόδοσης ισοδυναμίας όπου αποδέκτης του τίτλου 'συμβατότητας ή ισοδυναμίας' είναι άλλη πολιτική που έχει εκδοθεί από άλλον Π.Υ.Π. ή σχετική 'Αρχή' και οι οποίοι τυχόν αιτούνται αυτόν τον 'τίτλο' από την Επιτροπή, η τελευταία μπορεί να αξιολογήσει και να εγκρίνει ή να προτείνει τις τυχόν απαιτούμενες τροποποιήσεις στο κείμενο της συγκρινόμενης πολιτικής μόνο μετά την καταβολή από τους αιτούντες των ειδικών τελών για την παραχώρηση του **δικαιώματος 'επίκλησης της ισοδυναμίας'** που ορίζουν οι 'Υπηρεσίες Ψηφιακής Πιστοποίησης' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ.

10.3.2 Έγκριση Κανονισμών Πιστοποίησης ως σύμφωνων με τις παρούσες πολιτικές

Στην περίπτωση που κάποιος άλλος Π.Υ.Π., εκτός των 'Υπηρεσιών Ψηφιακής Πιστοποίησης' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ, επιθυμεί να υιοθετήσει αυτούσιους τους όρους που περιλαμβάνονται στις παρούσες «Πολιτικές Προσωπικών Πιστοποιητικών τύπου 'SMART-SIGN™' *(διπλού κλειδιού)* του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ –Κλάσης $2^{ης}$» ώστε να εκδίδει προς τους συνδρομητές του προσωπικά πιστοποιητικά που θα φέρουν τον τίτλο «Προσωπικά πιστοποιητικά SMART-SIGN™ –Κλάσης $2^{ης}$» ο οποίος περιλαμβάνει και το εμπορικό σήμα του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ 'SMART-SIGN™' θα πρέπει:

α) να καταβάλει στο ΧΡΗΜΑΤΙΣΤΗΡΙΟ ΑΘΗΝΩΝ τα συμφωνηθέντα με αυτήν **τέλη για την συνεκμετάλλευση των εμπορικών σημάτων της**, και,

β) να λάβει **γραπτή έγκριση** από την 'Επιτροπή Διαχείρισης Πολιτικών' του ΧΡΗΜΑΤΙΣΤΗΡΙΟΥ ΑΘΗΝΩΝ για την συμμόρφωση του Κανονισμού Πιστοποιήσεών του με την παρούσα πολιτική **καταβάλλοντας και τα τυχόν τέλη αξιολόγησης** που έχει προσδιορίσει για την διαδικασία αξιολόγησης και έκδοσης της τελικής έγκρισης η Επιτροπή.

Για να λάβει ένας Π.Υ.Π. την παραπάνω γραπτή έγκριση συμμόρφωσης με την παρούσα πολιτική προσωπικών πιστοποιητικών SMART-SIGN™, **πρέπει να υποβάλει** -σε γραπτή και σε ηλεκτρονική μορφή- στην Επιτροπή τον υπάρχοντα Κανονισμό Πιστοποιήσεών της **προς αξιολόγησή του από αυτήν**, αποδεχόμενος

εκ των προτέρων τις τυχόν απαραίτητες τροποποιήσεις που τυχόν αυτός θα πρέπει να υποστεί **κατά τις υποδείξεις και την αποκλειστική κρίση της Επιτροπής**, ώστε να καταστεί συμβατός με τις παρούσα πολιτική.