Το έγγραφο αυτό συνιστά βοήθημα τεκμηρίωσης και δεν δεσμεύει τα κοινοτικά όργανα

►**B** ►**C1** **ΑΠΟΦΑΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ**

της 16ης Οκτωβρίου 2009

σχετικά τη θέσπιση μέτρων που διευκολύνουν τη χρήση διαδικασιών με ηλεκτρονικά μέσα μέσω των «ενιαίων κέντρων εξυπηρέτησης» βάσει της οδηγίας 2006/123/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τις υπηρεσίες στην εσωτερική αγορά

[κοινοποιηθείσα υπό τον αριθμό Ε(2009) 7806]

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

(2009/767/ΕΚ) ◄

(ΕΕ L 274 της 20.10.2009, σ. 36)

Τροποποιείται από:

		Επίσημη Εφημερίδα		
		αριθ.	σελίδα	ημερομηνία
►**M1**	Απόφαση 2010/425/ΕΕ της Επιτροπής της 28ης Ιουλίου 2010	L 199	30	31.7.2010

Διορθώνεται από:

►**C1** Διορθωτικό ΕΕ L 299 της 14.11.2009, σ. 18 (2009/767/ΕΚ)
►**C2** Διορθωτικό ΕΕ L 4 της 7.1.2011, σ. 6 (2009/767/ΕΚ)

▼B
▼C1

ΑΠΟΦΑΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 16ης Οκτωβρίου 2009

σχετικά τη θέσπιση μέτρων που διευκολύνουν τη χρήση διαδικασιών με ηλεκτρονικά μέσα μέσω των «ενιαίων κέντρων εξυπηρέτησης» βάσει της οδηγίας 2006/123/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου σχετικά με τις υπηρεσίες στην εσωτερική αγορά

[κοινοποιηθείσα υπό τον αριθμό Ε(2009) 7806]

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

(2009/767/ΕΚ)

Η ΕΠΙΤΡΟΠΗ ΤΩΝ ΕΥΡΩΠΑΪΚΩΝ ΚΟΙΝΟΤΗΤΩΝ,

Έχοντας υπόψη:

τη συνθήκη για την ίδρυση της Ευρωπαϊκής Κοινότητας,

την οδηγία 2006/123/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Δεκεμβρίου 2006, σχετικά με τις υπηρεσίες στην εσωτερική αγορά [1], και ιδίως το άρθρο 8 παράγραφος 3,

Εκτιμώντας τα ακόλουθα:

(1) Οι υποχρεώσεις διοικητικής απλούστευσης που επιβάλλονται στα κράτη μέλη δυνάμει του κεφαλαίου ΙΙ της οδηγίας 2006/123/ΕΚ, ιδίως δυνάμει των άρθρων 5 και 8 της εν λόγω οδηγίας, συμπεριλαμβάνουν την υποχρέωση απλούστευσης των διαδικασιών και των διατυπώσεων που ισχύουν για την πρόσβαση σε δραστηριότητες παροχής υπηρεσιών και για την άσκησή τους, καθώς και την υποχρέωση διασφάλισης ότι οι πάροχοι υπηρεσιών μπορούν εύκολα να πραγματοποιούν τις εν λόγω διαδικασίες και διατυπώσεις από απόσταση και με ηλεκτρονικά μέσα, μέσω των «ενιαίων κέντρων εξυπηρέτησης».

(2) Η διεκπεραίωση των διαδικασιών και των διατυπώσεων μέσω των «ενιαίων κέντρων εξυπηρέτησης» πρέπει να είναι εφικτή μεταξύ των κρατών μελών, όπως ορίζει το άρθρο 8 της οδηγίας 2006/123/ΕΚ.

(3) Προκειμένου να υπάρξει συμμόρφωση με την υποχρέωση απλούστευσης των διαδικασιών και των διατυπώσεων, καθώς και για τη διευκόλυνση της διασυνοριακής χρήσης των «ενιαίων κέντρων εξυπηρέτησης», οι διαδικασίες με ηλεκτρονικά μέσα πρέπει να βασίζονται σε απλές λύσεις, μεταξύ των οποίων η χρήση των ηλεκτρονικών υπογραφών. Σε περιπτώσεις κατά τις οποίες, μετά από κατάλληλη εκτίμηση επικινδυνότητας συγκεκριμένων διαδικασιών και διατυπώσεων, θεωρείται απαραίτητο ένα υψηλό επίπεδο ασφαλείας ή ισοδυναμία με τη χειρόγραφη υπογραφή, οι πάροχοι υπηρεσιών, για ορισμένες διαδικασίες και διατυπώσεις, θα απαιτείται να διαθέτουν προηγμένες ηλεκτρονικές υπογραφές βάσει αναγνωρισμένου πιστοποιητικού, με ή χωρίς ασφαλή διάταξη δημιουργίας υπογραφών.

[1] ΕΕ L 376 της 27.12.2006, σ. 36.

▼C1

(4) Το κοινοτικό πλαίσιο για τις ηλεκτρονικές υπογραφές θεσπίστηκε με την οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές ([1]). Προκειμένου να διευκολυνθεί η αποτελεσματική διασυνοριακή χρήση των προηγμένων ηλεκτρονικών υπογραφών βάσει αναγνωρισμένου πιστοποιητικού, πρέπει να αυξηθεί η εμπιστοσύνη στις εν λόγω ηλεκτρονικές υπογραφές, ανεξάρτητα από το κράτος μέλος όπου είναι εγκατεστημένος ο υπογράφων ή ο πάροχος της υπηρεσίας πιστοποίησης που εκδίδει το αναγνωρισμένο πιστοποιητικό. Αυτό επιτυγχάνεται καθιστώντας τις πληροφορίες που απαιτούνται για την επικύρωση των ηλεκτρονικών υπογραφών ευκολότερα διαθέσιμες σε αξιόπιστη μορφή, ιδίως τις πληροφορίες που αφορούν τους παρόχους υπηρεσιών πιστοποίησης, οι οποίοι εποπτεύονται/διαπιστεύονται σε ένα κράτος μέλος, καθώς και τις υπηρεσίες που παρέχουν.

(5) Είναι αναγκαίο να διασφαλιστεί ότι το κράτος μέλος θέτει τις πληροφορίες αυτές στη διάθεση του κοινού μέσω ενός κοινού προτύπου, προκειμένου να διευκολύνει τη χρήση τους και να διασφαλίσει ένα κατάλληλο επίπεδο λεπτομερειών, που θα επιτρέπει σε εκείνον που τις λαμβάνει να επικυρώνει την ηλεκτρονική υπογραφή,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

Άρθρο 1

Χρήση και αποδοχή ηλεκτρονικών υπογραφών

1. Αν αιτιολογείται βάσει κατάλληλης εκτίμησης επικινδυνότητας και σύμφωνα με το άρθρο 5 παράγραφοι 1 και 3 της οδηγίας 2006/123/ΕΚ, τα κράτη μέλη μπορούν να απαιτούν, για τη διεκπεραίωση ορισμένων διαδικασιών και διατυπώσεων μέσω των ενιαίων κέντρων εξυπηρέτησης, δυνάμει του άρθρου 8 της οδηγίας 2006/123/ΕΚ, να χρησιμοποιεί ο πάροχος της υπηρεσίας προηγμένες ηλεκτρονικές υπογραφές βάσει αναγνωρισμένου πιστοποιητικού, με ή χωρίς ασφαλή διάταξη δημιουργίας υπογραφών, όπως ορίζεται και προβλέπεται στην οδηγία 1999/93/ΕΚ.

2. Τα κράτη μέλη υποχρεούνται να αποδέχονται οποιεσδήποτε προηγμένες ηλεκτρονικές υπογραφές βάσει αναγνωρισμένου πιστοποιητικού, με ή χωρίς ασφαλή διάταξη δημιουργίας υπογραφών, για τη διεκπεραίωση των διαδικασιών και των διατυπώσεων που αναφέρονται στην παράγραφο 1, υπό την επιφύλαξη της δυνατότητας των κρατών μελών να περιορίζουν αυτή την αποδοχή σε προηγμένες ηλεκτρονικές υπογραφές βάσει αναγνωρισμένου πιστοποιητικού, που δημιουργήθηκαν μέσω ασφαλούς διάταξης δημιουργίας υπογραφών, αν αυτό συμφωνεί με την εκτίμηση επικινδυνότητας που αναφέρεται στην παράγραφο 1.

3. Τα κράτη μέλη δεν εξαρτούν την αποδοχή προηγμένων ηλεκτρονικών υπογραφών βάσει αναγνωρισμένου πιστοποιητικού, με ή χωρίς ασφαλή διάταξη δημιουργίας υπογραφών, από απαιτήσεις που θέτουν εμπόδια στους παρόχους υπηρεσιών όσον αφορά τη χρήση διαδικασιών με ηλεκτρονικά μέσα μέσω των ενιαίων κέντρων εξυπηρέτησης.

([1]) ΕΕ L 13 της 19.1.2000, σ. 12.

▼C1

4. Η παράγραφος 2 δεν εμποδίζει τα κράτη μέλη να αποδέχονται άλλες ηλεκτρονικές υπογραφές εκτός από τις προηγμένες ηλεκτρονικές υπογραφές βάσει αναγνωρισμένου πιστοποιητικού, με ή χωρίς τη χρήση ασφαλούς διάταξης δημιουργίας υπογραφών.

Άρθρο 2

Κατάρτιση, τήρηση και δημοσίευση καταλόγων εμπίστευσης

1. Κάθε κράτος μέλος καταρτίζει, τηρεί και δημοσιεύει, σύμφωνα με τις τεχνικές προδιαγραφές που ορίζονται στο παράρτημα, «κατάλογο εμπίστευσης», ο οποίος περιέχει τις ελάχιστες πληροφορίες που αφορούν τους παρόχους υπηρεσιών πιστοποίησης, οι οποίοι εκδίδουν αναγνωρισμένα πιστοποιητικά για το κοινό, και οι οποίοι εποπτεύονται/διαπιστεύονται από το εκάστοτε κράτος μέλος.

▼M1

2. Τα κράτη μέλη καταρτίζουν και δημοσιεύσουν τόσο μια αναγνώσιμη από άνθρωπο όσο και μια μηχανικά επεξεργάσιμη μορφή του καταλόγου εμπίστευσης, σύμφωνα με τις προδιαγραφές που ορίζονται στο παράρτημα.

2α. Τα κράτη μέλη υπογράφουν ηλεκτρονικά τη μηχανικά επεξεργάσιμη μορφή των καταλόγων εμπίστευσής τους και δημοσιεύουν, ως ελάχιστη προϋπόθεση, μια αναγνώσιμη από άνθρωπο μορφή του καταλόγου εμπίστευσης μέσω ασφαλούς διόδου προκειμένου να διασφαλίζεται η αυθεντικότητα και η ακεραιότητά του.

3. Τα κράτη μέλη κοινοποιούν στην Επιτροπή τις ακόλουθες πληροφορίες:

α) τον αρμόδιο φορέα ή τους αρμόδιους φορείς για την κατάρτιση, την τήρηση και τη δημοσίευση της αναγνώσιμης από άνθρωπο μορφής ή της μηχανικά επεξεργάσιμης μορφής καταλόγου εμπίστευσης·

β) τους τόπους δημοσίευσης της αναγνώσιμης από άνθρωπο μορφής ή της μηχανικά επεξεργάσιμης μορφής καταλόγου εμπίστευσης·

γ) το πιστοποιητικό δημόσιου κλειδιού που χρησιμοποιείται για την εφαρμογή του ασφαλούς διαύλου μέσω του οποίου δημοσιεύεται η αναγνώσιμη από άνθρωπο μορφή του καταλόγου εμπίστευσης ή, αν ο αναγνώσιμος από άνθρωπο κατάλογος είναι ηλεκτρονικά υπογεγραμμένος, το πιστοποιητικό δημοσίου κλειδιού που χρησιμοποιείται για την υπογραφή του·

δ) το πιστοποιητικό δημόσιου κλειδιού που χρησιμοποιείται για την ηλεκτρονική υπογραφή της μηχανικά επεξεργάσιμης μορφής του καταλόγου εμπίστευσης·

ε) τυχόν αλλαγές σχετικά με τις πληροφορίες που αναφέρονται στα στοιχεία α) έως δ).

4. Η Επιτροπή θέτει στη διάθεση όλων των κρατών μελών, μέσω ασφαλούς διαύλου σε έναν επικυρωμένο εξυπηρετητή διαδικτύου, τις πληροφορίες που αναφέρονται στην παράγραφο 3, όπως κοινοποιήθηκαν από τα κράτη μέλη, τόσο σε αναγνώσιμη από άνθρωπο μορφή όσο και σε μηχανικά επεξεργάσιμη υπογεγραμμένη μορφή.

▼C1

Άρθρο 3

Έναρξη ισχύος

Η παρούσα απόφαση εφαρμόζεται από τις 28 Δεκεμβρίου 2009.

Άρθρο 4

Αποδέκτες

Η απόφαση απευθύνεται στα κράτη μέλη.

▼C1

ΠΑΡΑΡΤΗΜΑ

ΤΕΧΝΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΝΟΣ ΚΟΙΝΟΥ ΣΧΕΔΙΟΤΥΠΟΥ ΓΙΑ ΤΟΝ «ΚΑΤΑΛΟΓΟ ΕΜΠΙΣΤΕΥΣΗΣ ΕΠΟΠΤΕΥΟΜΕΝΩΝ/ΔΙΑΠΙΣΤΕΥΜΕΝΩΝ ΠΑΡΟΧΩΝ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ»

ΕΙΣΑΓΩΓΗ

1. **Γενικές παρατηρήσεις**

Σκοπός του κοινού σχεδιοτύπου «Κατάλογος εμπίστευσης εποπτευόμενων/-διαπιστευμένων παρόχων υπηρεσιών πιστοποίησης» των κρατών μελών είναι η θέσπιση ενός ενιαίου τρόπου για την παροχή πληροφοριών από έκαστο κράτος μέλος όσον αφορά την κατάσταση εποπτείας/διαπίστευσης των υπηρεσιών πιστοποίησης από τους παρόχους υπηρεσιών πιστοποίησης ([1]) (Certification Service Providers — CSP), οι οποίοι εποπτεύονται/διαπιστεύονται από τα κράτη μέλη, με στόχο τη συμμόρφωση με τις σχετικές διατάξεις της οδηγίας 1999/93/ΕΚ. Σε αυτόν συμπεριλαμβάνεται η παροχή πληροφοριών για το ιστορικό της κατάστασης εποπτείας/διαπίστευσης των εποπτευόμενων/διαπιστευμένων υπηρεσιών πιστοποίησης.

Στις υποχρεωτικές πληροφορίες του καταλόγου εμπίστευσης (Trusted List-TL) πρέπει να συμπεριλαμβάνονται κάποιες ελάχιστες πληροφορίες για τους εποπτευόμενους/διαπιστευμένους CSP που εκδίδουν αναγνωρισμένα πιστοποιητικά (Qualified Certificate-QC) ([2]) σύμφωνα με τις διατάξεις που ορίζονται στην οδηγία 1999/93/ΕΚ [άρθρο 3 παράγραφοι 3 και 2, και άρθρο 7 παράγραφος 1 στοιχείο α), συμπεριλαμβανομένων πληροφοριών σχετικά με τα QC που υποστηρίζουν μια ηλεκτρονική υπογραφή και σχετικά με το αν η υπογραφή δημιουργείται ή όχι μέσω μιας ασφαλούς διάταξης δημιουργίας υπογραφής (Secure Signature Creation Device – SSCD] ([3]).

Ο κατάλογος εμπίστευσης μπορεί να συμπεριλαμβάνει εθελοντικά και σε εθνική βάση επιπλέον πληροφορίες σχετικά με άλλους εποπτευόμενους/διαπιστευμένους CSP που δεν εκδίδουν QC, αλλά που παρέχουν υπηρεσίες σχετικά με τις ηλεκτρονικές υπογραφές (π.χ. CSP που παρέχουν υπηρεσίες χρονοσφράγισης και που εκδίδουν αδειοδοτικά χρονοσφράγισης, CSP που εκδίδουν μη αναγνωρισμένα πιστοποιητικά κ.λπ.).

Αυτές οι πληροφορίες αποσκοπούν κυρίως στην υποστήριξη της επικύρωσης των αναγνωρισμένων ηλεκτρονικών υπογραφών (Qualified Electronic Signature - QES) και των προηγμένων ηλεκτρονικών υπογραφών (Advanced Electronic Signature - AdES) ([4]) τις οποίες υποστηρίζει ένα αναγνωρισμένο πιστοποιητικό ([5]) ([6]).

Το προτεινόμενο κοινό σχεδιότυπο είναι σύμμορφο με την εφαρμογή του βάσει των προδιαγραφών του ETSI TS 102 231 ([7]) οι οποίες χρησιμοποιούνται όσον αφορά την κατάρτιση, τη δημοσίευση, τον τόπο, την πρόσβαση, την επαλήθευση ταυτότητας και την εμπιστοσύνη σε τέτοιου είδους καταλόγους.

([1]) Όπως ορίζεται στο άρθρο 2 σημείο11 της οδηγίας 1999/93/ΕΚ.
([2]) Όπως ορίζεται στο άρθρο 2 σημείο10 της οδηγίας 1999/93/ΕΚ.
([3]) Όπως ορίζεται στο άρθρο 2 σημείο6 της οδηγίας 1999/93/ΕΚ.
([4]) Όπως ορίζεται στο άρθρο 2 σημείο2 της οδηγίας 1999/93/ΕΚ.
([5]) Για μια AdES που υποστηρίζεται από ένα QC χρησιμοποιείται το ακρώνυμο «AdESQC» σε όλο το παρόν έγγραφο.
([6]) Επισημαίνεται ότι υπάρχουν πολλές ηλεκτρονικές υπηρεσίες που βασίζονται σε απλές AdES, των οποίων η διασυνοριακή χρήση θα διευκολυνόταν επίσης, δεδομένου ότι οι βοηθητικές υπηρεσίες πιστοποίησης (π.χ. η έκδοση μη αναγνωρισμένων πιστοποιητικών) αποτελούν μέρος των εποπτευόμενων/διαπιστευμένων υπηρεσιών που καλύπτονται από την ενότητα εθελοντικών πληροφοριών του καταλόγου εμπίστευσης των κρατών μελών.
([7]) ETSI TS 102 231 — Ηλεκτρονικές Υπογραφές και Υποδομές (Electronic Signatures and Infrastructures - ESI): Παροχή εναρμονισμένων πληροφοριών για την κατάσταση υπηρεσιών εμπίστευσης.

▼C1

2. **Οδηγίες για την επεξεργασία καταχωρίσεων του TL**

2.1. *Ένας TL που επικεντρώνεται στις εποπτευόμενες/διαπιστευμένες υπηρεσίες πιστοποίησης*

Σχετικές υπηρεσίες πιστοποίησης και πάροχοι υπηρεσιών πιστοποίησης σε έναν ενιαίο κατάλογο

Ο κατάλογος εμπίστευσης ενός κράτους μέλους ορίζεται ως ο «Κατάλογος κατάστασης εποπτείας/διαπίστευσης των υπηρεσιών πιστοποίησης από παρόχους υπηρεσιών πιστοποίησης οι οποίοι εποπτεύονται/διαπιστεύονται από το εκάστοτε κράτος μέλος ως προς τη συμμόρφωση με τις σχετικές διατάξεις της οδηγίας 1999/93/ΕΚ».

Ένας τέτοιος κατάλογος εμπίστευσης πρέπει να καλύπτει:

— **όλους τους παρόχους υπηρεσιών πιστοποίησης**, όπως ορίζονται στο άρθρο 2 σημείο 11 της οδηγίας 1999/93/ΕΚ, ήτοι «φορέας ή φυσικό ή νομικό πρόσωπο που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες, συναφείς με τις ηλεκτρονικές υπογραφές»,

— **που εποπτεύονται/διαπιστεύονται** ως προς τη συμμόρφωση με τις συναφείς διατάξεις που ορίζονται από την οδηγία 1999/93/ΕΚ.

Αν εξεταστούν οι ορισμοί και οι διατάξεις που ορίζονται στην οδηγία 1999/93/ΕΚ, ειδικά όσον αφορά τους συναφείς CSP και τα συστήματα εποπτείας/εθελοντικής διαπίστευσής τους, μπορεί να γίνει διάκριση σε δύο ομάδες CSP, δηλαδή τους CSP που εκδίδουν QC για το κοινό (CSP_{QC}), και τους CSP που δεν εκδίδουν QC για το κοινό, αλλά που παρέχουν «λοιπές (βοηθητικές) υπηρεσίες συναφείς με τις ηλεκτρονικές υπογραφές»

— **CSP που εκδίδουν QC:**

— Πρέπει να εποπτεύονται από το κράτος μέλος όπου είναι εγκατεστημένοι (αν είναι εγκατεστημένοι σε ένα κράτος μέλος) και μπορούν επίσης να λάβουν διαπίστευση ως προς τη συμμόρφωση με τις διατάξεις της οδηγίας 1999/93/ΕΚ, συμπεριλαμβανομένων των απαιτήσεων του παραρτήματος I (απαιτήσεις για τα QC), και των απαιτήσεων του παραρτήματος II (απαιτήσεις για τους CSP που εκδίδουν QC). Οι CSP που εκδίδουν QC οι οποίοι είναι διαπιστευμένοι σε ένα κράτος μέλος πρέπει να εξακολουθούν να εμπίπτουν στο κατάλληλο σύστημα εποπτείας του εν λόγω κράτους μέλους, εκτός αν δεν είναι εγκατεστημένοι στο εν λόγω κράτος μέλος.

— Το ισχύον σύστημα «εποπτείας» (αντίστοιχα σύστημα «εθελοντικής διαπίστευσης») ορίζεται και πρέπει να πληροί τις σχετικές απαιτήσεις της οδηγίας 1999/93/ΕΚ, ειδικά εκείνες που ορίζονται στο άρθρο 3 παράγραφος 3, άρθρο 8 παράγραφος 1, άρθρο 11, αιτιολογική σκέψη (13) [αντίστοιχα, άρθρο 2 σημείο 13, άρθρο 3 παράγραφος 2, άρθρο 7 παράγραφος 1 στοιχείο α), άρθρο 8 παράγραφος 1, άρθρο 11, αιτιολογικές σκέψεις (4)-(11-13)].

— **CSP που δεν εκδίδουν QC**

— Μπορούν να εμπίπτουν σε ένα σύστημα «εθελοντικής διαπίστευσης» (όπως ορίζεται στην οδηγία 199/93/ΕΚ και σε συμμόρφωση με αυτήν) ή/και στο πλαίσιο ενός εθνικά καθορισμένου «αναγνωρισμένου σχήματος έγκρισης», το οποίο εφαρμόζεται σε εθνική βάση για την εποπτεία της συμμόρφωσης με τις διατάξεις που ορίζονται στην οδηγία και ενδεχομένως με τις εθνικές διατάξεις όσον αφορά την παροχή υπηρεσιών πιστοποίησης (υπό την έννοια του άρθρου 2 σημείο 11 της οδηγίας).

— Κάποια από τα φυσικά ή ψηφιακά (λογικά) αντικείμενα που δημιουργούνται ή που εκδίδονται ως αποτέλεσμα της παροχής μιας υπηρεσίας πιστοποίησης μπορεί να δικαιούνται μια ειδική «αναγνώριση» βάσει της συμμόρφωσής τους με τις διατάξεις και τις απαιτήσεις που ορίζονται σε εθνικό επίπεδο, αλλά η έννοια μιας τέτοιας «αναγνώρισης» ενδέχεται να περιοριστεί αποκλειστικά σε εθνικό επίπεδο.

▼C1

Ο κατάλογος εμπίστευσης ενός κράτους μέλους πρέπει να παρέχει κάποιες ελάχιστες πληροφορίες για τους εποπτευόμενους/διαπιστευμένους CSP που εκδίδουν αναγνωρισμένα πιστοποιητικά στο κοινό σύμφωνα με τις διατάξεις που ορίζονται στην οδηγία 1999/93/ΕΚ [άρθρο 3 παράγραφοι 3 και 2 και άρθρο 7 παράγραφος 1 στοιχείο α)], πληροφορίες σχετικά με τα QC που υποστηρίζουν την ηλεκτρονική υπογραφή και σχετικά με το αν η υπογραφή δημιουργείται ή όχι μέσω μιας ασφαλούς διάταξης δημιουργίας υπογραφής.

Ο κατάλογος εμπίστευσης μπορεί να συμπεριλαμβάνει σε εθνικό επίπεδο και εθελοντικά επιπλέον πληροφορίες σχετικά με άλλους εποπτευόμενους/διαπιστευμένους CSP που δεν εκδίδουν QC (π.χ. CSP που παρέχουν υπηρεσίες χρονοσφράγισης και που εκδίδουν αδειοδοτικά χρονοσφράγισης, CSP που εκδίδουν μη αναγνωρισμένα πιστοποιητικά κ.λπ.).

Ο κατάλογος εμπίστευσης αποσκοπεί στα εξής:

— στην καταγραφή και στην παροχή αξιόπιστων πληροφοριών σχετικά με την κατάσταση εποπτείας/διαπίστευσης των υπηρεσιών πιστοποίησης από παρόχους υπηρεσιών πιστοποίησης οι οποίοι εποπτεύονται/διαπιστεύονται από το κράτος μέλος το οποίο είναι υπεύθυνο για την κατάρτιση και την τήρηση του καταλόγου, ως προς τη συμμόρφωση με τις σχετικές διατάξεις της οδηγίας 1999/93/ΕΚ,

— στη διευκόλυνση της επικύρωσης των ηλεκτρονικών υπογραφών που υποστηρίζονται από τις εποπτευόμενες/διαπιστευμένες υπηρεσίες πιστοποίησης του καταλόγου από τους CSP του καταλόγου.

Ενιαίο σύνολο τιμών κατάστασης εποπτείας/διαπίστευσης

Πρέπει να καταρτιστεί και να τηρείται μόνο ένας ενιαίος TL ανά κράτος μέλος, για να υποδεικνύει την κατάσταση εποπτείας ή/και διαπίστευσης των υπηρεσιών πιστοποίησης από τους CSP που εποπτεύονται/διαπιστεύονται από το κράτος μέλος.

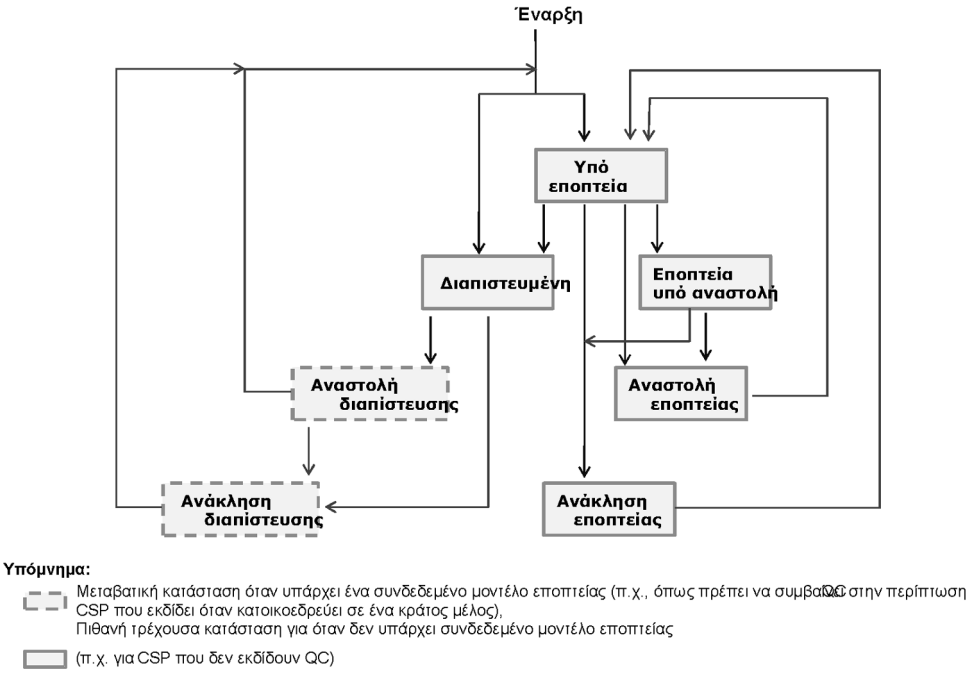
Το γεγονός ότι η υπηρεσία αυτή τη στιγμή υπόκειται είτε σε εποπτεία είτε σε διαπίστευση αποτελεί μέρος της τρέχουσας κατάστασής της. Επιπλέον, μια κατάσταση εποπτείας ή διαπίστευσης μπορεί να είναι «σε εξέλιξη», «υπό αναστολή», «σε αναστολή» ή ακόμη και «σε ανάκληση». Για όλη τη διάρκεια της ζωής της, η ίδια υπηρεσία πιστοποίησης μπορεί να μεταβεί από κατάσταση εποπτείας σε κατάσταση διαπίστευσης και αντίστροφα ([1]).

Το διάγραμμα 1 παρακάτω περιγράφει την αναμενόμενη ροή, για μια ενιαία υπηρεσία πιστοποίησης, ανάμεσα σε πιθανές καταστάσεις εποπτείας/διαπίστευσης:

([1]) Π.χ., ένας πάροχος υπηρεσιών διαπίστευσης ο οποίος είναι εγκατεστημένος σε ένα κράτος μέλος, ο οποίος παρέχει μια υπηρεσία πιστοποίησης που αρχικά εποπτεύεται από το κράτος μέλος (εποπτική αρχή), μπορεί, μετά την πάροδο ορισμένου χρονικού διαστήματος, να αποφασίσει να προβεί σε εθελοντική διαπίστευση για την υπηρεσία πιστοποίησης που αυτή τη στιγμή εποπτεύεται. Αντίθετα, ένας πάροχος υπηρεσιών πιστοποίησης σε ένα άλλο κράτος μέλος μπορεί να αποφασίσει να μην διακόψει μια διαπιστευμένη υπηρεσία πιστοποίησης αλλά να τη μεταφέρει από την κατάσταση διαπίστευσης στην κατάσταση εποπτείας, π.χ. για επιχειρηματικούς ή/και οικονομικούς λόγους.

▼C1

Αναμενόμενη ροή κατάστασης εποπτείας/διαπίστευσης για μια ενιαία υπηρεσία CS



Διάγραμμα 1

Μια υπηρεσία πιστοποίησης που εκδίδει QC πρέπει να εποπτεύεται (αν είναι εγκατεστημένη σε ένα κράτος μέλος) και μπορεί να διαπιστευτεί εθελοντικά. Η κατάσταση μιας τέτοιας υπηρεσίας όταν συγκαταλέγεται σε έναν κατάλογο εμπίστευσης μπορεί να λάβει μια οποιαδήποτε από τις παραπάνω καταστάσεις ως «τιμή τρέχουσας κατάστασης». Ωστόσο, πρέπει να επισημανθεί ότι οι καταστάσεις «Αναστολή διαπίστευσης» και «Ανάκληση διαπίστευσης» πρέπει να είναι και οι δύο «μεταβατικές καταστάσεις» μόνο σε περίπτωση υπηρεσιών CSPQC που είναι εγκατεστημένες σε ένα κράτος μέλος, καθώς οι εν λόγω υπηρεσίες πρέπει να εποπτεύονται εξ ορισμού (ακόμη κι όταν δεν είναι πλέον διαπιστευμένες).

Είναι απαραίτητο τα κράτη μέλη που θεσπίζουν ή που έχουν θεσπίσει «αναγνωρισμένο σχήμα/αναγνωρισμένα σχήματα έγκρισης» σε εθνικό επίπεδο, τα οποία τίθενται σε εφαρμογή σε εθνική βάση για την εποπτεία της συμμόρφωσης υπηρεσιών από CSP που δεν εκδίδουν QC με τις διατάξεις που ορίζονται στην οδηγία 1999/93/ΕΚ, και ενδεχομένως με τις εθνικές διατάξεις σχετικά με την παροχή υπηρεσιών πιστοποίησης (υπό την έννοια του άρθρου 2 σημείο 11 της οδηγίας) να κατατάξουν το εν λόγω σχήμα/τα εν λόγω σχήματα στις παρακάτω δυο κατηγορίες:

— «εθελοντική διαπίστευση», όπως ορίζεται και διέπεται από την οδηγία 1999/93/ΕΚ [άρθρο 2 σημείο 13, άρθρο 3 παράγραφος 2, άρθρο 7 παράγραφος 1 στοιχείο α), άρθρο 8 παράγραφος 1, άρθρο 11 αιτιολογικές σκέψεις (4)-(11-13)],

— «εποπτεία», όπως απαιτείται από την οδηγία 1999/93/ΕΚ και τίθεται σε εφαρμογή από τις εθνικές διατάξεις και απαιτήσεις, σύμφωνα με τους εθνικούς νόμους.

▼C1

Έτσι, μια υπηρεσία πιστοποίησης που δεν εκδίδει αναγνωρισμένα πιστοποιητικά μπορεί να εποπτεύεται ή να διαπιστεύεται εθελοντικά. Η κατάσταση μιας τέτοιας υπηρεσίας όταν συγκαταλέγεται σε έναν κατάλογο εμπίστευσης μπορεί να βρίσκεται σε μια οποιαδήποτε από τις παραπάνω καταστάσεις ως «τρέχουσα κατάσταση» (βλέπε διάγραμμα 1).

Ο κατάλογος εμπίστευσης πρέπει να περιλαμβάνει πληροφορίες σχετικά με το υπάρχον σχήμα/τα υπάρχοντα σχήματα εποπτείας/διαπίστευσης και ειδικά:

— πληροφορίες σχετικά με το σχήμα εποπτείας που ισχύει για κάθε CSP_{QC},

— πληροφορίες, όταν υπάρχουν, για το εθνικό σχήμα «εθελοντικής διαπίστευσης» που ισχύει για κάθε CSP_{QC},

— πληροφορίες, όταν υπάρχουν, για το σύστημα εποπτείας που ισχύει για κάθε CSP που δεν εκδίδει QC,

— πληροφορίες, όταν υπάρχουν, για το εθνικό σχήμα «εθελοντικής διαπίστευσης» που ισχύει για κάθε CSP που δεν εκδίδει QC.

Τα δυο τελευταία σύνολα πληροφοριών είναι κρίσιμης σημασίας για τα μέρη που βασίζονται σε αυτά, προκειμένου να αξιολογούν την ποιότητα και το επίπεδο ασφαλείας των εν λόγω συστημάτων εποπτείας/διαπίστευσης που ισχύουν σε εθνικό επίπεδο για τους CSP που δεν εκδίδουν QC. Όταν οι πληροφορίες για την κατάσταση εποπτείας/διαπίστευσης παρέχονται μέσω του TL όσον αφορά τις υπηρεσίες των CSP που δεν εκδίδουν QC, τα προαναφερθέντα σύνολα πληροφοριών πρέπει να παρέχονται σε επίπεδο TL μέσω της χρήσης του «URI σχήματος πληροφοριών» (διάταξη 5.3.7 – πληροφορίες που παρέχουν τα κράτη μέλη), «Τύπος σχήματος/κοινότητα/κανόνες» (διάταξη 5.3.9 – μέσω της χρήσης ενός κειμένου κοινού για όλα τα κράτη μέλη, και προαιρετικών ειδικών πληροφοριών που παρέχει ένα κράτος μέλος) και του «Πολιτική/νομική σημείωση TSL» (διάταξη 5.3.11 – κείμενο κοινό για όλα τα κράτη μέλη, το οποίο αναφέρεται στην οδηγία 1999/93/ΕΚ, μαζί με τη δυνατότητα κάθε κράτους μέλους να προσθέτει κείμενα/παραπομπές που να αφορούν ειδικά το εκάστοτε κράτος μέλος). Επιπλέον πληροφορίες «αναγνώρισης», οι οποίες ορίζονται στο επίπεδο των εθνικών συστημάτων εποπτείας/διαπίστευσης για τους CSP που δεν εκδίδουν QC μπορούν να παρέχονται όταν υπάρχουν και απαιτούνται (π.χ. για να γίνει διάκριση μεταξύ πολλών επιπέδων ποιότητας/ασφάλειας) μέσω της χρήσης της επέκτασης «additionalServiceInformation» (διάταξη 5.8.2) ως μέρος του πεδίου «Service information extension» (επέκταση πληροφοριών υπηρεσιών) (διάταξη 5.5.9). Περαιτέρω πληροφορίες σχετικά με τις αντίστοιχες τεχνικές προδιαγραφές παρέχονται στις αναλυτικές προδιαγραφές στο κεφάλαιο I.

Παρότι ενδέχεται χωριστοί φορείς ενός κράτους μέλους να είναι αρμόδιοι για την εποπτεία και τη διαπίστευση των υπηρεσιών πιστοποίησης στο εν λόγω κράτος μέλος, αναμένεται να χρησιμοποιείται μόνο μία καταχώριση για μια ενιαία υπηρεσία πιστοποίησης [η οποία ορίζεται μέσω της «Ψηφιακής ταυτότητας υπηρεσίας» της σύμφωνα με το ETSI TS 102 231 ([1])] και να επικαιροποιείται αναλόγως η κατάσταση εποπτείας/διαπίστευσής της. Η σημασία των προαναφερθεισών καταστάσεων περιγράφεται στη σχετική διάταξη 5.5.4 των αναλυτικών τεχνικών προδιαγραφών στο κεφάλαιο I.

2.2. *Καταχωρίσεις TL με στόχο τη διευκόλυνση της επικύρωσης QES και* $AdES_{QC}$

Το πιο κρίσιμο μέρος της δημιουργίας του TL είναι η κατάρτιση του υποχρεωτικού μέρους του TL, δηλαδή του «Καταλόγου υπηρεσιών» ανά CSP που εκδίδει QC, προκειμένου να παρουσιαστεί σωστά η ακριβής κατάσταση έκδοσης καθεμιάς από τις υπηρεσίες πιστοποίησης με έκδοση QC και να διασφαλίζεται ότι οι πληροφορίες που παρέχονται μέσω κάθε καταχώρισης επαρκούν για τη διευκόλυνση της επικύρωσης των QES και των $AdES_{QC}$ (σε συνδυασμό με το περιεχόμενο του QC για την οντότητα-τελικό αποδέκτη το οποίο εκδίδεται από τον CSP σύμφωνα με την υπηρεσία πιστοποίησης που αναγράφεται στην εν λόγω καταχώριση).

([1]) ETSI TS 102 231 — Ηλεκτρονικές Υπογραφές και Υποδομές (ESI): Παροχή εναρμονισμένων πληροφοριών για την κατάσταση υπηρεσιών εμπίστευσης.

▼C1

Εφόσον δεν υπάρχει πραγματικά διαλειτουργικό και διασυνοριακό προφίλ για το QC, στις απαραίτητες πληροφορίες ενδέχεται να συμπεριλαμβάνονται κι άλλες πληροφορίες εκτός από την «Ψηφιακή ταυτότητα υπηρεσίας» μιας ενιαίας αρχής πιστοποίησης βάσης (Root) CA, ειδικά πληροφορίες που ορίζουν την κατάσταση QC του εκδιδόμενου πιστοποιητικού και πληροφορίες για το αν οι υποστηριζόμενες υπογραφές δημιουργούνται από μια SSCD ή όχι. Ο φορέας ενός κράτους μέλους ο οποίος είναι υπεύθυνος για την κατάρτιση, την επεξεργασία και την τήρηση του TL (δηλαδή ο υπεύθυνος διαχείρισης του σχήματος σύμφωνα με το ETSI TS 102 231) πρέπει, επομένως, να λαμβάνει υπόψη το τρέχον προφίλ και το περιεχόμενο του πιστοποιητικού για κάθε εκδιδόμενο QC, ανά CSP_{QC} που συμπεριλαμβάνεται στον TL.

Θεωρητικά, κάθε εκδιδόμενο QC πρέπει να συμπεριλαμβάνει τη δήλωση QcCompliance, η οποία ορίζεται από το ETSI ([1]) όταν υποστηρίζεται ότι είναι QC και πρέπει να συμπεριλαμβάνει τη δήλωση QcSSCD, η οποία ορίζεται από το ETSI, όταν υποστηρίζεται ότι υποστηρίζεται από μια SSCD για τη δημιουργία ηλεκτρονικών υπογραφών ή/και ότι κάθε εκδιδόμενο QC συμπεριλαμβάνει ένα από τα QCP/QCP+, τα αναγνωριστικά αντικειμένου πολιτικής πιστοποιητικού (OID), τα οποία ορίζονται στις τεχνικές προδιαγραφές του ETSI, TS 101 456 ([2]). Το γεγονός ότι οι CSP που εκδίδουν QC χρησιμοποιούν διαφορετικά πρότυπα ως αναφορές, το μεγάλο εύρος για την ερμηνεία των εν λόγω προτύπων, καθώς και η μη επίγνωση της ύπαρξης και του προηγούμενου κάποιων κανονιστικών τεχνικών προδιαγραφών ή προτύπων, οδήγησε σε διαφορές στο πραγματικό περιεχόμενο των QC που εκδίδονται τώρα (π.χ. η χρήση ή η μη χρήση των εν λόγω δηλώσεων QcStatements που ορίζονται στο ETSI) και κατά συνέπεια αποτρέπουν τον αποδέκτη να βασίζεται απλά στο πιστοποιητικό του υπογράφοντος (και στη συνδεδεμένη αλυσίδα/διαδρομή) για να αξιολογήσει, τουλάχιστον με τρόπο ανάγνωσης από μηχανή, αν το πιστοποιητικό που υποστηρίζει ηλεκτρονική υπογραφή υποστηρίζεται ότι αποτελεί QC και αν συνδέεται με μια ασφαλή διάταξη δημιουργίας υπογραφής μέσω της οποίας δημιουργήθηκε η ηλεκτρονική υπογραφή.

Η συμπλήρωση των πεδίων «Αναγνωριστικό τύπου υπηρεσίας» (Service type identifier - «Sti»), «Ονομασία υπηρεσίας» (Service name - «Sn») και «Ψηφιακή ταυτότητα υπηρεσίας» (Service digital identity - «Sdi») ([3]) με τις πληροφορίες που παρέχονται από το πεδίο «Επεκτάσεις πληροφοριών υπηρεσίας» (Service information extensions - «Sie») επιτρέπει στο προτεινόμενο κοινό σχεδιότυπο TL να καθορίσει πλήρως έναν συγκεκριμένο τύπο αναγνωρισμένου πιστοποιητικού που εκδίδεται από μια καταγεγραμμένη υπηρεσία πιστοποίησης CSP που εκδίδει QC για την παροχή πληροφοριών σχετικά με το αν υποστηρίζεται ή όχι από μια ασφαλή διάταξη δημιουργίας υπογραφής (όταν οι πληροφορίες αυτές απουσιάζουν από το εκδιδόμενο QC). Πληροφορίες για μια συγκεκριμένη «Τρέχουσα κατάσταση υπηρεσίας» (Service current status - «Scs») ασφαλώς σχετίζονται με αυτή την καταχώριση. Αυτό παρουσιάζεται στο διάγραμμα 2 παρακάτω.

Η καταγραφή μιας υπηρεσίας απλά παρέχοντας το «Sdi» μιας αρχής πιστοποίησης βάσης (Root) CA σημαίνει ότι εξασφαλίζεται (από τον CSP που εκδίδει QC αλλά και από τον φορέα εποπτείας/διαπίστευσης, που είναι υπεύθυνος για την εποπτεία/διαπίστευση του εν λόγω CSP) ότι οποιοδήποτε πιστοποιητικό για οντότητες-τελικούς αποδέκτες, το οποίο εκδίδεται βάσει της εν λόγω αρχής πιστοποίησης βάσης (Root) CA (ιεραρχία) περιέχει αρκετές πληροφορίες οριζόμενες από το ETSI και με δυνατότητα επεξεργασίας με μηχανικά μέσα για να αξιολογηθεί αν πρόκειται για QC ή όχι και αν υποστηρίζεται από SSCD. Σε περίπτωση, για παράδειγμα, που αυτή η τελευταία πρόταση δεν είναι αληθής (π.χ. αν δεν υπάρχουν στο QC ενδείξεις τυποποιημένες βάσει του ETSI και με δυνατότητα επεξεργασίας με μηχανικά μέσα σχετικά με το αν υποστηρίζεται από SSCD), τότε καταγράφοντας μόνο το «Sdi» της εν λόγω αρχής πιστοποίησης βάσης (Root) CA, το μόνο συμπέρασμα που μπορεί να εξαχθεί είναι ότι τα QC που εκδόθηκαν σύμφωνα με την εν λόγω ιεραρχία αρχής πιστοποίησης βάσης (Root) CA δεν υποστηρίζονται από καμία SSCD. Προκειμένου να θεωρηθεί ότι τα εν λόγω QC υποστηρίζονται από SSCD, πρέπει να χρησιμοποιηθεί το «Sie» για να δηλώσει αυτό το γεγονός (αυτό υποδεικνύει επίσης ότι παρέχει σχετικές εγγυήσεις ο CSP που εκδίδει QC και που εποπτεύεται/διαπιστεύεται από τον φορέα εποπτείας/διαπίστευσης αντίστοιχα).

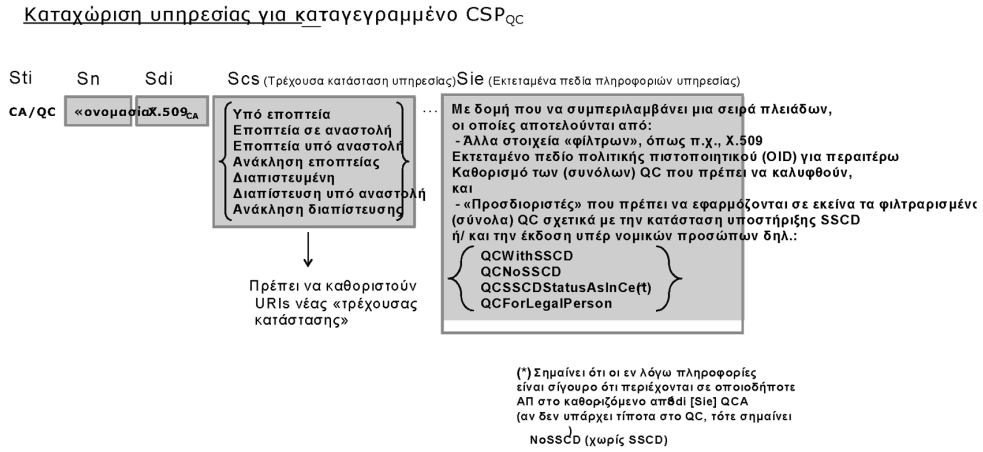
([1]) Ανατρέξτε στις τεχνικές προδιαγραφές του ETSI, TS 101 862 – Ηλεκτρονικές Υπογραφές και Υποδομές (ESI): Προφίλ Αναγνωρισμένου Πιστοποιητικού.

([2]) ETSI TS 101 456 — Ηλεκτρονικές Υπογραφές και Υποδομές (ESI)· απαιτήσεις πολιτικής για τις αρχές πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά.

([3]) δηλαδή και ως ελάχιστο, ένα πιστοποιητικό X.509 v3 του εκδίδοντος QCA ή μιας ανώτερης CA στη διαδρομή πιστοποίησης.

▼C1

Γενικές αρχές — Κανόνες επεξεργασίας — Καταχωρίσεις CSP_{QC} (καταγεγραμμένες υπηρεσίες)



Διάγραμμα 2

Καταχώριση υπηρεσίας στον TL, για καταγεγραμμένο CSP που εκδίδει QC, η οποία εφαρμόζεται σε μορφή TSL

Οι τρέχουσες τεχνικές προδιαγραφές του κοινού σχεδιοτύπου του TL επιτρέπουν τη χρήση ενός συνδυασμού πέντε κυρίων μερών πληροφοριών στην καταχώριση της υπηρεσίας:

— του «Αναγνωριστικού τύπου υπηρεσίας» (Service type identifier - «Sti»), π.χ. με το οποίο αναγνωρίζεται μια CA που εκδίδει QC («CA/QC»),

— της «Ονομασίας υπηρεσίας» (Service name - «Sn»),

— τις πληροφορίες «Ψηφιακής ταυτότητας υπηρεσίας» (Service digital identity - «Sdi»), οι οποίες καθορίζουν μια καταγεγραμμένη υπηρεσία, π.χ. το πιστοποιητικό X.509v3 (ως ελάχιστο) ενός CA που εκδίδει QC,

— Για τις υπηρεσίες CA/QC, τις προαιρετικές πληροφορίες «Επεκτάσεων πληροφοριών υπηρεσίας» (Service information extensions - «Sie»), οι οποίες επιτρέπουν να συμπεριληφθεί σειρά μιας ή περισσότερων πλειάδων, καθεμία από τις οποίες παρέχει:

  — Κριτήρια, τα οποία θα χρησιμοποιούνται για την περαιτέρω αναγνώριση (φιλτράρισμα) στη θέση της αναγνωρισμένης υπηρεσίας πιστοποίησης «Sdi» της υπηρεσίας εκείνης (δηλαδή το σύνολο αναγνωρισμένων πιστοποιητικών), για την οποία απαιτούνται/παρέχονται επιπλέον πληροφορίες, όσον αφορά την ένδειξη της υποστήριξης από SSCD (ή/και την έκδοση υπέρ ενός νομικού προσώπου) και

  — τις συνδεδεμένες πληροφορίες («προσδιοριστές») σχετικά με το αν αυτό το περαιτέρω ταυτοποιημένο σύνολο υπηρεσιών αναγνωρισμένων πιστοποιητικών υποστηρίζεται ή όχι από μια SSCD ή σχετικά με το αν οι εν λόγω συνδεδεμένες πληροφορίες αποτελούν μέρος του QC βάσει τυποποιημένης μορφής με δυνατότητα επεξεργασίας από μηχανή, ή/και τις πληροφορίες όσον αφορά το γεγονός ότι τα εν λόγω QC εκδίδονται υπέρ νομικών προσώπων (εξ ορισμού πρέπει να θεωρείται ότι εκδίδονται μόνο υπέρ φυσικών προσώπων).

▼C1

— Τις πληροφορίες «τρέχουσας κατάστασης» για την εν λόγω καταχώριση υπηρεσίας, οι οποίες πληροφορούν:

— για το αν πρόκειται για εποπτευόμενη ή διαπιστευμένη υπηρεσία και

— για την ίδια την κατάσταση εποπτείας/διαπίστευσης.

2.3. *Κατευθυντήριες γραμμές επεξεργασίας και χρήσης για τις καταχωρίσεις υπηρεσιών CSP_{QC}*

Οι **γενικές κατευθυντήριες γραμμές επεξεργασίας** είναι οι εξής:

1. Αν διασφαλίζεται (η εγγύηση παρέχεται από τον CSP_{QC} και εποπτεύεται/διαπιστεύεται από τον φορέα εποπτείας (Supervisory Body - SB)/τον φορέα διαπίστευσης (Accreditation Body - AB)) ότι, για μια καταγεγραμμένη υπηρεσία που προσδιορίζεται με ένα «Sdi», οποιοδήποτε QC που υποστηρίζεται από μια SSCD, περιέχει την καθοριζόμενη από το ETSI δήλωση συμμόρφωσης QcCompliance, και περιέχει τη δήλωση QcSSCD ή/και το QCP + αναγνωριστικό αντικειμένου (Object Identifier - OID), τότε η χρήση ενός καταλλήλου «Sdi» αρκεί και το πεδίο «Sie» μπορεί να χρησιμοποιηθεί προαιρετικά και δεν θα είναι απαραίτητο να περιέχει πληροφορίες υποστήριξης της SSCD.

2. Αν διασφαλίζεται (η εγγύηση παρέχεται από τον CSP_{QC} και εποπτεύεται/διαπιστεύεται από τον SB/AB) ότι, για μια καταγεγραμμένη υπηρεσία που προσδιορίζεται με ένα «Sdi», οποιοδήποτε QC που δεν υποστηρίζεται από μια SSCD, περιέχει τη δήλωση συμμόρφωσης QcCompliance ή/και το QCP OID, και είναι τέτοιου είδους ώστε να πρόκειται να μην περιέχει τη δήλωση QcSSCD ή το QCP + OID, τότε η χρήση ενός καταλλήλου «Sdi» αρκεί και το πεδίο «Sie» μπορεί να χρησιμοποιηθεί προαιρετικά και δεν θα είναι απαραίτητο να περιέχει πληροφορίες υποστήριξης της SSCD (πράγμα που σημαίνει ότι δεν υποστηρίζεται από τέτοια SSCD).

3. Αν διασφαλίζεται (η εγγύηση παρέχεται από τον CSP_{QC} και εποπτεύεται/διαπιστεύεται από τον SB/AB) ότι, για μια καταγεγραμμένη υπηρεσία, η οποία αναγνωρίζεται με ένα «Sdi», οποιοδήποτε QC περιέχει τη δήλωση συμμόρφωσης QcCompliance, και κάποια από αυτά τα QC πρέπει να υποστηρίζονται από ασφαλείς διατάξεις δημιουργίας υπογραφών, ενώ κάποια άλλα όχι (π.χ. μπορεί να γίνει αυτή η διάκριση μέσω διαφορετικών OID πολιτικών πιστοποιητικού ανά CSP ή μέσω άλλων πληροφοριών για κάθε CSP στο QC, άμεσα ή έμμεσα, με ή χωρίς δυνατότητα επεξεργασίας με μηχανικά μέσα), αλλά δεν περιέχει ΟΥΤΕ τη δήλωση QcSSCD ΟΥΤΕ το QCP(+) OID του ETSI, τότε η χρήση ενός κατάλληλου «Sdi» ενδέχεται να μην αρκεί ΚΑΙ το πεδίο «Sie» πρέπει να χρησιμοποιηθεί για να υποδείξει ρητές πληροφορίες υποστήριξης από SSCD, καθώς και μια πιθανή επέκταση πληροφοριών για την αναγνώριση του καλυπτόμενου συνόλου πιστοποιητικών. Γι' αυτό ενδέχεται να απαιτηθεί να συμπεριληφθούν διαφορετικές «τιμές πληροφοριών με υποστήριξη από SSCD» για το ίδιο «Sdi» όταν γίνεται χρήση του πεδίου «Sie».

4. Αν διασφαλίζεται (η εγγύηση παρέχεται από τον CSP_{QC} και εποπτεύεται/διαπιστεύεται από τον SB/AB) ότι, για μια καταγεγραμμένη υπηρεσία, η οποία αναγνωρίζεται με ένα «Sdi», οποιοδήποτε QC δεν περιέχει καμία δήλωση συμμόρφωσης QcCompliance, ούτε και QCP OID, ούτε δήλωση QcSSCD, ούτε QCP + OID, αλλά διασφαλίζεται ότι κάποια από αυτά τα πιστοποιητικά για οντότητες-τελικούς αποδέκτες που εκδίδονται βάσει του εν λόγω «Sdi» πρέπει να είναι QC ή/και να υποστηρίζονται από SSCD, ενώ κάποια άλλα όχι (π.χ. μπορεί να γίνει αυτή η διάκριση μέσω διαφορετικών OIDs πολιτικών πιστοποιητικού ανά CSPQC ή μέσω άλλων πληροφοριών για κάθε CSPQC στο QC, άμεσα ή έμμεσα, με ή χωρίς δυνατότητα επεξεργασίας με μηχανικά μέσα), τότε η χρήση ενός κατάλληλου «Sdi» δεν θα αρκεί ΚΑΙ το πεδίο «Sie» πρέπει να χρησιμοποιηθεί για να συμπεριληφθούν ρητές πληροφορίες υποστήριξης από SSCD. Γι' αυτό ενδέχεται να απαιτηθεί να συμπεριληφθούν διαφορετικές «τιμές πληροφοριών με υποστήριξη από SSCD» για το ίδιο «Sdi» όταν γίνεται χρήση του πεδίου «Sie».

▼C1

Ως γενική εξ ορισμού αρχή, για έναν CSP ο οποίος είναι καταγεγραμμένος στον κατάλογο εμπίστευσης πρέπει να υπάρχει μία καταχώριση υπηρεσίας για κάθε πιστοποιητικό X.509v3 ανά υπηρεσία πιστοποίησης τύπου CA/QC, δηλαδή ανά αρχή πιστοποίησης που εκδίδει QC (άμεσα). Σε κάποιες προσεκτικά προβλεπόμενες περιπτώσεις και υπό προσεκτικά ρυθμιζόμενες συνθήκες, ο φορέας εποπτείας/διαπίστευσης ενός κράτους μέλους μπορεί να αποφασίσει να χρησιμοποιήσει το πιστοποιητικό X.509v3 μιας αρχής πιστοποίησης βάσης ή ανώτερου επιπέδου (δηλαδή μιας αρχής πιστοποίησης η οποία δεν εκδίδει άμεσα QC για οντότητες-τελικούς αποδέκτες, αλλά η οποία πιστοποιεί μια ιεραρχία αρχών πιστοποίησης μέχρι εκείνες τις αρχές που εκδίδουν QC για οντότητες-τελικούς αποδέκτες) ως το «Sdi» μιας ενιαίας καταχώρισης στον κατάλογο υπηρεσιών ενός καταγεγραμμένου CSP. Οι συνέπειες (υπέρ και κατά) της χρήσης του εν λόγω X.509v3 Αρχής Πιστοποίησης Βάσης ή Αρχής Πιστοποίησης Ανώτερης Βαθμίδας ως τιμών «Sdi» για τις καταχωρίσεις των υπηρεσιών του TL πρέπει να ληφθούν σοβαρά υπόψη και η ευθύνη να αναληφθεί από τα κράτη μέλη. Επιπλέον, χρησιμοποιώντας αυτή την επιτρεπόμενη εξαίρεση από την εξ ορισμού αρχή, το κράτος μέλος πρέπει να παράσχει την τεκμηρίωση που απαιτείται για να διευκολύνει τη δημιουργία και την επαλήθευση της διαδρομής πιστοποίησης.

Προκειμένου να παρουσιαστούν οι γενικές κατευθυντήριες γραμμές επεξεργασίας, μπορούν να δοθούν τα παρακάτω παραδείγματα: Στο πλαίσιο ενός CSP_{QC} ο οποίος χρησιμοποιεί μια αρχή πιστοποίησης βάσης, στο πλαίσιο της οποίας πολλές αρχές πιστοποίησης εκδίδουν τόσο αναγνωρισμένα όσο και μη αναγνωρισμένα πιστοποιητικά, αλλά τα QC που εκδίδονται περιέχουν μόνο τη δήλωση συμμόρφωσης QcCompliance και καμία ένδειξη για το αν υποστηρίζονται από SSCD, η καταγραφή του «Sdi» της αρχής πιστοποίησης βάσης σημαίνει μόνο, βάσει των κανόνων που εξηγήθηκαν παραπάνω, ότι οποιοδήποτε QC που εκδίδεται υπό την εν λόγω ιεραρχία αρχής πιστοποίησης βάσης ΔΕΝ υποστηρίζεται από κάποια SSCD. Αν τα εν λόγω QC πράγματι υποστηρίζονται από SSCD, συνιστάται ιδιαίτερα να χρησιμοποιηθεί η δήλωση QcSSCD στα QC που θα εκδίδονται μελλοντικά. Εν τω μεταξύ (μέχρι τη λήξη του τελευταίου QC που δεν περιέχει αυτές τις πληροφορίες), στον TSL μπορεί να χρησιμοποιηθεί το πεδίο «Sie» και η συσχετισμένη επέκταση «Προσδιορισμοί», π.χ. φιλτράροντας τα πιστοποιητικά μέσω ειδικού/ειδικών OID που καθορίζονται από τον CSP_{QC}, τα οποία χρησιμοποιούνται ενδεχομένως από τον CSP_{QC} για να κάνει διάκριση ανάμεσα στους διάφορους τύπους QC (κάποια από τα οποία υποστηρίζονται από SSCD, ενώ κάποια άλλα όχι) και τα οποία περιέχουν ρητές «πληροφορίες υποστήριξης SSCD» όσον αφορά τα πιστοποιητικά που φιλτράρονται μέσω της χρήσης «Προσδιοριστών».

Οι **γενικές κατευθυντήριες γραμμές χρήσης** για τις εφαρμογές, τις υπηρεσίες ή τα προϊόντα που αφορούν τις ηλεκτρονικές υπογραφές, και που βασίζονται στην εφαρμογή TSL ενός καταλόγου εμπίστευσης, σύμφωνα με τις παρούσες τεχνικές προδιαγραφές έχουν ως εξής:

Μια καταχώριση «CA/QC»«Sti» (παρομοίως μια καταχώριση CA/QC που αναγνωρίζεται περαιτέρω ότι αποτελεί «RootCA/QC» μέσω της χρήσης της επέκτασης «Sie» additionalServiceInformation)

— Δηλώνει ότι από την αρχή πιστοποίησης με αναγνωριστικό «Sdi» (παρομοίως με ιεραρχία αρχής πιστοποίησης η οποία ξεκινά από την αρχή πιστοποίησης βάσης με αναγνωριστικό «Sdi»), όλα τα εκδιδόμενα πιστοποιητικά για οντότητες-τελικούς αποδέκτες είναι QC, **εφόσον** υποστηρίζεται ότι είναι τέτοια στο πιστοποιητικό μέσω της χρήσης των κατάλληλων δηλώσεων QcStatements (δηλαδή QcC, QcSSCD) ή/και των QCP(+) OID που ορίζονται μέσω του ETSI (και αυτό διασφαλίζεται από το φορέα εποπτείας/διαπίστευσης, βλέπε παραπάνω «γενικές κατευθυντήριες γραμμές επεξεργασίας»).

Σημείωση: σε περίπτωση που δεν υπάρχουν πληροφορίες «Sie»«Αναγνώριση» ή σε περίπτωση που ένα πιστοποιητικό για οντότητες-τελικούς αποδέκτες το οποίο υποστηρίζεται ότι είναι QC δεν «αναγνωρίζεται περαιτέρω» μέσω σχετικής καταχώρισης «Sie», τότε οι πληροφορίες «με δυνατότητα επεξεργασίας με μηχανικά μέσα» που βρίσκονται στο QC θεωρούνται, βάσει της εποπτείας/διαπίστευσης, ως ακριβείς. Αυτό σημαίνει ότι η χρήση (ή μη χρήση) των κατάλληλων δηλώσεων QcStatements (δηλαδή QcC, QcSSCD) ή/και QCP(+) OIDs καθοριζόμενων βάσει του ETSI βεβαιώνεται ότι συμφωνεί με αυτό που υποστηρίζει ο CSP_{QC}

▼C1

— **και AN** υπάρχουν πληροφορίες «Sie»«Αναγνώριση», τότε εκτός από τον παραπάνω εξ ορισμού κανόνα ερμηνείας χρήσης, τα πιστοποιητικά εκείνα που ορίζονται μέσω της χρήσης της εν λόγω καταχώρισης «Sie»«Αναγνώριση», η οποία βασίζεται στην αρχή της αλληλουχίας των «φίλτρων», εντοπίζοντας περαιτέρω ένα σύνολο πιστοποιητικών και παρέχοντας επιπλέον πληροφορίες αναφορικά με την «υποστήριξη SSCD» ή/και το «Νομικό πρόσωπο ως υποκείμενο» (π.χ. τα πιστοποιητικά εκείνα που περιέχουν συγκεκριμένο αναγνωριστικό αντικειμένου στην επέκταση της πολιτικής πιστοποιητικού ή/και που έχουν συγκεκριμένη σχηματομορφή «Χρήσης κλειδιού» ή/και που φιλτράρονται μέσω της χρήσης συγκεκριμένης τιμής, η οποία εμφανίζεται σε συγκεκριμένο πεδίο ή εκτεταμένο πεδίο του πιστοποιητικού κ.λπ.), πρέπει να εξετάζονται σύμφωνα με το παρακάτω σύνολο «προσδιοριστών», επανορθώνοντας την έλλειψη πληροφοριών στο αντίστοιχο QC, δηλαδή:

— για να υποδειχθεί υποστήριξη από SSCD:

  — τιμή προσδιοριστή «QCWithSSCD», η οποία σημαίνει «το QC υποστηρίζεται από SSCD» ή

  — τιμή προσδιοριστή «QCNoSSCD», η οποία σημαίνει «το QC δεν υποστηρίζεται από SSCD» ή

  — τιμή προσδιοριστή «QCSSCDStatusAsInCert», η οποία σημαίνει ότι οι πληροφορίες υποστήριξης από SSCD είναι βέβαιο ότι περιλαμβάνονται σε οποιοδήποτε QC βάσει των πληροφοριών «Sdi»-«Sie» που παρέχονται στην εν λόγω καταχώριση CA/QC,

  Ή/ΚΑΙ

— για να υποδειχθεί έκδοση υπέρ νομικού προσώπου:

  — τιμή προσδιοριστή «QCForLegalPerson», η οποία σημαίνει «το πιστοποιητικό εκδόθηκε υπέρ νομικού προσώπου»

2.4. *Υπηρεσίες που υποστηρίζουν υπηρεσίες «CA/QC» αλλά που δεν αποτελούν μέρος των «CA/QC»«Sdi»*

Πρέπει επίσης να καλύπτονται οι περιπτώσεις κατά τις οποίες οι CRL και οι αποκρίσεις OCSP υπογράφονται από κλειδιά που δεν προέρχονται από μια αρχή πιστοποίησης που εκδίδει QC («CA/QC»). Αυτό μπορεί να καλυφθεί καταγράφοντας τις υπηρεσίες αυτές ως τέτοιες κατά την εφαρμογή TSL του TL (δηλαδή με ένα «Αναγνωριστικό τύπου υπηρεσίας» επιπλέον αναγνωρισμένο με μια επέκταση «additionalServiceInformation», η οποία παρουσιάζει μια υπηρεσία OCSP ή CRL ως μέρος της παροχής QC, π.χ. με τύπο υπηρεσίας «OCSP/QC» ή «CRL/QC» αντίστοιχα), εφόσον οι εν λόγω υπηρεσίες μπορούν να θεωρηθούν μέρος των εποπτευόμενων/διαπιστευμένων «αναγνωρισμένων» υπηρεσιών που έχουν σχέση με την παροχή υπηρεσιών πιστοποίησης QC. Ασφαλώς, οι αποκριτές OCSP ή οι εκδότες CRL, των οποίων τα πιστοποιητικά είναι υπογεγραμμένα από τις αρχές πιστοποίησης στην ιεραρχία μιας καταγεγραμμένης υπηρεσίας CA/QC πρέπει να θεωρούνται «έγκυρα» και σύμφωνα με την τιμή κατάστασης της καταγεγραμμένης υπηρεσίας CA/QC.

Παρόμοια διάταξη μπορεί να ισχύει και για υπηρεσίες πιστοποίησης που εκδίδουν μη αναγνωρισμένα πιστοποιητικά (τύπου υπηρεσίας «CA/PKC»), χρησιμοποιώντας εξ ορισμού τους τύπους υπηρεσιών OCSP και CRL βάσει των τεχνικών προδιαγραφών του ETSI, TS 102 231.

Επισημαίνεται ότι η εφαρμογή TSL του TL ΠΡΕΠΕΙ να συμπεριλαμβάνει υπηρεσίες ανάκλησης όταν οι σχετικές πληροφορίες δεν υπάρχουν στο πεδίο AIA των τελικών πιστοποιητικών ή όταν δεν φέρει την υπογραφή μιας αρχής πιστοποίησης από τις καταγεγραμμένες.

2.5. *Μετάβαση προς διαλειτουργικό προφίλ QC*

Κατά γενικό κανόνα, πρέπει να γίνει προσπάθεια για την απλούστευση (τη μείωση) όσο το δυνατόν περισσότερο του αριθμού των καταχωρίσεων υπηρεσιών (διαφορετικών «Sdi»). Αυτό ωστόσο πρέπει να εξισορροπηθεί με τη σωστή αναγνώριση των υπηρεσιών που σχετίζονται με την έκδοση QC και με την παροχή των εμπιστευμένων πληροφοριών σχετικά με το αν τα εν λόγω QC υποστηρίζονται από SSCD όταν οι πληροφορίες αυτές απουσιάζουν από το εκδοθέν QC.

▼C1

Θεωρητικά, η χρήση του πεδίου «Sie» και της επέκτασης «Qualification» (Αναγνώριση) πρέπει να περιορίζεται (αυστηρά) σε εκείνες τις συγκεκριμένες περιπτώσεις που επιλύονται με αυτό τον τρόπο, καθώς τα QC πρέπει να περιλαμβάνουν επαρκείς πληροφορίες όσον αφορά την υποστηριζόμενη κατάσταση αναγνώρισης και την υποστηριζόμενη υποστήριξη ή μη από μια SSCD.

Τα κράτη μέλη πρέπει, στο μέτρο του δυνατού, να ενισχύσουν την υιοθέτηση και τη χρήση διαλειτουργικών προφίλ QC.

3. **Δομή του κοινού σχεδιοτύπου για τον κατάλογο εμπίστευσης**

Το προτεινόμενο κοινό σχεδιότυπο για έναν κατάλογο εμπίστευσης των κρατών μελών θα είναι δομημένο σύμφωνα με τις παρακάτω κατηγορίες πληροφοριών:

1. πληροφορίες σχετικά με τον κατάλογο εμπίστευσης και το σχήμα έκδοσής του·

2. μια αλληλουχία πεδίων που διαθέτουν αδιαμφισβήτητες πληροφορίες ταυτότητας σχετικά με κάθε εποπτευόμενο/διαπιστευμένο CSP σύμφωνα με το σχήμα (η εν λόγω αλληλουχία είναι προαιρετική, δηλαδή όταν δεν χρησιμοποιείται, ο κατάλογος θα θεωρείται ότι είναι κενός, πράγμα που σημαίνει ότι κανένας CSP ούτε εποπτεύεται ούτε διαπιστεύεται στο σχετικό κράτος μέλος στο πλαίσιο του καταλόγου εμπίστευσης·

3. για κάθε καταγεγραμμένο CSP, μια αλληλουχία πεδίων με αδιαμφισβήτητες πληροφορίες ταυτότητας μιας εποπτευόμενης/διαπιστευμένης υπηρεσίας πιστοποίησης που παρέχει ο CSP (αυτή η αλληλουχία πρέπει να έχει τουλάχιστον μία καταχώριση)·

4. για έκαστη καταγεγραμμένη εποπτευόμενη/διαπιστευμένη υπηρεσία πιστοποίησης, αναγνώριση της τρέχουσας κατάστασης της υπηρεσίας και του ιστορικού της εν λόγω κατάστασης.

Στο πλαίσιο ενός CSP που εκδίδει QC, η αδιαμφισβήτητη ταυτοποίηση μιας εποπτευόμενης/διαπιστευμένης υπηρεσίας πιστοποίησης προς καταγραφή πρέπει να λαμβάνει υπόψη τις καταστάσεις εκείνες κατά τις οποίες δεν είναι διαθέσιμες αρκετές πληροφορίες στο αναγνωρισμένο πιστοποιητικό σχετικά με την «αναγνωρισμένη» κατάστασή του, την ενδεχόμενη υποστήριξή του από μια SSCD και ειδικά προκειμένου να αντιμετωπιστεί το επιπλέον γεγονός ότι οι περισσότεροι από τους (εμπορικούς) CSP χρησιμοποιούν μια ενιαία αναγνωρισμένη εκδίδουσα αρχή πιστοποίησης για την έκδοση πολλών τύπων πιστοποιητικών για οντότητες-τελικούς αποδέκτες, αναγνωρισμένων και μη.

Ο αριθμός καταχωρίσεων στον κατάλογο ανά αναγνωρισμένο CSP μπορεί να μειωθεί σε περιπτώσεις όπου υπάρχουν μια ή περισσότερες υπηρεσίες αρχής πιστοποίησης ανώτερης βαθμίδας, π.χ. στο πλαίσιο μιας εμπορικής ιεραρχίας αρχών πιστοποίησης από μια αρχή πιστοποίησης βάσης μέχρι εκδίδουσες αρχές πιστοποίησης. Ωστόσο, ακόμη και σε αυτές τις περιπτώσεις, πρέπει να διατηρηθεί και να διασφαλιστεί η αρχή διασφάλισης του αδιαμφισβήτητου δεσμού μεταξύ μιας υπηρεσίας πιστοποίησης CSP_{QC} και του συνόλου πιστοποιητικών που πρέπει να αναγνωριστούν ως QC.

1. *Πληροφορίες σχετικά με τον κατάλογο εμπίστευσης και το σχήμα έκδοσής του.*

Οι παρακάτω πληροφορίες θα αποτελούν μέρος αυτής της κατηγορίας:

— μια **ετικέτα** καταλόγου εμπίστευσης, η οποία θα διευκολύνει την ταυτοποίηση του καταλόγου εμπίστευσης κατά τις ηλεκτρονικές αναζητήσεις και επίσης θα επιβεβαιώνει τους σκοπούς της όταν θα έχει μορφή με δυνατότητα ανάγνωσης από άνθρωπο,

— **ένα αναγνωριστικό μορφής και έκδοσης μορφής** καταλόγου εμπίστευσης,

— **ένας αριθμός αλληλουχίας (ή έγκρισης)** καταλόγου εμπίστευσης,

— **ένας τύπος πληροφοριών** καταλόγου εμπίστευσης (π.χ. για αναγνώριση του ότι ο εν λόγω έμπιστος κατάλογος παρέχει πληροφορίες σχετικά με την κατάσταση εποπτείας/διαπίστευσης των υπηρεσιών πιστοποίησης από CSP που εποπτεύονται/διαπιστεύονται από το εκάστοτε κράτος μέλος ως προς τη συμμόρφωση με τις διατάξεις που ορίζονται στην οδηγία 1999/93/ΕΚ),

▼C1

— **πληροφορίες κατόχου** του καταλόγου εμπίστευσης (π.χ. ονοματεπώνυμο, διεύθυνση, στοιχεία επικοινωνίας κ.λπ. του φορέα του κράτους μέλους που είναι υπεύθυνος για την κατάρτιση, την ασφαλή δημοσίευση και την τήρηση του καταλόγου εμπίστευσης),

— **πληροφορίες σχετικά με το υπάρχον/υπάρχοντα σχήμα/σχήματα εποπτείας/διαπίστευσης** με τα οποία σχετίζεται ο κατάλογος εμπίστευσης, μεταξύ άλλων:

  — η χώρα όπου ισχύει,

  — πληροφορίες ή αναφορά στον τόπο όπου μπορούν να εντοπιστούν οι πληροφορίες για το σχήμα/τα σχήματα (μοντέλο σχήματος, κανόνες, κριτήρια, ισχύουσα κοινότητα, τύπος κ.λπ.),

  — διάστημα διατήρησης πληροφοριών (ιστορικού),

— **πολιτική ή/και νομική σημείωση, αστική ευθύνη, αρμοδιότητες** όσον αφορά τον κατάλογο εμπίστευσης,

— **ημερομηνία και χρόνος έκδοσης και επόμενη προβλεπόμενη ενημέρωση** του καταλόγου εμπίστευσης.

2. *Σαφείς πληροφορίες ταυτοποίησης για κάθε CSP που αναγνωρίζεται από το σχήμα*

Αυτό το σύνολο πληροφοριών θα συμπεριλαμβάνει τουλάχιστον τα εξής:

— την επωνυμία του οργανισμού του CSP όπως χρησιμοποιείται στις επίσημες καταγραφές στα μητρώα (ενδέχεται να συμπεριλαμβάνει το αναγνωριστικό χρήστη του οργανισμού του CSP, ανάλογα με τις πρακτικές του κράτους μέλους),

— τη διεύθυνση και τα στοιχεία επικοινωνίας του CSP,

— επιπλέον πληροφορίες σχετικά με τον CSP οι οποίες είτε συμπεριλαμβάνονται άμεσα είτε δι' αναφοράς σε έναν τόπο από όπου είναι δυνατή η μεταφόρτωση των εν λόγω πληροφοριών.

3. *Για κάθε καταγεγραμμένο CSP, μια σειρά πεδίων με σαφείς πληροφορίες ταυτότητας μιας υπηρεσίας πιστοποίησης που παρέχει ο CSP και που εποπτεύεται/διαπιστεύεται στο πλαίσιο της οδηγίας 1999/93/ΕΚ*

Αυτό το σύνολο πληροφοριών θα συμπεριλαμβάνει τουλάχιστον τα παρακάτω για κάθε υπηρεσία πιστοποίησης από έναν καταγεγραμμένο CSP:

— ένα αναγνωριστικό του τύπου της υπηρεσίας πιστοποίησης (π.χ. ένα αναγνωριστικό το οποίο δηλώνει ότι η εποπτευόμενη/διαπιστευμένη υπηρεσία πιστοποίησης από τον CSP είναι μια αρχή πιστοποίησης που εκδίδει QC),

— την (εμπορική) επωνυμία της εν λόγω υπηρεσίας πιστοποίησης,

— ένα σαφές μονοσήμαντο αναγνωριστικό της υπηρεσίας πιστοποίησης,

— επιπλέον πληροφορίες σχετικά με την υπηρεσία πιστοποίησης (π.χ. άμεση συμπερίληψη ή συμπερίληψη δι' αναφοράς σε μια τοποθεσία από όπου είναι δυνατή η μεταφόρτωση των πληροφοριών, πληροφορίες πρόσβασης όσον αφορά την υπηρεσία)

— για υπηρεσίες CA/QC, μια προαιρετική σειρά πλειάδων πληροφοριών, με κάθε πλειάδα να παρέχει

  i) κριτήρια, τα οποία θα χρησιμοποιούνται για την περαιτέρω αναγνώριση (φιλτράρισμα) στην αναγνωρισμένη υπηρεσία πιστοποίησης «Sdi» της υπηρεσίας εκείνης (δηλαδή του συνόλου αναγνωρισμένων πιστοποιητικών), για την οποία απαιτούνται/παρέχονται επιπλέον πληροφορίες, όσον αφορά την ένδειξη της υποστήριξης από SSCD (ή/και την έκδοση υπέρ ενός νομικού προσώπου) και

  ii) τους συναφείς «προσδιοριστές» που παρέχουν πληροφορίες για το αν το σύνολο αναγνωρισμένων πιστοποιητικών από αυτή την περαιτέρω αναγνωρισμένη υπηρεσία υποστηρίζεται ή όχι από μια SSCD ή/και πληροφορίες για το αν τα εν λόγω QC εκδίδονται υπέρ νομικού προσώπου (εξ ορισμού πρέπει να θεωρείται ότι εκδίδονται υπέρ φυσικών προσώπων).

▼C1

4. *Για έκαστη καταγεγραμμένη υπηρεσία πιστοποίησης, η αναγνώριση της τρέχουσας κατάστασης της υπηρεσίας και του ιστορικού της εν λόγω κατάστασης*

Αυτό το σύνολο πληροφοριών θα συμπεριλαμβάνει τουλάχιστον τα εξής:

— Ένα αναγνωριστικό της τρέχουσας κατάστασης

— Την ημερομηνία και την ώρα έναρξης της τρέχουσας κατάστασης

— Πληροφορίες ιστορικού για την εν λόγω κατάσταση.

4. **Ορισμοί και συντμήσεις**

Για τους σκοπούς του παρόντος εγγράφου, ισχύουν οι παρακάτω ορισμοί και ακρώνυμα:

Όρος	Ακρώνυμο	Ορισμός
Πάροχος υπηρεσιών πιστοποίησης	CSP	Όπως ορίζεται στο άρθρο 2 σημείο 11 της οδηγίας 1999/93/ΕΚ.
Αρχή πιστοποίησης	CA	Μια CA είναι ένας CSP και μπορεί να χρησιμοποιεί διάφορα τεχνικά ιδιωτικά κλειδιά υπογραφών της CA, καθένα εκ των οποίων διαθέτει ένα συνδεδεμένο πιστοποιητικό, προκειμένου να εκδίδει πιστοποιητικά για οντότητες-τελικούς αποδέκτες. Μια CA είναι μια αρχή την οποία εμπιστεύονται ένας ή περισσότεροι χρήστες για τη δημιουργία και τη χορήγηση πιστοποιητικών. Προαιρετικά, η αρχή πιστοποίησης μπορεί να δημιουργεί τα κλειδιά των χρηστών [ETSI TS 102 042]. Η CA θεωρείται ότι ταυτοποιείται μέσω των πληροφοριών ταυτοποίησης του πεδίου Εκδότης του πιστοποιητικού CA, το οποίο αφορά (την πιστοποίηση) του δημόσιου κλειδιού που συνδέεται με το ιδιωτικό κλειδί υπογραφών της CA και το οποίο ουσιαστικά χρησιμοποιεί η CA για να εκδίδει πιστοποιητικά για τις οντότητες. Μια CA μπορεί να έχει διάφορα κλειδιά υπογραφών. Κάθε κλειδί υπογραφής της CA ταυτοποιείται μέσω ενός μοναδικού αναγνωριστικού, το οποίο αποτελεί μέρος του πεδίου Authority Key Identifier (αναγνωριστικό κλειδιού αρχής) στο πιστοποιητικό της CA.
Αρχή πιστοποίησης που εκδίδει αναγνωρισμένα πιστοποιητικά	CA/QC	Μια CA η οποία πληροί τις απαιτήσεις που ορίζονται στο παράρτημα II της οδηγίας 1999/93/ΕΚ και εκδίδει αναγνωρισμένα πιστοποιητικά τα οποία πληρούν τις προϋποθέσεις που ορίζονται στο παράρτημα I της οδηγίας 1999/93/ΕΚ.
Πιστοποιητικό	Πιστοποιητικό	Όπως ορίζεται στο άρθρο 2 σημείο 9 της οδηγίας 1999/93/ΕΚ.
Αναγνωρισμένο πιστοποιητικό	QC	Όπως ορίζεται στο άρθρο 2 σημείο 10 της οδηγίας 1999/93/ΕΚ.
Υπογράφων	Υπογράφων	Όπως ορίζεται στο άρθρο 2 σημείο 3 της οδηγίας 1999/93/ΕΚ.
Εποπτεία	Εποπτεία	Η «εποπτεία» χρησιμοποιείται κατά την έννοια της οδηγίας 1999/93/ΕΚ (άρθρο 3 παράγραφος 3). Η οδηγία επιβάλλει στα κράτη μέλη να καθιερώσουν ένα κατάλληλο σύστημα, που καθιστά δυνατή την εποπτεία των εγκατεστημένων στο έδαφός τους CSP οι οποίοι εκδίδουν αναγνωρισμένα πιστοποιητικά για το κοινό, το οποίο να διασφαλίζει την εποπτεία της συμμόρφωσης με τις διατάξεις της οδηγίας.
Εθελοντική διαπίστευση	Διαπίστευση	Όπως ορίζεται στο άρθρο 2 σημείο 13 της οδηγίας 1999/93/ΕΚ.
Κατάλογος εμπίστευσης	TL	Ορίζει τον κατάλογο που υποδεικνύει την κατάσταση εποπτείας/διαπίστευσης των υπηρεσιών πιστοποίησης από παρόχους υπηρεσιών πιστοποίησης οι οποίοι εποπτεύονται/διαπιστεύονται από το σχετικό κράτος μέλος ως προς τη συμμόρφωση με τις σχετικές διατάξεις της οδηγίας 1999/93/ΕΚ.

▼C1

Όρος	Ακρώνυμο	Ορισμός
Κατάλογος κατάστασης υπηρεσιών εμπίστευσης	TSL	Μορφή υπογεγραμμένου καταλόγου ο οποίος χρησιμοποιείται ως βάση για την παρουσίαση πληροφοριών της κατάστασης των υπηρεσιών εμπίστευσης σύμφωνα με τις προδιαγραφές του ETSI TS 102 231.
Υπηρεσία εμπίστευσης		Υπηρεσία η οποία αυξάνει την αξιοπιστία των ηλεκτρονικών συναλλαγών και την εμπιστοσύνη σε αυτές (συνήθως, όχι όμως και απαραίτητα, με χρήση τεχνικών κρυπτογραφίας ή με συμπερίληψη απόρρητου υλικού) (ETSI TS 102 231).
Πάροχος υπηρεσιών εμπίστευσης	TSP	Φορέας ο οποίος παρέχει μία ή περισσότερες (ηλεκτρονικές) υπηρεσίες εμπίστευσης (ο όρος αυτός χρησιμοποιείται με ευρύτερη εφαρμογή απ' ό,τι ο CSP).
Αδειοδοτικό υπηρεσίας εμπίστευσης	TrST	Ένα φυσικό ή ψηφιακό (λογικό) αντικείμενο το οποίο δημιουργείται ή εκδίδεται ως αποτέλεσμα της χρήσης μιας υπηρεσίας εμπίστευσης. Παραδείγματα ψηφιακών TrST αποτελούν τα πιστοποιητικά, τα CRL, τα αδειοδοτικά χρονοσφράγισης και οι αποκρίσεις OCSP.
Αναγνωρισμένη ηλεκτρονική υπογραφή	QES	Μια AdES η οποία υποστηρίζεται από ένα QC και η οποία δημιουργείται από μια SSCD, όπως ορίζεται στο άρθρο 2 της οδηγίας 1999/93/ΕΚ.
Προηγμένη ηλεκτρονική υπογραφή	AdES	Όπως ορίζεται στο άρθρο 2 σημείο 2 της οδηγίας 1999/93/ΕΚ.
Προηγμένη ηλεκτρονική υπογραφή που υποστηρίζεται από αναγνωρισμένο πιστοποιητικό	$AdES_{QC}$	Νοείται μια ηλεκτρονική υπογραφή η οποία πληροί τις προϋποθέσεις μιας AdES και υποστηρίζεται από QC, όπως ορίζεται στο άρθρο 2 της οδηγίας 1999/93/ΕΚ.
Ασφαλής διάταξη δημιουργίας υπογραφής	SSCD	Όπως ορίζεται στο άρθρο 2 σημείο 6 της οδηγίας 1999/93/ΕΚ

ΚΕΦΑΛΑΙΟ I

ΑΝΑΛΥΤΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΕΝΟΣ ΚΟΙΝΟΥ ΣΧΕΔΙΟΤΥΠΟΥ ΓΙΑ ΤΟΝ «ΚΑΤΑΛΟΓΟ ΕΜΠΙΣΤΕΥΣΗΣ ΕΠΟΠΤΕ ΥΟΜΕΝΩΝ/ΔΙΑΠΙΣΤΕΥΜΕΝΩΝ ΠΑΡΟΧΩΝ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ»

Στο παρακάτω μέρος του εγγράφου, οι λέξεις-κλειδιά «ΠΡΕΠΕΙ ΝΑ», «ΔΕΝ ΠΡΕΠΕΙ ΝΑ», «ΑΠΑΙΤΕΙΤΑΙ», «ΘΑ ΠΡΕΠΕΙ ΝΑ», «ΔΕΝ ΘΑ ΠΡΕΠΕΙ ΝΑ», «ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ», «ΔΕΝ ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ», «ΣΥΝΙΣΤΑΤΑΙ ΝΑ», «ΔΥΝΑΤΑΙ ΝΑ» και «ΠΡΟΑΙΡΕΤΙΚΑ» πρέπει να ερμηνεύονται όπως περιγράφεται στο RFC (αίτηση για σχολιασμό) 2119 ([1]).

►M1 Οι παρούσες προδιαγραφές βασίζονται στις προδιαγραφές και τις απαιτήσεις που δηλώνονται στο ETSI TS 102 231 v.3.1.2. Όταν δεν δηλώνεται συγκεκριμένη απαίτηση στις παρούσες προδιαγραφές, ισχύουν εξ ολοκλήρου οι απαιτήσεις του ETSI TS 102 231 v.3.1.2. ◄ Όταν δηλώνονται συγκεκριμένες απαιτήσεις στις παρούσες προδιαγραφές, ΘΑ ΠΡΕΠΕΙ ΝΑ υπερισχύουν των αντίστοιχων απαιτήσεων του ETSI TS 102 231, ενώ θα συμπληρώνονται από τις προδιαγραφές μορφής που ορίζονται στο ETSI TS 102 231. Σε περίπτωση αποκλίσεων μεταξύ των εν λόγω προδιαγραφών από το ETSI TS 102 231, οι παρούσες προδιαγραφές ΘΑ ΠΡΕΠΕΙ ΝΑ έχουν κανονιστική ισχύ.

([1]) IETF RFC 2119: «Λέξεις κλειδιά για χρήση στις αιτήσεις για σχολιασμό, για να υποδείξουν τα επίπεδα συμμόρφωσης».

▼C1

ΘΑ ΠΡΕΠΕΙ ΝΑ εφαρμόζεται γλωσσική υποστήριξη και να παρέχεται τουλάχιστον στα αγγλικά (EN) και ενδεχομένως επιπρόσθετα στις γλώσσες μιας ή περισσότερων άλλων χωρών.

Η ένδειξη ημερομηνίας-ώρας ΘΑ ΠΡΕΠΕΙ ΝΑ συμμορφώνεται με τη διάταξη 5.1.4 του ETSI TS 102 231.

Η χρήση URI ΘΑ ΠΡΕΠΕΙ ΝΑ συμμορφώνεται με τη διάταξη 5.1.5 του ETSI TS 102 231.

Πληροφορίες σχετικά με το σχήμα έκδοσης του καταλόγου εμπίστευσης

Tag

TSL tag (διάταξη 5.2.1)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ συμμορφώνεται με τη διάταξη 5.2.1 του ETSI TS 102 231.

▼M1

_____

▼C1

Scheme Information

TSL version identifier (διάταξη 5.3.1)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ οριστεί στο «3» (ακέραιος αριθμός).

TSL sequence number (διάταξη 5.3.2)

▼M1

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ. ΚΑΘΟΡΙΖΕΙ τον αριθμό ακολουθίας του TSL. Ξεκινώντας από το «1» στην πρώτη έκδοση του TSL, αυτή η ακέραιη τιμή ΑΥΞΑΝΕΤΑΙ κατά 1 σε κάθε μετέπειτα έκδοση του TSL. ΔΕΝ ανακυκλώνεται σε «1» όταν εφαρμοστεί το προαναφερθέν πεδίο «TSL version identifier» (αναγνωριστικό έκδοσης TSL).

▼C1

TSL type (διάταξη 5.3.3)

▼M1

Αυτό το πεδίο ΑΠΑΙΤΕΙΤΑΙ για να καθοριστεί ο τύπος του TSL. ΟΡΙΖΕΤΑΙ σε http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/TSLType/generic (Generic).

▼C1

Σημείωση: Προκειμένου να υπάρξει συμμόρφωση με το ETSI TS 102 231, τη διάταξη 5.3.3, και να υποδειχθεί ο συγκεκριμένος τύπος TSL, κάνοντας αναφορά στην ύπαρξη των εκάστοτε προδιαγραφών που διέπουν την καθιέρωση της εφαρμογής του TSL του καταλόγου εμπίστευσης των κρατών μελών ([1]) και επιτρέποντας σε έναν κατατμητή να καθορίσει ποια μορφή οποιωνδήποτε από τα παρακάτω πεδία ([2]) είναι αναμενόμενη, σε περιπτώσεις κατά τις οποίες τα εν λόγω πεδία έχουν καθορισμένες (ή εναλλακτικές) έννοιες, ανάλογα με τον τύπο TSL στον οποίο αντιστοιχούν (στην προκειμένη περίπτωση, σε έναν κατάλογο εμπίστευσης ενός κράτους μέλους), το παραπάνω ειδικό URI ΘΑ ΠΡΕΠΕΙ ΝΑ καταγραφεί και να περιγραφεί ως εξής:

([1]) Δηλ. τον «κατάλογο κατάστασης εποπτείας/διαπίστευσης των υπηρεσιών πιστοποίησης από παρόχους υπηρεσιών πιστοποίησης οι οποίοι εποπτεύονται/διαπιστεύονται από το εκάστοτε κράτος μέλος για συμμόρφωση με τις σχετικές διατάξεις της οδηγίας 1999/93/ΕΚ» (εν συντομία «Κατάλογος εμπίστευσης»).

([2]) Δηλαδή, τα πεδία που καθορίζονται στο ETSI TS 102 231 – Ηλεκτρονικές Υπογραφές και Υποδομές (ESI): Παροχή εναρμονισμένων πληροφοριών κατάστασης υπηρεσιών εμπίστευσης και «καταγραφή προφίλ» από τις σημερινές προδιαγραφές για να καθοριστεί η κατάρτιση του καταλόγου εμπίστευσης των κρατών μελών.

▼M1

URI: (Generic) http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/-TSLType/generic

▼C1

Περιγραφή: Μια εφαρμογή TSL ενός καταλόγου κατάστασης εποπτείας/διαπίστευσης των υπηρεσιών πιστοποίησης από τους παρόχους υπηρεσιών πιστοποίησης, οι οποίοι εποπτεύονται/διαπιστεύονται από το εκάστοτε κράτος μέλος που είναι υπεύθυνο για την εφαρμογή του TSL σχετικά με τη συμμόρφωσή τους με τις σχετικές διατάξεις της οδηγίας 1999/93/ΕΚ για ηλεκτρονικές υπογραφές, μέσω μιας διαδικασίας άμεσου ελέγχου (εθελοντικού ή ρυθμιστικού).

Scheme operator name (διάταξη 5.3.4)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ. ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει την επωνυμία του φορέα του κράτους μέλους που είναι υπεύθυνος για την κατάρτιση, τη δημοσίευση και την τήρηση του εθνικού καταλόγου εμπίστευσης. ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει την επίσημη επωνυμία υπό την οποία λειτουργεί το συσχετιζόμενο νομικό πρόσωπο ή το εντεταλμένο νομικό πρόσωπο (π.χ., για κυβερνητικές διοικητικές υπηρεσίες) που συσχετίζεται με τον εν λόγω φορέα. ΠΡΕΠΕΙ ΝΑ είναι η επωνυμία που χρησιμοποιείται στις επίσημες εγγραφές σε μητρώα ή στην άδεια και εκείνη προς την οποία πρέπει να απευθύνεται κάθε επίσημη επικοινωνία. ΘΑ ΠΡΕΠΕΙ ΝΑ αποτελεί σειρά πολύγλωσσων στοιχειοσειρών και ΘΑ ΠΡΕΠΕΙ ΝΑ εφαρμοστεί με την αγγλική (EN) ως υποχρεωτική γλώσσα και με ενδεχομένως μια ή περισσότερες εθνικές γλώσσες.

Σημείωση: Μια χώρα ΔΥΝΑΤΑΙ ΝΑ διαθέτει χωριστούς φορείς εποπτείας και διαπίστευσης και ακόμη και συμπληρωματικούς φορείς για τυχόν επιχειρησιακές δραστηριότητες. ►M1 Απόκειται σε έκαστο κράτος μέλος να ορίσει τον Scheme operator για την εφαρμογή TSL του TL του κράτους μέλους. ◄ Αναμένεται ο φορέας εποπτείας, ο φορέας διαπίστευσης και ο υπεύθυνος σχήματος (όταν εμφανίζονται ως χωριστοί φορείς) να αναλάβουν έκαστος τις δικές του αρμοδιότητες και ευθύνες.

Οποιαδήποτε κατάσταση στην οποία πολλοί φορείς είναι υπεύθυνοι για την εποπτεία, τη διαπίστευση ή τις επιχειρησιακές πτυχές ΘΑ ΠΡΕΠΕΙ ΝΑ αντικατοπτρίζεται με συνέπεια και να αναγνωρίζεται ως τέτοια στις πληροφορίες σχήματος στο πλαίσιο του TL, συμπεριλαμβανομένων των πληροφοριών που αφορούν ειδικά το σχήμα, οι οποίες ορίζονται στο πεδίο «Scheme information URI» (URI πληροφοριών σχήματος) (διάταξη 5.3.7).

▼M1

Ο κατονομαζόμενος Scheme Operator (διάταξη 5.3.4) είναι ο φορέας που θα υπογράφει το TSL.

▼C1

Scheme operator address (διάταξη 5.3.5)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ. ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει τη διεύθυνση του νομικού προσώπου ή του εντεταλμένου οργανισμού που ορίζεται στο πεδίο «Scheme operator name» (διάταξη 5.3.4) τόσο για τις ταχυδρομικές όσο και για τις ηλεκτρονικές επικοινωνίες. ΘΑ ΠΡΕΠΕΙ ΝΑ συμπεριλαμβάνει την «PostalAddress» (δηλαδή οδό, τόπο, [πολιτεία ή επαρχία], [ταχυδρομικό κωδικό] και τον κωδικό χώρας ISO 3166-1 alpha-2), σύμφωνα με τη διάταξη 5.3.5.1 και την «ElectronicAddress» (δηλαδή διεύθυνση ηλεκτρονικού ταχυδρομείου ή/και URI διαδικτυακού τόπου), σύμφωνα με τη διάταξη 5.3.5.2.

Scheme name (διάταξη 5.3.6)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ, καθώς καθορίζει την ονομασία υπό την οποία λειτουργεί το σχήμα. ΘΑ ΠΡΕΠΕΙ ΝΑ αποτελεί αλληλουχία πολύγλωσσων στοιχειοσειρών (με υποχρεωτική γλώσσα την EN και με ενδεχομένως μια ή περισσότερες εθνικές γλώσσες) και ορίζεται όπως παρακάτω:

▼C1

— Η EN έκδοση ΘΑ ΠΡΕΠΕΙ ΝΑ είναι μια στοιχειοσειρά που να έχει την παρακάτω δομή:

CC:EN_name_value

όπου

— «CC» = ο κωδικός χώρας ISO 3166-1 alpha-2 που χρησιμοποιείται στο πεδίο «Scheme territory» (επικράτεια σχήματος) (διάταξη 5.3.10),

— «:» = χρησιμοποιείται ως ο διαχωριστής,

▼M1

— «EN_name_value» = «Supervision/Accreditation Status List of certification services from Certification Service Providers, which are supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC and its implementation in the referenced Member State's laws,»

▼C1

— Η έκδοση σε οποιαδήποτε επίσημη γλώσσα κάποιου κράτους μέλους ΘΑ ΠΡΕΠΕΙ ΝΑ είναι μια στοιχειοσειρά που να έχει την παρακάτω δομή:

CC:name_value

όπου

— «CC» = ο κωδικός χώρας ISO 3166-1 alpha-2 που χρησιμοποιείται στο πεδίο «Scheme territory» (επικράτεια σχήματος) (διάταξη 5.3.10),

— «:» = χρησιμοποιείται ως ο διαχωριστής,

— «name_value» = Επίσημη μετάφραση στην εθνική γλώσσα της παραπάνω «EN_name_value».

Η ονομασία του σχήματος είναι απαραίτητη για τη μονοσήμαντη ταυτοποίηση, βάσει της ονομασίας, του σχήματος που παρουσιάζεται στο «Scheme information URI», καθώς και για να διασφαλίσει ότι σε περίπτωση που ένας υπεύθυνος σχήματος λειτουργεί σε περισσότερα από ένα σχήματα, υπάρχει μια χωριστή ονομασία που δίνεται σε καθέναν εξ αυτών.

Τα κράτη μέλη και οι υπεύθυνοι σχήματος ΘΑ ΠΡΕΠΕΙ ΝΑ βεβαιωθούν ότι όταν ένα κράτος μέλος ή ένας υπεύθυνος σχήματος διαχειρίζεται περισσότερα από ένα σχήματα, σε καθένα εξ αυτών δίνεται χωριστή ονομασία.

Scheme information URI (διάταξη 5.3.7)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει το/τα URI από όπου οι χρήστες (τα εξαρτώμενα μέρη) μπορούν να λάβουν πληροφορίες για το σχήμα (με την EN ως υποχρεωτική γλώσσα και με ενδεχομένως μια ή περισσότερες εθνικές γλώσσες). Αυτό ΘΑ ΠΡΕΠΕΙ ΝΑ αποτελεί σειρά πολύγλωσσων δεικτών (με υποχρεωτική γλώσσα την EN και με ενδεχομένως μια ή περισσότερες εθνικές γλώσσες). Το/τα εκάστοτε URI ΠΡΕΠΕΙ ΝΑ παρέχουν μια διαδρομή προς πληροφορίες, οι οποίες αντιστοιχούν στην περιγραφή «κατάλληλες πληροφορίες για το σχήμα».

Οι «κατάλληλες πληροφορίες για το σχήμα» ΘΑ ΠΡΕΠΕΙ ΝΑ συμπεριλαμβάνουν τουλάχιστον:

— Τις γενικές εισαγωγικές πληροφορίες που θα είναι κοινές για όλα τα κράτη μέλη όσον αφορά το πεδίο εφαρμογής και το πλαίσιο του καταλόγου εμπίστευσης και το υπάρχον σχήμα/τα υπάρχοντα σχήματα εποπτείας/διαπίστευσης. Το κοινό κείμενο που πρέπει να χρησιμοποιηθεί είναι όπως παρακάτω:

▼C2

The present list is the TSL implementation of [*name of the relevant Member State*] 'Trusted List of supervised/accredited Certification Service Providers' providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The Trusted List aims at:

— listing and providing reliable information on the supervision/accreditation status of certification services from Certification Service Providers, who are supervised/accredited by [*name of the relevant Member State*] for compliance with the relevant provisions laid down in Directive 1999/93/EC;

— facilitating the validation of electronic signatures supported by those listed supervised/accredited certification services from the listed CSPs.

The Trusted List of a Member State provides a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 7.1(a)), including information on the QC supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

The CSPs issuing Qualified Certificates (QCs) listed here are supervised by [*name of the relevant Member State*] and may also be accredited for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). The applicable 'supervision' system (respectively 'voluntary accreditation' system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3.3, Art. 8.1, Art. 11 (respectively, Art.2.13, Art. 3.2, Art 7.1(a), Art. 8.1, Art. 11)

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) are included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.

▼C1

— Καθορισμένες πληροφορίες σχετικά με το υπάρχον σχήμα/τα υπάρχοντα σχήματα εποπτείας/διαπίστευσης, συγκεκριμένα ([1]):

— Πληροφορίες σχετικά με το σύστημα εποπτείας που ισχύει για κάθε CSP_{QC}

([1]) Τα δυο τελευταία σύνολα πληροφοριών είναι κρίσιμης σημασίας για τα μέρη που βασίζονται σε αυτά για να αξιολογήσουν την ποιότητα και το επίπεδο ασφαλείας των εν λόγω συστημάτων εποπτείας/διαπίστευσης. Τα εν λόγω σύνολα πληροφοριών θα πρέπει να παρέχονται σε επίπεδο καταλόγου εμπίστευσης μέσω της χρήσης του παρόντος «URI σχήματος πληροφοριών» (διάταξη 5.3.7 – πληροφορίες που παρέχει το κράτος μέλος), του «Τύπου σχήματος/κοινότητα/κανόνες» (διάταξη 5.3.9 – μέσω της χρήσης ενός κειμένου κοινού για όλα τα κράτη μέλη), της «Πολιτικής/νομικής σημείωσης TSL» (διάταξη 5.3.11 – κείμενο κοινό για όλα τα κράτη μέλη, το οποίο αναφέρεται στην οδηγία 1999/93/ΕΚ, μαζί με τη δυνατότητα κάθε κράτους μέλους να προσθέτει κείμενα/-παραπομπές που να αφορούν ειδικά το εκάστοτε κράτος μέλος). Επιπλέον πληροφορίες σχετικά με τα συστήματα εποπτείας/διαπίστευσης για τους CSP που δεν εκδίδουν QC μπορούν να παρέχονται σε επίπεδο υπηρεσίας, όταν ισχύουν και όταν είναι απαραίτητες (π.χ. για να γίνεται διάκριση μεταξύ πολλών επιπέδων ποιότητας/ασφάλειας) μέσω της χρήσης του «URI ορισμού υπηρεσίας σχήματος» (διάταξη 5.5.6).

▼C1

— Πληροφορίες, όταν υπάρχουν, για το εθνικό σχήμα εθελοντικής διαπίστευσης που ισχύει για κάθε CSP_{QC}

— Πληροφορίες, όταν υπάρχουν, για το σύστημα εποπτείας που ισχύει για κάθε CSP που δεν εκδίδει QC

— Πληροφορίες, όταν υπάρχουν, για το εθνικό σχήμα εθελοντικής διαπίστευσης που ισχύει για κάθε CSP που δεν εκδίδει QC.

— Αυτές οι συγκεκριμένες πληροφορίες ΘΑ ΠΡΕΠΕΙ ΝΑ συμπεριλαμβάνουν, τουλάχιστον, για κάθε υπάρχον σχήμα από εκείνα που παρατίθενται παραπάνω:

— Γενική περιγραφή

— Πληροφορίες για τη διαδικασία που ακολουθείται από τον φορέα εποπτείας/διαπίστευσης για την εποπτεία/διαπίστευση των CSP και από τους CSP για να λάβουν την εποπτεία/διαπίστευση

— Πληροφορίες σχετικά με τα κριτήρια βάσει των οποίων εποπτεύονται/διαπιστεύονται οι CSP.

— Συγκεκριμένες πληροφορίες, όταν υπάρχουν, για την ειδική «αναγνώριση» που μπορεί να δικαιούνται να λάβουν κάποια από τα φυσικά ή ψηφιακά (λογικά) αντικείμενα που δημιουργούνται ή που εκδίδονται ως αποτέλεσμα της παροχής μιας υπηρεσίας πιστοποίησης, μια βάσει της συμμόρφωσής τους με τις διατάξεις και τις απαιτήσεις που ορίζονται σε εθνικό επίπεδο, συμπεριλαμβανομένης της έννοιας μιας τέτοιας «αναγνώρισης» και των σχετικών εθνικών διατάξεων και απαιτήσεων.

Επιπλέον ειδικές πληροφορίες ανά κράτος μέλος για το σχήμα ΔΥΝΑΤΑΙ ΝΑ παρέχονται εθελοντικά. Σε αυτές ΘΑ ΠΡΕΠΕΙ ΝΑ συμπεριλαμβάνονται:

— Πληροφορίες σχετικά με τα κριτήρια και τους κανόνες που χρησιμοποιούνται για την επιλογή υπεύθυνων για την εποπτεία/τη διαπίστευση και που ορίζουν πώς οι υπεύθυνοι αυτοί εποπτεύουν (ελέγχουν)/διαπιστεύουν (διερευνούν) τους CSP

— Λοιπά στοιχεία επικοινωνίας και γενικές πληροφορίες που ισχύουν για τη λειτουργία του σχήματος.

Status determination approach (διάταξη 5.3.8)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει το αναγνωριστικό της προσέγγισης καθορισμού κατάστασης. Το παρακάτω ειδικό URI ΘΑ ΠΡΕΠΕΙ ΝΑ χρησιμοποιηθεί όπως καταγράφεται και περιγράφεται παρακάτω:

URI: http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/StatusDetn/-appropriate

Περιγραφή: Η κατάσταση των καταγεγραμμένων υπηρεσιών καθορίζεται από ή εκ μέρους του υπεύθυνου σχήματος στο πλαίσιο ενός κατάλληλου συστήματος για κάθε κράτος μέλος που προβλέπει «εποπτεία» (και, όταν ισχύει, «εθελοντική διαπίστευση») των παρόχων υπηρεσιών πιστοποίησης οι οποίοι είναι εγκατεστημένοι στην επικράτειά του (ή είναι εγκατεστημένοι σε μια τρίτη χώρα στην περίπτωση της «εθελοντικής διαπίστευσης») και εκδίδουν αναγνωρισμένα πιστοποιητικά για το κοινό, σύμφωνα με το άρθρο 3 παράγραφος 3 [αντίστοιχα, το άρθρο 3 παράγραφος 2 ή το άρθρο 7 παράγραφος 1 στοιχείο α)] της οδηγίας 1999/93/ΕΚ και, όταν ισχύει, που προβλέπει την «εποπτεία»/«εθελοντική διαπίστευση» των παρόχων υπηρεσιών διαπίστευσης, οι οποίοι δεν εκδίδουν αναγνωρισμένα πιστοποιητικά, σύμφωνα με ένα καθορισμένο και καθιερωμένο σε εθνικό επίπεδο «αναγνωρισμένο σχήμα/αναγνωρισμένα σχήματα έγκρισης», το οποίο εφαρμόζεται σε εθνική βάση για την εποπτεία της συμμόρφωσης των υπηρεσιών από CSP που δεν εκδίδουν QC με τις διατάξεις που ορίζει η οδηγία 1999/93/ΕΚ και που ενδεχομένως επεκτείνονται με εθνικές διατάξεις όσον αφορά την παροχή των εν λόγω υπηρεσιών πιστοποίησης.

▼C1

Scheme type/community/rules (διάταξη 5.3.9)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ περιέχει τουλάχιστον τα παρακάτω καταγεγραμμένα URI:

— Ένα URI κοινό για τους καταλόγους εμπίστευσης όλων των κρατών μελών, το οποίο οδηγεί σε ένα περιγραφικό κείμενο το οποίο ΘΑ ΠΡΕΠΕΙ ΝΑ ισχύει για όλους τους TL:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/common

— Μέσω του οποίου δηλώνεται συμμετοχή του σχήματος του κράτους μέλους (το οποίο αναγνωρίζεται μέσω του «TSL type» (διάταξη 5.3.3) και του «Scheme name» (διάταξη 5.3.6) σε ένα σχήμα σχημάτων (δηλαδή μια καταγραφή TSL οδηγεί σε όλα τα κράτη μέλη που δημοσιεύουν και διατηρούν TL υπό τη μορφή TSL)

— Όπου οι χρήστες μπορούν να λάβουν πολιτική/κανόνες βάσει των οποίων ΘΑ ΠΡΕΠΕΙ ΝΑ αξιολογούνται οι υπηρεσίες που συμπεριλαμβάνονται στον κατάλογο και από το οποίο θα μπορεί να καθοριστεί ο τύπος του TSL (βλέπε διάταξη 5.3.3)

— Όπου οι χρήστες μπορούν να λάβουν μια περιγραφή σχετικά με το πώς να χρησιμοποιούν και να ερμηνεύουν το περιεχόμενο της εφαρμογής TSL του καταλόγου εμπίστευσης. Οι εν λόγω κανόνες χρήσης ΘΑ ΠΡΕΠΕΙ ΝΑ είναι κοινοί για τους έμπιστους καταλόγους όλων των κρατών μελών, ανεξάρτητα από τον τύπο της καταγεγραμμένης υπηρεσίας και ανεξάρτητα από το σύστημα/συστήματα εποπτείας/διαπίστευσης.

Περιγραφικό κείμενο:

▼C2

Participation in a scheme

Each Member State must create a 'Trusted List of supervised/accredited Certification Service Providers' providing information about the supervision/accreditation status of certification services from Certification Service Providers (CSPs) who are supervised/accredited by the relevant Member State for compliance with the relevant provisions of Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

The present TSL implementation of such Trusted Lists is also to be referred to in the list of links (pointers) towards each Member State's TSL implementation of their Trusted List, compiled by the European Commission.

Policy/rules for the assessment of the listed services

The Trusted List of a Member State must provide a minimum of information on supervised/accredited CSPs issuing Qualified Certificates in accordance with the provisions laid down in Directive 1999/93/EC (Art. 3.3, 3.2 and Art. 7.1(a)), including information on the Qualified Certificate (QC) supporting the electronic signature and whether the signature is or not created by a Secure Signature Creation Device.

▼C2

The CSPs issuing Qualified Certificates (QCs) must be supervised by the Member State in which they are established (if they are established in a Member State), and may also be accredited, for compliance with the provisions laid down in Directive 1999/93/EC, including with the requirements of Annex I (requirements for QCs), and those of Annex II (requirements for CSPs issuing QCs). CSPs issuing QCs that are accredited in a Member State must still fall under the appropriate supervision system of that Member State unless they are not established in that Member State. The applicable 'supervision' system (respectively 'voluntary accreditation' system) is defined and must meet the relevant requirements of Directive 1999/93/EC, in particular those laid down in Art. 3.3, Art. 8.1, Art. 11 (respectively, Art.2.13, Art. 3.2, Art 7.1(a), Art. 8.1, Art. 11)

Additional information on other supervised/accredited CSPs not issuing QCs but providing services related to electronic signatures (e.g. CSP providing Time Stamping Services and issuing Time Stamp Tokens, CSP issuing non-Qualified certificates, etc.) may be included in the Trusted List and the present TSL implementation at a national level on a voluntary basis.

CSPs not issuing QCs but providing ancillary services, may fall under a 'voluntary accreditation' system (as defined in and in compliance with Directive 1999/93/EC) and/or under a nationally defined 'recognised approval scheme' implemented on a national basis for the supervision of compliance with the provisions laid down in Directive 1999/93/EC and possibly with national provisions with regard to the provision of certification services (in the sense of Art. 2.11 of the Directive). Some of the physical or binary (logical) objects generated or issued as a result of the provision of a certification service may be entitled to receive a specific 'qualification' on the basis of their compliance with the provisions and requirements laid down at national level but the meaning of such a 'qualification' is likely to be limited solely to the national level.

Interpretation of the TSL implementation of the Trusted List

The **general user guidelines** for electronic signature applications, services or products relying on a TSL implementation of a Trusted List according to the Annex of Commission Decision [reference to the present Decision] are as follows:

A 'CA/QC''Service type identifier' ('Sti') entry (similarly a CA/QC entry further qualified as being a 'RootCA/QC' through the use of 'Service information extension' ('Sie') additionalServiceInformation extension)

— indicates that from the 'Service digital identifier' ('Sdi') identified CA (similarly within the CA hierarchy starting from the 'Sdi' identified RootCA) from the corresponding CSP (see associated TSP information fields), all issued end-entity certificates are Qualified Certificates (QCs) **provided** that it is claimed as such in the certificate through the use of appropriate ETSI TS 101 862 defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI TS 101 456 defined QCP(+) OIDs (and this is guaranteed by the issuing CSP and ensured by the Member State Supervisory/Accreditation Body)

▼C2

Note: if no ‘Sie’ ‘Qualification’ information is present or if an end-entity certificate that is claimed to be a QC is not ‘further identified’ through a related ‘Sie’ entry, then the ‘machine-processable’ information to be found in the QC is supervised/accredited to be accurate. That means that the usage (or not) of the appropriate ETSI defined QcStatements (i.e. QcC, QcSSCD) and/or ETSI defined QCP(+) OIDs is ensured to be in accordance with what it is claimed by the CSP issuing QCs.

— **and IF**‘Sie’‘Qualification’å information is present, then in addition to the above default usage interpretation rule, those certificates that are identified through the use of this ‘Sie’ ‘Qualification’ entry, which is constructed on the principle of a sequence of ‘filters’ further identifying a set of certificates, must be considered according to the associated ‘qualifiers’ providing some additional information regarding ‘SSCD support’ and/or ‘Legal person as subject’ (e.g. those certificates containing a specific OID in the Certificate Policy extension, and/or having a specific ‘Key usage’ pattern, and/or filtered through the use of a specific value to appear in one specific certificate field or extension, etc.). Those qualifiers are part of the following set of ‘qualifiers’ used to compensate for the lack of information in the corresponding QC content, and that are used respectively:

— to indicate the nature of the SSCD support:

— ‘QCWithSSCD’ qualifier value meaning ‘QC supported by an SSCD’, or

— ‘QCNoSSCD’ qualifier value meaning ‘QC not supported by an SSCD’, or

— ‘QCSSCDStatusAsInCert’ qualifier value meaning that the SSCD support information is ensured to be contained in any QC under the ‘Sdi’-‘Sie’ provided information in this CA/QC entry;

AND/OR

— to indicate issuance to Legal Person:

— ‘QCForLegalPerson’ qualifier value meaning ‘Certificate issued to a Legal Person’

The general interpretation rule for any other ‘Sti’ type entry is that the listed service named according to the ‘Sn’ field value and uniquely identified by the ‘Sdi’ field value has a current supervision/accreditation status according to the ‘Scs’ field value as from the date indicated in the ‘Current status starting date and time’. Specific interpretation rules for any additional information with regard to a listed service (e.g. ‘Service information extensions’ field) may be found, when applicable, in the Member State specific URI as part of the present ‘Scheme type/community/rules’ field.

Please refer to the Technical specifications for a Common Template for the ‘Trusted List of supervised/accredited Certification Service Providers’ in the Annex of Commission Decision [reference to the actual Decision] for further details on the fields, description and meaning for the TSL implementation of the Member States’ Trusted Lists.

▼C1

— Ένα URI ειδικά για τον κατάλογο εμπίστευσης έκαστου κράτους μέλους, το οποίο οδηγεί σε ένα περιγραφικό κείμενο το οποίο ΘΑ ΠΡΕΠΕΙ ΝΑ ισχύει για τον TL του εν λόγω κράτους μέλους:

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/schemerules/CC

όπου «CC» = ο κωδικός χώρας ISO 3166-1 alpha-2 που χρησιμοποιείται στο πεδίο «Scheme territory» (επικράτεια σχήματος) (διάταξη 5.3.10).

— Σε περιπτώσεις κατά τις οποίες οι χρήστες μπορούν να λάβουν τη συγκεκριμένη πολιτική/τους κανόνες του εκάστοτε κράτους μέλους έναντι των οποίων ΘΑ ΠΡΕΠΕΙ ΝΑ αξιολογηθούν οι υπηρεσίες που συμπεριλαμβάνονται στον κατάλογο, προκειμένου να διαπιστωθεί η συμμόρφωσή τους με το κατάλληλο σύστημα εποπτείας και τα σχήματα εθελοντικής διαπίστευσης του κράτους μέλους.

— Σε περιπτώσεις κατά τις οποίες οι χρήστες μπορούν να λάβουν τη συγκεκριμένη περιγραφή του εκάστοτε κράτους μέλους σχετικά με το πώς να χρησιμοποιήσουν και να ερμηνεύσουν το περιεχόμενο της εφαρμογής TSL του καταλόγου εμπίστευσης όσον αφορά τις υπηρεσίες πιστοποίησης που δεν σχετίζονται με την έκδοση QC. Αυτό μπορεί να χρησιμοποιηθεί για να υποδείξει μια πιθανή λεπτομερή ανάλυση των εθνικών συστημάτων εποπτείας/διαπίστευσης που συσχετίζονται με τους CSP που δεν εκδίδουν QC και το πώς χρησιμοποιούνται για αυτό το σκοπό τα πεδία «Scheme service definition URI» (URI ορισμού υπηρεσίας σχήματος) (διάταξη 5.5.6) και «Service information extension» (επέκταση πληροφοριών υπηρεσίας).

Τα κράτη μέλη ΔΥΝΑΝΤΑΙ ΝΑ καθορίσουν επιπλέον URI από το παραπάνω αποκλειστικό ανά κράτος μέλος URI (δηλαδή URI τα οποία καθορίζονται από αυτό το ιεραρχικά αποκλειστικό URI).

Scheme territory (διάταξη 5.3.10)

Στο πλαίσιο των σημερινών προδιαγραφών, το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει τη χώρα όπου καθιερώνεται το σχήμα (ISO 3166-1 alpha-2 κωδικός χώρας).

TSL policy/legal notice (διάταξη 5.3.11)

Στο πλαίσιο των σημερινών προδιαγραφών, το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει την πολιτική του σχήματος ή να παρέχει ένα σημείωμα όσον αφορά το νομικό καθεστώς του σχήματος ή τις νομικές προϋποθέσεις που πληροί το σχήμα όσον αφορά τη δικαιοδοσία στην οποία είναι εγκατεστημένο το σχήμα ή/και τυχόν περιορισμούς και όρους υπό τους οποίους τηρείται και δημοσιεύεται ο TL.

Αυτό ΘΑ ΠΡΕΠΕΙ ΝΑ είναι μια είναι μια πολύγλωσση στοιχειοσειρά (απλό κείμενο) η οποία αποτελείται από δυο μέρη:

— Ένα πρώτο υποχρεωτικό μέρος, κοινό για τους TL όλων των κρατών μελών (με υποχρεωτική γλώσσα την EN και ενδεχομένως μια ή περισσότερες εθνικές γλώσσες), το οποίο υποδεικνύει ότι το ισχύον νομικό πλαίσιο είναι η οδηγία 1999/93/ΕΚ και η αντίστοιχη εφαρμογή της στους νόμους του κράτους μέλους που υποδεικνύεται στο πεδίο «Scheme Territory» (Επικράτεια σχήματος).

Αγγλική έκδοση του κοινού κειμένου:

The applicable legal framework for the present TSL implementation of the Trusted List of supervised/accredited Certification Service Providers for [name of the relevant Member State] is the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures and its implementation in [name of the relevant Member State] laws.

Το κείμενο στην επίσημη γλώσσα/στις επίσημες γλώσσες ενός κράτους μέλους: [επίσημη μετάφραση/επίσημες μεταφράσεις του παραπάνω αγγλικού κειμένου].

▼C1

— Το ισχύον νομικό πλαίσιο για την παρούσα εφαρμογή TSL του καταλόγου εμπίστευσης των εποπτευόμενων/διαπιστευμένων παρόχων υπηρεσιών πιστοποίησης για την/το [ονομασία του οικείου κράτους μέλους] είναι η οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές, καθώς και η εφαρμογή της στη νομοθεσία της/του [ονομασία του οικείου κράτους μέλους].

Ένα δεύτερο προαιρετικό μέρος, ειδικό για κάθε TL (με υποχρεωτική γλώσσα την EN και με ενδεχομένως μια ή περισσότερες εθνικές γλώσσες), το οποίο περιέχει παραπομπές σε συγκεκριμένα ισχύοντα εθνικά νομικά πλαίσια (π.χ. συγκεκριμένα όσον αφορά εθνικά σχήματα εποπτείας/διαπίστευσης για τους CSP που δεν εκδίδουν QC).

Historical information period (διάταξη 5.3.12)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ διευκρινίζει τη διάρκεια (ακέραιος αριθμός) κατά την οποία παρέχονται πληροφορίες ιστορικού στον TSL. Αυτή η ακέραιη τιμή πρέπει να παρέχεται σε συγκεκριμένο αριθμό ημερών και στο πλαίσιο των σημερινών προδιαγραφών ΘΑ ΠΡΕΠΕΙ ΝΑ είναι μεγαλύτερη ή ίση με 3 653 (πράγμα που σημαίνει ότι η εφαρμογή TSL του TL των κρατών μελών ΠΡΕΠΕΙ ΝΑ περιέχει πληροφορίες ιστορικού για τουλάχιστον δέκα χρόνια). Σε μεγαλύτερες τιμές πρέπει να λαμβάνονται υπόψη οι νομικές απαιτήσεις για τη διατήρηση δεδομένων στο κράτος μέλος που υποδεικνύεται στο «Scheme Territory» (διάταξη 5.3.10).

Pointers to other TSLs (διάταξη 5.3.13)

Στο πλαίσιο των σημερινών προδιαγραφών, το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ συμπεριλαμβάνει, όταν είναι διαθέσιμος, το δείκτη προς μια μορφή του κοινοτικού καταλόγου συνδέσμων (δεικτών) προς όλες τις εφαρμογές TSL των καταλόγων εμπίστευσης των κρατών μελών, η οποία συμμορφώνεται με το ETSI TS 102 231. Ισχύουν οι προδιαγραφές του ETSI TS 102 231, διάταξη 5.3.13, ενώ καθίσταται υποχρεωτική η χρήση της προαιρετικής ψηφιακής ταυτότητας, η οποία αντιστοιχεί στον εκδότη του TSL στον οποίο οδηγεί η παραπομπή, και θα έχει τη μορφή που ορίζεται στη διάταξη 5.5.3.

Σημείωση: Περιμένοντας την εφαρμογή της σύμμορφης με το ETSI TS 102 231 εφαρμογής του κοινοτικού καταλόγου συνδέσμων προς την εφαρμογή TSL από τα κράτη μέλη των δικών τους TL, αυτό το πεδίο ΔΕΝ ΘΑ ΠΡΕΠΕΙ ΝΑ χρησιμοποιηθεί.

List issue date and time (διάταξη 5.3.14)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει την ημερομηνία και την ώρα (UTC εκπεφρασμένη ως Zulu) έκδοσης του TSL χρησιμοποιώντας τιμή ημερομηνίας/ώρας όπως καθορίζεται στο ETSI TS 102 231, διάταξη 5.1.4.

Next update (διάταξη 5.3.15)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει την τελευταία ημερομηνία και ώρα (UTC εκπεφρασμένη ως Zulu) ως την οποία θα εκδοθεί το επόμενο TSL ή η οποία θα είναι μηδενική, υποδεικνύοντας κλειστό TSL (χρησιμοποιώντας τιμή ημερομηνίας/ώρας όπως καθορίζεται στο ETSI TS 102 231, διάταξη 5.1.4).

Σε περίπτωση που δεν σημειωθούν ενδιάμεσες αλλαγές κατάστασης σε τυχόν TSP ή υπηρεσία που καλύπτεται από το σχήμα, το TSL ΠΡΕΠΕΙ ΝΑ επανεκδοθεί ως ο χρόνος εκπνοής του τελευταίου εκδοθέντος TSL.

Στο πλαίσιο των σημερινών προδιαγραφών, η διαφορά μεταξύ της ημερομηνίας και ώρας για «Next update» και της «List issue date and time» ΔΕΝ ΘΑ ΠΡΕΠΕΙ ΝΑ υπερβαίνει τους **έξι (6)** μήνες.

▼C1

Distribution points (διάταξη 5.3.16)

Το πεδίο αυτό είναι ΠΡΟΑΙΡΕΤΙΚΟ. Αν χρησιμοποιηθεί ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει τους τόπους όπου δημοσιεύεται η τρέχουσα εφαρμογή TSL του TL και όπου βρίσκονται οι ενημερώσεις για το τρέχον TSL. Αν καθοριστούν πολλαπλά σημεία διανομής, ΠΡΕΠΕΙ ΝΑ παράσχουν όλα πανομοιότυπα αντίγραφα του τρέχοντος TSL ή της ενημερωμένης του έκδοσης. Το πεδίο αυτό, όταν χρησιμοποιείται, λαμβάνει τη μορφή μη κενής σειράς αλγορίθμων, καθένας εκ των οποίων είναι σύμμορφος με το RFC 3986 ([1]).

Scheme extensions (διάταξη 5.3.17)

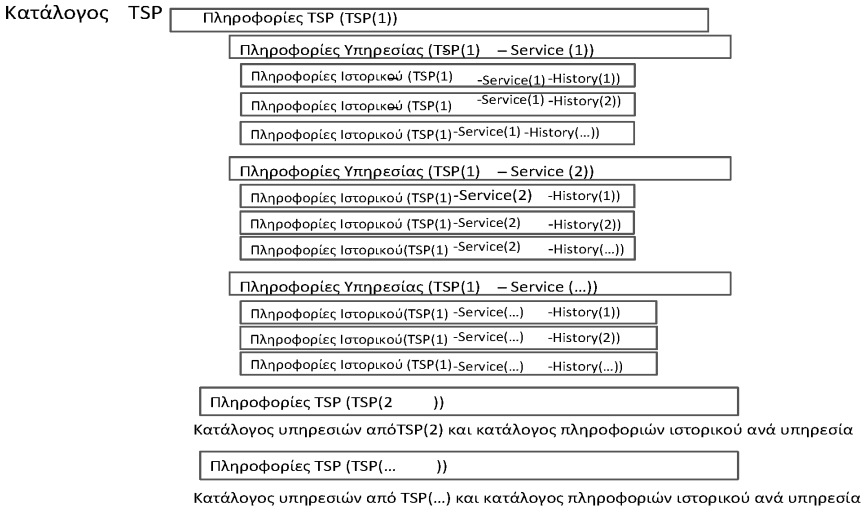
Το πεδίο αυτό είναι ΠΡΟΑΙΡΕΤΙΚΟ και δεν χρησιμοποιείται στο πλαίσιο της παρούσας προδιαγραφής.

List of Trust Service Providers

Το πεδίο αυτό είναι ΠΡΟΑΙΡΕΤΙΚΟ.

Σε περίπτωση που δεν υπάρχουν ή δεν υπήρχαν εποπτευόμενοι/διαπιστευμένοι CSP στο πλαίσιο του σχήματος σε ένα κράτος μέλος, το πεδίο αυτό ΘΑ ΠΡΕΠΕΙ ΝΑ απουσιάζει. Συμφωνείται, ωστόσο, ότι ακόμη κι όταν ένα κράτος μέλος δεν έχει CSP που να εποπτεύονται ή που να διαπιστεύονται από το σχήμα, τα κράτη μέλη ΘΑ ΠΡΕΠΕΙ ΝΑ θέσουν σε εφαρμογή ένα TSL με το πεδίο αυτό να απουσιάζει. Η απουσία CSP από τον κατάλογο ΘΑ ΠΡΕΠΕΙ ΝΑ σημαίνει ότι δεν υπάρχουν CSP που να εποπτεύονται/να διαπιστεύονται στη χώρα που ορίζεται στο πεδίο «Scheme Territory» (Επικράτεια σχήματος).

Σε περίπτωση που μια ή περισσότερες υπηρεσίες CSP εποπτεύονται/διαπιστεύονται τώρα ή κατά το παρελθόν από το σχήμα, τότε το πεδίο ΘΑ ΠΡΕΠΕΙ ΝΑ περιέχει μια αλληλουχία που να ορίζει έκαστο CSP ο οποίος παρέχει μια ή περισσότερες από τις εν λόγω εποπτευόμενες/διαπιστευμένες υπηρεσίες, με λεπτομέρειες σχετικά με την κατάσταση εποπτείας/διαπίστευσης και ιστορικό κατάστασης κάθε υπηρεσίας του CSP (TSP = CSP στο παρακάτω διάγραμμα).



([1]) IETF RFC 3986: «Ενιαία αναγνωριστικά πόρων (URI): Γενική σύνταξη».

▼C1

Ο κατάλογος TSP διαρθρώνεται όπως παρουσιάζεται στο παραπάνω διάγραμμα. Για κάθε TSP, υπάρχει μια αλληλουχία πεδίων που έχουν πληροφορίες για το TSP («TSP Information»), τα οποία ακολουθούνται από έναν κατάλογο υπηρεσιών. Για καθεμιά από τις εν λόγω καταγεγραμμένες υπηρεσίες, υπάρχει μια σειρά πεδίων που διαθέτουν πληροφορίες για την υπηρεσία («Service Information»), και μια σειρά πεδίων σχετικά με το ιστορικό της κατάστασης έγκρισης της υπηρεσίας («Service approval history»).

TSP Information

TSP(1)

T S P n a m e (διάταξη 5.4.1)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει την επωνυμία του **νομικού προσώπου** που είναι αρμόδιο για τις υπηρεσίες του CSP που εποπτεύονται ή διαπιστεύονται σήμερα ή παλαιότερα στο πλαίσιο του σχήματος. Αυτό αποτελεί σειρά πολύγλωσσων στοιχειοσειρών (με υποχρεωτική γλώσσα την EN και με ενδεχομένως μια ή περισσότερες εθνικές γλώσσες). Η επωνυμία αυτή ΠΡΕΠΕΙ ΝΑ είναι η επωνυμία που χρησιμοποιείται στις επίσημες εγγραφές σε μητρώα και εκείνη προς την οποία πρέπει να απευθύνεται κάθε επίσημη επικοινωνία.

T S P t r a d e n a m e (διάταξη 5.4.2)

Το πεδίο αυτό είναι ΠΡΟΑΙΡΕΤΙΚΟ και, αν υπάρχει, ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει μια εναλλακτική επωνυμία ταυτοποίησης του CSP σε ειδικό πλαίσιο της παροχής των υπηρεσιών του εκείνων που βρίσκονται στο εν λόγω TSL στο πεδίο καταχώρισης «TSP name» (επωνυμία TSL) (διάταξη 5.4.1).

Σημείωση: Σε περιπτώσεις κατά τις οποίες ένα μοναδικό νομικό πρόσωπο CSP παρέχει υπηρεσίες υπό διαφορετικές εμπορικές επωνυμίες ή υπό διαφορετικά συγκεκριμένα πλαίσια, μπορούν να υπάρχουν τόσες καταχωρίσεις CSP όσα και τα συγκεκριμένα πλαίσια (π.χ. καταχωρίσεις Επωνυμίας/Εμπορικής Επωνυμίας). Μια εναλλακτική είναι να παρατεθεί κάθε και όλοι οι CSP (νομικό πρόσωπο) μόνο μια φορά και να παρασχεθούν πληροφορίες για το συγκεκριμένο πλαίσιο παροχής υπηρεσιών. Είναι στη δικαιοδοσία του υπεύθυνου σχήματος έκαστου κράτους μέλους να συζητήσει και να συμφωνήσει με τον CSP ποια είναι η καταλληλότερη προσέγγιση.

T S P a d d r e s s (διάταξη 5.4.3)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει τη διεύθυνση του νομικού προσώπου ή του εντεταλμένου οργανισμού που ορίζεται στο πεδίο «TSP name» (διάταξη 5.4.1) τόσο για τις ταχυδρομικές όσο και για τις ηλεκτρονικές επικοινωνίες. ΘΑ ΠΡΕΠΕΙ ΝΑ συμπεριλαμβάνει την «PostalAddress» (δηλαδή οδό, τοποθεσία, [πολιτεία ή επαρχία], [ταχυδρομικό κωδικό] και τον κωδικό χώρας ISO 3166-1 alpha-2), σύμφωνα με τη διάταξη 5.3.5.1 και την «ElectronicAddress» (δηλαδή διεύθυνση ηλεκτρονικού ταχυδρομείου ή/και URI διαδικτυακού τόπου), σύμφωνα με τη διάταξη 5.3.5.2.

T S P i n f o r m a t i o n U R I (διάταξη 5.4.4)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίσει το/τα URI από όπου οι χρήστες (π.χ. τα εξαρτώμενα μέρη) μπορούν να λάβουν ειδικές πληροφορίες για τον CSP. Αυτό ΘΑ ΠΡΕΠΕΙ ΝΑ αποτελεί αλληλουχία πολύγλωσσων δεικτών (με υποχρεωτική γλώσσα την EN και με ενδεχομένως μια ή περισσότερες εθνικές γλώσσες). Το/τα καταγεγραμμένο(-α) URI ΠΡΕΠΕΙ ΝΑ παρέχουν μια διαδρομή προς πληροφορίες που περιγράφουν τους γενικούς όρους και συνθήκες του CSP, των πρακτικών του, των νομικών θεμάτων του, των πολιτικών εξυπηρέτησης πελατών του και άλλες γενικές πληροφορίες που εφαρμόζονται σε όλες τις υπηρεσίες του που καταγράφονται υπό την καταχώριση του εν λόγω CSP στο TSL.

Σημείωση: Σε περιπτώσεις κατά τις οποίες ένα μοναδικό νομικό πρόσωπο CSP παρέχει υπηρεσίες υπό διαφορετικές εμπορικές επωνυμίες ή υπό διαφορετικά ειδικά πλαίσια, και αυτό εμφανίζεται ως πολλές καταχωρίσεις TSP στα εν λόγω ειδικά πλαίσια, το πεδίο αυτό ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίσει πληροφορίες που αφορούν το συγκεκριμένο σύνολο υπηρεσιών που καταγράφονται υπό μια καθορισμένη καταχώριση TSP/TradeName.

▼C1

TSP information extensions (διάταξη 5.4.5)

Το πεδίο αυτό είναι ΠΡΟΑΙΡΕΤΙΚΟ και, αν υπάρχει, ΔΥΝΑΤΑΙ ΝΑ χρησιμοποιηθεί από τον υπεύθυνο σχήματος, σύμφωνα με τις προδιαγραφές ETSI TS 102 231 (διάταξη 5.4.5), προκειμένου να παράσχει ειδικές πληροφορίες, οι οποίες θα ερμηνευτούν σύμφωνα με τους κανόνες του καθορισμένου σχήματος.

List of Services

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ περιέχει μια σειρά που ταυτοποιεί καθεμιά από τις αναγνωρισμένες υπηρεσίες του CSP και την κατάσταση έγκρισης (και το ιστορικό αυτής της κατάστασης) της εν λόγω υπηρεσίας. Πρέπει να καταγραφεί τουλάχιστον μια υπηρεσία (ακόμα κι αν οι καταγεγραμμένες πληροφορίες αφορούν αποκλειστικά το ιστορικό).

Καθώς η συγκράτηση πληροφοριών ιστορικού σχετικά με τις καταγεγραμμένες υπηρεσίες ΑΠΑΙΤΕΙΤΑΙ ΝΑ γίνεται σύμφωνα με τις παρούσες προδιαγραφές, οι εν λόγω πληροφορίες ιστορικού ΠΡΕΠΕΙ ΝΑ διατηρούνται ακόμη κι αν η τρέχουσα κατάσταση της υπηρεσίας δεν απαιτεί κανονικά την καταγραφή τους (π.χ. αν η υπηρεσία ανασταλεί). Έτσι, ένας CSP ΠΡΕΠΕΙ ΝΑ συμπεριλαμβάνεται ακόμη κι αν η μοναδική καταγεγραμμένη υπηρεσία του βρίσκεται σε μια τέτοια κατάσταση, προκειμένου να διατηρηθεί το ιστορικό.

Service Information

►C2 *TSP(1) Service (1)* ◄

Service type identifier (διάταξη 5.5.1)

▼M1

Αυτό το πεδίο ΑΠΑΙΤΕΙΤΑΙ και καθορίζει το αναγνωριστικό του τύπου της υπηρεσίας, σύμφωνα με τον τύπο των τρεχουσών προδιαγραφών TSL (δηλαδή «/eSigDir-1999-93-EC-TrustedList/TSLType/generic»).

▼C1

Όταν η καταγεγραμμένη υπηρεσία συσχετίζεται με την έκδοση αναγνωρισμένων πιστοποιητικών, το καταγεγραμμένο URI ΘΑ ΠΡΕΠΕΙ ΝΑ είναι http://uri.etsi.org/TrstSvc/Svctype/CA/QC (μια αρχή πιστοποίησης που εκδίδει αναγνωρισμένα πιστοποιητικά).

Όταν η καταγεγραμμένη υπηρεσία συσχετίζεται με την έκδοση αδειοπλαισίων υπηρεσιών εμπιστοσύνης, τα οποία δεν είναι QC και δεν υποστηρίζουν την έκδοση QC, το εν λόγω URI ΘΑ ΠΡΕΠΕΙ ΝΑ είναι ένα από τα URI που ορίζονται στο ETSI 102 231 και που παρατίθενται στη διάταξή του D.2, η οποία αφορά αυτό το πεδίο. Αυτό ΘΑ ΠΡΕΠΕΙ ΝΑ ισχύει ακόμα και για εκείνα τα αδειοδοτικά υπηρεσιών εμπιστοσύνης τα οποία εποπτεύονται/διαπιστεύονται προκειμένου να πληρούν κάποιες συγκεκριμένες προϋποθέσεις, σύμφωνα με τους εθνικούς νόμους των κρατών μελών (π.χ. τα αποκαλούμενα αναγνωρισμένα αδειοδοτικά χρονοσφράγισης στα DE ή τα HU), το εν λόγω URI ΘΑ ΠΡΕΠΕΙ ΝΑ είναι ένα από τα URI που ορίζονται στο ETSI 102 231 και παρατίθενται στη διάταξή του D.2, η οποία αφορά αυτό το πεδίο (π.χ. TSA για τα εθνικά καθορισμένα αναγνωρισμένα αδειοδοτικά χρονοσφράγισης). Όταν ισχύει, η εν λόγω ειδική εθνική αναγνώριση των αδειοπλαισίων υπηρεσίας εμπιστοσύνης ΔΥΝΑΤΑΙ ΝΑ παρέχεται στην καταχώριση υπηρεσίας και η επέκταση additionalServiceInformation (διάταξη 5.8.2) στη διάταξη 5.5.9 («Service information extension» – επέκταση πληροφοριών υπηρεσίας) ΘΑ ΠΡΕΠΕΙ να χρησιμοποιηθεί για αυτό το σκοπό.

▼C1

Ως γενική εξ ορισμού αρχή, ΘΑ ΠΡΕΠΕΙ ΝΑ υπάρχει μία καταχώριση για κάθε πιστοποιητικό X.509v3 (π.χ. για μια υπηρεσία πιστοποίησης τύπου CA/QC) υπό τις καταγεγραμμένες υπηρεσίες πιστοποίησης από έναν CSP που είναι καταγεγραμμένος στον κατάλογο εμπίστευσης (π.χ., μια αρχή πιστοποίησης που εκδίδει QC (άμεσα). Σε κάποιες προσεκτικά σχεδιασμένες περιπτώσεις και υπό προσεκτικά ρυθμιζόμενες και επικυρωμένες συνθήκες, ο φορέας εποπτείας/-διαπίστευσης ενός κράτους μέλους ΔΥΝΑΤΑΙ ΝΑ αποφασίσει να χρησιμοποιήσει το πιστοποιητικό X.509v3 μιας αρχής πιστοποίησης βάσης ή ανώτερου επιπέδου (δηλαδή μιας αρχής πιστοποίησης η οποία δεν εκδίδει άμεσα QC για οντότητα-τελικό αποδέκτη, αλλά η οποία πιστοποιεί μια ιεραρχία αρχών πιστοποίησης μέχρι εκείνες τις αρχές που εκδίδουν QC στα τελικά νομικά πρόσωπα) ως το «Sdi» μιας ενιαίας καταχώρισης στον κατάλογο υπηρεσιών ενός καταγεγραμμένου CSP. Οι συνέπειες (υπέρ και κατά) της χρήσης του εν λόγω X.509v3 Αρχής Πιστοποίησης Βάσης ή Αρχής Πιστοποίησης Ανώτερης Βαθμίδας ως τιμή «Sdi» για τις καταχωρίσεις των υπηρεσιών του TL πρέπει να ληφθούν σοβαρά υπόψη και να αναληφθούν από τα κράτη μέλη [1].Επιπλέον, χρησιμοποιώντας αυτή την επιτρεπόμενη εξαίρεση από την εξ ορισμού αρχή, τα κράτη μέλη ΠΡΕΠΕΙ ΝΑ παρέχουν την τεκμηρίωση που απαιτείται για να διευκολυνθεί η δημιουργία και η επαλήθευση της διαδρομής πιστοποίησης.

Σημείωση: Οι TSP όπως οι αποκριτές OCSP και οι εκδότες CRL που αποτελούν μέρος των υπηρεσιών πιστοποίησης CSPQC και που υπόκεινται στη χρήση ξεχωριστών ζευγών κλειδιών για να υπογράψουν αντίστοιχα αποκρίσεις OCSP και CRL ΔΥΝΑΝΤΑΙ ΝΑ καταγράφονται επίσης στο παρόν σχεδιότυπο TSL, χρησιμοποιώντας τον παρακάτω συνδυασμό URI:

— Τιμή «Service type identifier» (αναγνωριστικό τύπου υπηρεσίας) (διάταξη 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP

σε συνδυασμό με την παρακάτω τιμή «Service information extension» (επέκταση πληροφοριών υπηρεσίας) (διάταξη 5.5.9) additionalServiceInformation extension (διάταξη 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/OCSP-QC

Περιγραφή: ένας πάροχος κατάστασης πιστοποιητικού, ο οποίος λειτουργεί ένα κεντρικό υπολογιστή OCSP ως μέρος μιας υπηρεσίας ενός CSP που εκδίδει αναγνωρισμένα πιστοποιητικά.

— Τιμή «Service type identifier» (αναγνωριστικό τύπου υπηρεσίας) (διάταξη 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL

σε συνδυασμό με την παρακάτω τιμή «Service information extension» (επέκταση πληροφοριών υπηρεσίας) (διάταξη 5.5.9) επέκταση additionalServiceInformation (διάταξη 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/CRL-QC

Περιγραφή: ένας πάροχος κατάστασης πιστοποιητικού, ο οποίος λειτουργεί CRL ως μέρος μιας υπηρεσίας ενός CSP που εκδίδει αναγνωρισμένα πιστοποιητικά.

— Τιμή «Service type identifier» (αναγνωριστικό τύπου υπηρεσίας) (διάταξη 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/CA/QC

[1] Η χρήση ενός πιστοποιητικού RootCA X.509v3 ως τιμή «Sdi» για μια καταγεγραμμένη υπηρεσία θα αναγκάσει τον υπεύθυνο του σχήματος να εξετάσει ολόκληρο το σύνολο υπηρεσιών ταυτοποίησης υπό το εν λόγω Root CA συνολικά όσον αφορά την «κατάσταση εποπτείας/διαπίστευσης». Π.χ., οποιαδήποτε αλλαγή κατάστασης που απαιτείται από μια μεμονωμένη CA υπό την καταγεγραμμένη ιεραρχία βάσης θα εξαναγκάσει ολόκληρη την ιεραρχία να επηρεαστεί από την εν λόγω αλλαγή κατάστασης.

▼C1

σε συνδυασμό με την παρακάτω τιμή «Service information extension» (επέκταση πληροφοριών υπηρεσίας) (διάταξη 5.5.9) additionalServiceInformation extension (διάταξη 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/RootCA-QC

Περιγραφή: μια αρχή πιστοποίησης βάσης από την οποία μπορεί να θεσπιστεί μια διαδρομή πιστοποίησης προς μια αρχή πιστοποίησης η οποία εκδίδει αναγνωρισμένα πιστοποιητικά.

— Τιμή «Service type identifier» (αναγνωριστικό τύπου υπηρεσίας) (διάταξη 5.5.1):

http://uri.etsi.org/TrstSvc/Svctype/TSA

σε συνδυασμό με την παρακάτω τιμή «Service information extension» (επέκταση πληροφοριών υπηρεσίας) (διάταξη 5.5.9) additionalServiceInformation extension (διάταξη 5.8.2):

http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/TSS-QC

Περιγραφή: μια υπηρεσία χρονοσφράγισης στο πλαίσιο μιας υπηρεσίας από έναν πάροχο υπηρεσιών πιστοποίησης, ο οποίος εκδίδει αναγνωρισμένα πιστοποιητικά, που εκδίδει TST που μπορεί να χρησιμοποιηθεί στη διαδικασία επαλήθευσης της αναγνωρισμένης υπογραφής, προκειμένου να εξακριβωθεί και να επεκταθεί η εγκυρότητα της υπογραφής μετά από την ανάκληση ή την εκπνοή του QC.

Service name (διάταξη 5.5.2)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζεται η ονομασία υπό την οποία ο CSP που ορίζεται στο πεδίο «TSP name» (διάταξη 5.4.1) παρέχει την υπηρεσία που ορίζεται στο πεδίο «Service type identifier» (διάταξη 5.5.1). Αυτό ΘΑ ΠΡΕΠΕΙ ΝΑ είναι μια σειρά πολύγλωσσων στοιχειοσειρών (με υποχρεωτική γλώσσα την EN και με ενδεχομένως μια ή περισσότερες εθνικές γλώσσες).

Service digital identity (διάταξη 5.5.3)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει τουλάχιστον μια απεικόνιση ενός ψηφιακού αναγνωριστικού μοναδικού για την υπηρεσία, ο τύπος της οποίας καθορίζεται στο πεδίο «Service type identifier» (διάταξη 5.5.1), με το οποίο η υπηρεσία μπορεί να ταυτοποιηθεί μοναδικά.

Στις παρούσες προδιαγραφές, το ψηφιακό αναγνωριστικό που χρησιμοποιείται σε αυτό το πεδίο ΘΑ ΠΡΕΠΕΙ ΝΑ είναι το σχετικό πιστοποιητικό X.509v3, το οποίο αποτελεί απεικόνιση του δημόσιου κλειδιού/των δημόσιων κλειδιών που χρησιμοποιεί ο CSP για να παράσχει την υπηρεσία, ο τύπος της οποίας καθορίζεται από το πεδίο «Service type identifier» (διάταξη 5.5.1) (δηλαδή το κλειδί που χρησιμοποιείται από μια RootCA/QC, το κλειδί που χρησιμοποιείται για την υπογραφή πιστοποιητικών ([1]), ή εναλλακτικά για την έκδοση αδειοπλαισίων χρονοσφράγισης, ή για την υπογραφή CRL, ή για την υπογραφή αποκρίσεων OCSP). Το εν λόγω συσχετιζόμενο πιστοποιητικό X.509v3 ΘΑ ΠΡΕΠΕΙ ΝΑ χρησιμοποιηθεί ως το ελάχιστο απαραίτητο ψηφιακό αναγνωριστικό (καθώς αποτελεί απεικόνιση του δημοσίου κλειδιού/των δημόσιων κλειδιών που χρησιμοποιεί ο CSP για να παρέχει την καταγεγραμμένη υπηρεσία). Επιπλέον αναγνωριστικά ΔΥΝΑΤΑΙ ΝΑ χρησιμοποιηθούν όπως παρακάτω, αλλά ΠΡΕΠΕΙ όλοι ΝΑ παραπέμπουν στην ίδια ταυτότητα (δηλαδή στο συσχετισμένο πιστοποιητικό X.509v3):

([1]) Αυτό μπορεί να είναι το πιστοποιητικό μιας CA που εκδίδει πιστοποιητικά για οντότητες-τελικούς αποδέκτες (π.χ. CA/PKC, CA/QC) ή το πιστοποιητικό μιας εμπιστευμένης CA βάσης από την οποία μπορεί να εντοπιστεί μια διαδρομή ως τα αναγνωρισμένα πιστοποιητικά για οντότητες-τελικούς αποδέκτες. Ανάλογα με το εάν οι πληροφορίες αυτές και οι πληροφορίες που βρίσκονται σε κάθε πιστοποιητικό για οντότητες-τελικούς αποδέκτες το οποίο εκδίδεται υπό την εν λόγω εμπιστευμένη αρχή βάσης μπορούν να χρησιμοποιηθούν για να καθορίσουν αδιαμφισβήτητα τα κατάλληλα χαρακτηριστικά οποιουδήποτε αναγνωρισμένου πιστοποιητικού, οι πληροφορίες αυτές («Service digital identity» - ψηφιακή ταυτότητα υπηρεσίας) ενδέχεται να πρέπει να συμπληρωθούν με δεδομένα «Service information extensions» (εκτεταμένα πεδία πληροφοριών υπηρεσίας) (βλέπε διάταξη 5.5.9).

▼C1

α) η διακριτική ονομασία (DN) του πιστοποιητικού η οποία μπορεί να χρησιμοποιηθεί για την επαλήθευση των ηλεκτρονικών υπογραφών της υπηρεσίας του CSP, η οποία καθορίζεται στο πεδίο «Service type identifier» (διάταξη 5.5.1)·

β) το σχετικό αναγνωριστικό δημοσίου κλειδιού (δηλαδή X.509v3 SubjectKeyIdentifier ή τιμή SKI)·

γ) Το σχετικό δημόσιο κλειδί.

Ως γενική εξ ορισμού αρχή, το ψηφιακό αναγνωριστικό (δηλαδή το σχετικό πιστοποιητικό X.509v3) ΔΕΝ ΘΑ ΠΡΕΠΕΙ να υπάρχει για περισσότερες από μια φορές στον κατάλογο εμπίστευσης, δηλαδή ΘΑ ΠΡΕΠΕΙ ΝΑ υπάρχει μια καταχώριση ανά πιστοποιητικό X.509v3 για μια υπηρεσία πιστοποίησης δυνάμει των καταγεγραμμένων υπηρεσιών πιστοποίησης από έναν CSP που είναι καταγεγραμμένος στον κατάλογο εμπίστευσης. Αντίθετα, ένα μεμονωμένο πιστοποιητικό X.509v3 ΘΑ ΠΡΕΠΕΙ ΝΑ χρησιμοποιηθεί σε μια μεμονωμένη καταχώριση υπηρεσίας ως η τιμή «Sdi».

Σημείωση (1): Η μοναδική περίπτωση στην οποία η παραπάνω γενική εξ ορισμού αρχή ενδέχεται να μην ισχύει είναι η κατάσταση κατά την οποία χρησιμοποιείται ένα μεμονωμένο πιστοποιητικό X.509v3 κατά την έκδοση διαφορετικών τύπων αδειοδοτικών χρονοσφράγισης για τους οποίους ισχύουν διαφορετικά σχήματα εποπτείας/διαπίστευσης, για παράδειγμα χρησιμοποιείται ένα μεμονωμένο πιστοποιητικό X.509v3 από έναν CSP αφενός μεν όταν εκδίδει αναγνωρισμένα πιστοποιητικά σύμφωνα με ένα κατάλληλο σύστημα εποπτείας, αφετέρου δε όταν εκδίδει μη αναγνωρισμένα πιστοποιητικά σύμφωνα με μια διαφορετική κατάσταση εποπτείας/διαπίστευσης. Σε αυτή την περίπτωση και σε αυτό το παράδειγμα μπορούν να χρησιμοποιηθούν δυο καταχωρίσεις με διαφορετικές τιμές «Sti» (π.χ. CA/QC και CA/PKC αντίστοιχα στο δεδομένο παράδειγμα) και με την ίδια τιμή «Sdi» (το σχετικό πιστοποιητικό X.509v3).

Οι εφαρμογές εξαρτώνται από το ASN.1 ή το XML και ΘΑ ΠΡΕΠΕΙ ΝΑ συμμορφώνονται με τις προδιαγραφές του ETSI TS 102 231 (για το ASN.1 βλέπε παράρτημα A του ETSI TS 102 231, και για το XML δείτε παράρτημα B του ETSI TS 102 231).

Σημείωση (2): Όταν πρέπει να παρασχεθούν επιπλέον πληροφορίες «αναγνώρισης» όσον αφορά την καταχώριση ταυτοποιημένης υπηρεσίας, τότε, όταν είναι κατάλληλο, ο υπεύθυνος σχήματος ΘΑ ΠΡΕΠΕΙ ΝΑ εξετάσει τη χρήση της επέκτασης «additionalServiceInformation» (διάταξη 5.8.2) του πεδίου «Service information extension» (διάταξη 5.5.9) ανάλογα με το σκοπό της παροχής των εν λόγω επιπλέον πληροφοριών «αναγνώρισης». Επιπλέον, ο υπεύθυνος σχήματος μπορεί προαιρετικά να χρησιμοποιήσει μια διάταξη 5.5.6 («Scheme service definition URI» – URI καθορισμού υπηρεσίας σχήματος).

Service current status (διάταξη 5.5.4)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει το αναγνωριστικό κατάστασης της υπηρεσίας μέσω ενός από τα παρακάτω URI:

▼C2

— **Under Supervision (Υπό εποπτεία)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/undersupervision),

— **Supervision of Service in Cessation (Εποπτεία υπηρεσίας υπό αναστολή)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/-supervisionincessation),

— **Supervision Ceased (Αναστολή εποπτείας)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionceased),

— **Supervision Revoked (Ανάκληση εποπτείας)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/supervisionrevoked),

— **Accredited (Διαπιστευμένη)** (http://uri.etsi.org/TrstSvc/Svcstatus/eSigDir-1999-93-EC-TrustedList/Svcstatus/accredited),

— **Accreditation Ceased (Αναστολή διαπίστευσης)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationceased),

— **Accreditation Revoked (Ανάκληση διαπίστευσης)** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/Svcstatus/accreditationrevoked).

▼C1

Οι παρακάτω καταστάσεις ΘΑ ΠΡΕΠΕΙ ΝΑ ερμηνευτούν στο πλαίσιο των εν λόγω προδιαγραφών του καταλόγου εμπίστευσης ως εξής:

— ***Υπό εποπτεία:*** Η υπηρεσία που ταυτοποιείται στο «Service digital identity» (διάταξη 5.5.3) την οποία παρέχει ο πάροχος υπηρεσίας ταυτοποίησης (CSP) που ορίζεται στο «TSP name» (διάταξη 5.4.1) βρίσκεται επί του παρόντος υπό εποπτεία, ως προς τη συμμόρφωση με τις διατάξεις που ορίζονται στην οδηγία 1999/93/ΕΚ, από το κράτος μέλος που ορίζεται στο πεδίο «Scheme territory» (διάταξη 5.3.10) στο οποίο καθορίζεται ο CSP.

▼M1

— ***Εποπτεία της υπηρεσίας υπό αναστολή:*** Η υπηρεσία που ορίζεται στο πεδίο «Service digital identity» (διάταξη 5.5.3) την οποία παρέχει ο CSP που ορίζεται στο πεδίο «TSP name» (διάταξη 5.4.1) είναι επί του παρόντος σε φάση αναστολής αλλά εξακολουθεί να εποπτεύεται έως ότου η εποπτεία είτε ανασταλεί είτε ανακληθεί. Σε περίπτωση που αναλάβει την ευθύνη της διασφάλισης της εν λόγω φάσης αναστολής διαφορετικό νομικό πρόσωπο από εκείνο που ορίζεται στο «TSP name», η ταυτοποίηση αυτού του νέου ή έκτακτου νομικού προσώπου (έκτακτος CSP) θα πρέπει να προβλέπεται από τον «Scheme service definition URI» (διάταξη 5.5.6) και από την επέκταση «TakenOverBy» (διάταξη L.3.2) της καταχώρισης υπηρεσίας.

▼C1

— ***Αναστολή εποπτείας:*** Η εγκυρότητα της αξιολόγησης εποπτείας έληξε χωρίς να έχει γίνει νέα αξιολόγηση της υπηρεσίας που ορίζεται στο πεδίο «Service digital identity» (διάταξη 5.5.3). Η υπηρεσία αυτή τη στιγμή δεν τελεί πλέον υπό εποπτεία από την ημερομηνία της τρέχουσας κατάστασης, καθώς γίνεται κατανοητό ότι η υπηρεσία έχει ανασταλεί.

— ***Ανάκληση εποπτείας:*** Η υπηρεσία του CSP και ενδεχομένως ο ίδιος ο CSP, ο οποίος εποπτευόταν κατά το παρελθόν, απέτυχε να εξακολουθήσει να συμμορφώνεται με τις διατάξεις που ορίζει η οδηγία 1999/93/ΕΚ, όπως ορίζεται από το κράτος μέλος που ορίζεται στο πεδίο «Scheme territory» (διάταξη 5.3.10) όπου είναι εγκατεστημένος ο CSP. Αναλόγως, η υπηρεσία αναγκάστηκε να αναστείλει τις δραστηριότητές της και πρέπει να θεωρείται ότι η παροχή της έχει ανασταλεί για τον παραπάνω λόγο.

Σημείωση (1): Η τιμή κατάστασης «Supervision Revoked» (ανάκληση εποπτείας) μπορεί να είναι μια οριστική κατάσταση, ακόμη κι αν ο CSP μετά διακόψει εντελώς τις δραστηριότητές του· δεν υπάρχει ανάγκη μετάβασης ούτε στην κατάσταση «Supervision of Service in Cessation» (Εποπτεία υπηρεσίας υπό αναστολή) ούτε στην κατάσταση «Supervision Ceased» (Αναστολή εποπτείας) σε αυτή την περίπτωση. Μάλιστα, ο μόνος τρόπος για να αλλάξει η κατάσταση «Supervision Revoked» (Ανάκληση εποπτείας) είναι να περάσει ο πάροχος από κατάσταση μη συμμόρφωσης σε κατάσταση συμμόρφωσης με τις διατάξεις που ορίζονται στην οδηγία 1999/93/ΕΚ, ανάλογα με το κατάλληλο σύστημα εποπτείας στο κράτος μέλος στο οποίο ανήκει ο TL, ανακτώντας έτσι την κατάσταση «Under Supervision» (υπό εποπτεία). Η κατάσταση «Supervision of Service in Cessation» (Εποπτεία υπηρεσίας υπό αναστολή) ή «Supervision Ceased» (Αναστολή εποπτείας) παρατηρείται μόνο όταν ένας CSP αναστέλλει άμεσα τις σχετικές εποπτευόμενες υπηρεσίες του, όχι όταν ανακαλείται η εποπτεία.

— ***Διαπιστευμένη:*** Ο φορέας διαπίστευσης πραγματοποίησε μια αξιολόγηση διαπίστευσης εκ μέρους του κράτους μέλους που ορίζεται στο πεδίο «Scheme territory» (Επικράτεια σχήματος) (διάταξη 5.3.10) και η υπηρεσία που ορίζεται στο πεδίο «Service digital identity» (διάταξη 5.5.3), την οποία παρέχει ο CSP ([1]) που ορίζεται στο πεδίο «TSP name» (διάταξη 5.4.1) διαπιστώνεται ότι συμμορφώνεται με τις διατάξεις της οδηγίας 1999/93/ΕΚ.

([1]) Σημειώστε ότι ο εν λόγω διαπιστευμένος CSP μπορεί να είναι εγκατεστημένος σε ένα άλλο κράτος μέλος από εκείνο που ορίζεται στο πεδίο «Scheme territory» (Επικράτεια σχήματος) για την υλοποίηση TSL του TL ή σε μια Τρίτη χώρα (βλέπε άρθρο 7 παράγραφος 1 στοιχείο α) της Οδηγίας 1999/93/ΕΚ).

▼C1

Σημείωση (2): Όταν χρησιμοποιείται στο πλαίσιο ενός CSP που εκδίδει QC, ο οποίος είναι εγκατεστημένος στο «Scheme territory» (διάταξη 5.3.10), ΠΡΕΠΕΙ ΝΑ εξεταστούν οι παρακάτω δυο καταστάσεις «Ανάκληση διαπίστευσης» και «Αναστολή διαπίστευσης» ως «μεταβατικές καταστάσεις» και ΔΕΝ ΠΡΕΠΕΙ ΝΑ χρησιμοποιηθούν ως τιμές για το πεδίο «Τρέχουσα κατάσταση υπηρεσίας», καθώς, σε περίπτωση που συμβεί κάτι τέτοιο, ΠΡΕΠΕΙ μια κατάσταση «Υπό εποπτεία» ΝΑ ακολουθήσει άμεσα τις «Πληροφορίες ιστορικού έγκρισης υπηρεσίας» ή στην «Τρέχουσα κατάσταση υπηρεσίας», την οποία ενδεχομένως θα ακολουθήσει μια άλλη οποιαδήποτε κατάσταση εποπτείας, η οποία ορίστηκε παραπάνω και παρουσιάζεται στο διάγραμμα 1. Όταν χρησιμοποιείται στο πλαίσιο ενός CSP που δεν εκδίδει QC, όταν υπάρχει μόνο ένα συσχετισμένο σχήμα «εθελοντικής διαπίστευσης» χωρίς συσχετισμένο σχήμα εποπτείας ή στο πλαίσιο ενός CSP που εκδίδει QC, όπου ο CSP δεν είναι εγκατεστημένος στο «Scheme territory» (διάταξη 5.3.10) (π.χ. σε τρίτη χώρα), οι καταστάσεις «Ανάκληση διαπίστευσης» και «Αναστολή διαπίστευσης» ΔΥΝΑΤΑΙ ΝΑ χρησιμοποιηθούν ως τιμή για την «Τρέχουσα κατάσταση υπηρεσίας»:

— ***Αναστολή διαπίστευσης:*** Η εγκυρότητα της αξιολόγησης διαπίστευσης έληξε χωρίς να έχει γίνει νέα αξιολόγηση της υπηρεσίας που ορίζεται στο πεδίο «Service digital identity» (διάταξη 5.5.3).

— ***Ανάκληση διαπίστευσης:*** Αν και παλαιότερα είχε διαπιστωθεί ότι η υπηρεσία που ορίζεται στο πεδίο «Service digital identity» (διάταξη 5.5.3) που παρέχεται από τον πάροχο υπηρεσιών πιστοποίησης (CSP) που ορίζεται στο πεδίο «TSP name» (διάταξη 5.4.1) ήταν σύμμορφη με τα κριτήρια του σχήματος, η εν λόγω υπηρεσία και ίσως και ο ίδιος ο CSP δεν κατάφεραν να εξακολουθήσουν να συμμορφώνονται με τις διατάξεις που ορίζονται στην οδηγία 1999/93/ΕΚ.

Σημείωση (3): Πρέπει να χρησιμοποιούνται ακριβώς οι ίδιες τιμές κατάστασης για τους CSP που εκδίδουν QC και για τους CSP που δεν εκδίδουν QC (π.χ. για τους παρόχους υπηρεσιών χρονοσφράγισης που εκδίδουν TST, τους CSP που εκδίδουν μη αναγνωρισμένα πιστοποιητικά κ.λπ.). Το «Service Type identifier» (διάταξη 5.5.1) θα πρέπει να χρησιμοποιηθεί για να γίνει διάκριση μεταξύ των ισχυόντων συστημάτων εποπτείας/διαπίστευσης.

Σημείωση (4): Επιπλέον πληροφορίες «αναγνώρισης» που έχουν να κάνουν με την κατάσταση, οι οποίες ορίζονται στο επίπεδο των εθνικών συστημάτων εποπτείας/διαπίστευσης για τους CSP που δεν εκδίδουν QC ΔΥΝΑΝΤΑΙ ΝΑ παρασχεθούν όταν υπάρχουν και απαιτούνται (π.χ. για να γίνει διάκριση μεταξύ πολλών επιπέδων ποιότητας/ασφάλειας) στο επίπεδο υπηρεσιών. Οι υπεύθυνοι σχήματος ΘΑ ΠΡΕΠΕΙ ΝΑ χρησιμοποιήσουν την επέκταση «additionalServiceInformation» (διάταξη 5.8.2) του πεδίου «Service information extension» (διάταξη 5.5.9) ανάλογα με το σκοπό της παροχής των εν λόγω επιπλέον πληροφοριών «αναγνώρισης». Επιπλέον, ο υπεύθυνος σχήματος μπορεί προαιρετικά να χρησιμοποιήσει τη διάταξη 5.5.6 («URI καθορισμού υπηρεσίας σχήματος»).

Current status starting date and time (διάταξη 5.5.5)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει την ημερομηνία και την ώρα έναρξης ισχύος της τρέχουσας κατάστασης έγκρισης (τιμή ημερομηνίας/ώρας όπως καθορίζεται στο ETSI TS 102 231, διάταξη 5.1.4).

Scheme service definition URI (διάταξη 5.5.6)

Το πεδίο αυτό είναι ΠΡΟΑΙΡΕΤΙΚΟ και αν υπάρχει ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει το/τα URI από όπου τα εξαρτώμενα μέρη μπορούν να λάβουν πληροφορίες ειδικά για την υπηρεσία, τις οποίες παρέχει ο υπεύθυνος του σχήματος ως σειρά πολύγλωσσων δεικτών (με την ΕΝ ως υποχρεωτική γλώσσα και με ενδεχομένως μια ή περισσότερες εθνικές γλώσσες).

Όταν χρησιμοποιείται/ούνται το/τα εκάστοτε URI ΠΡΕΠΕΙ ΝΑ παρέχουν μια διαδρομή προς πληροφορίες, οι οποίες περιγράφουν την υπηρεσία όπως καθορίζεται από το σχήμα Ειδικά, αυτό, όταν ισχύει, ΔΥΝΑΤΑΙ ΝΑ περιλαμβάνει:

α) ένα URI το οποίο υποδεικνύει την ταυτότητα του εφεδρικού CSP σε περίπτωση εποπτείας μιας υπηρεσίας υπό ανάκληση, στην οποία συμμετέχει ένας εφεδρικός CSP (βλέπε «Service current status» – διάταξη 5.5.4)·

▼C1

β) ένα URI το οποίο οδηγεί σε έγγραφα που παρέχουν επιπλέον πληροφορίες όσον αφορά τη χρήση κάποιας εθνικά καθορισμένης ειδικής αναγνώρισης για μια εποπτευόμενη/διαπιστευμένη υπηρεσία παροχής αδειοδοτικού υπηρεσίας εμπίστευσης σύμφωνα με τη χρήση του πεδίου «Επέκταση πληροφοριών υπηρεσίας» (διάταξη 5.5.9) με επέκταση «additionalServiceInformation», όπως ορίζεται στη διάταξη 5.8.2.

Service supply points (διάταξη 5.5.7)

Το πεδίο αυτό είναι ΠΡΟΑΙΡΕΤΙΚΟ και αν υπάρχει ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει το/τα URI μέσω των οποίων τα εξαρτώμενα μέρη μπορούν να έχουν πρόσβαση στην υπηρεσία μέσω μιας σειράς στοιχειοσειρών, η σύνταξη των οποίων ΠΡΕΠΕΙ ΝΑ συμμορφώνεται με το RFC 3986.

TSP service definition URI (διάταξη 5.5.8)

Το πεδίο αυτό είναι ΠΡΟΑΙΡΕΤΙΚΟ και αν υπάρχει ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει το/τα URI από όπου τα εξαρτώμενα μέρη μπορούν να λάβουν πληροφορίες ειδικά για την υπηρεσία, τις οποίες παρέχει ο TSP ως σειρά πολύγλωσσων δεικτών (με την EN ως υποχρεωτική γλώσσα και με ενδεχομένως μια ή περισσότερες εθνικές γλώσσες). Το (τα) εκάστοτε URI ΠΡΕΠΕΙ ΝΑ παρέχουν μια διαδρομή προς πληροφορίες, οι οποίες περιγράφουν την υπηρεσία όπως καθορίζεται από τον TSP.

Service information extensions (διάταξη 5.5.9)

Στο πλαίσιο των εν λόγω προδιαγραφών, το πεδίο αυτό είναι ΠΡΟΑΙΡΕΤΙΚΟ αλλά ΘΑ ΠΡΕΠΕΙ ΝΑ υπάρχει όταν οι πληροφορίες που παρέχονται στο πεδίο «Service digital identity» (διάταξη 5.5.3) δεν είναι αρκετές για την αδιαμφισβήτητη ταυτοποίηση των αναγνωρισμένων πιστοποιητικών που εξέδωσε η εν λόγω υπηρεσία ή/και όταν οι πληροφορίες που υπάρχουν στα σχετικά αναγνωρισμένα πιστοποιητικά δεν επιτρέπουν αναγνώριση με μηχανικά μέσα επεξεργασίας των στοιχείων σχετικά με το αν το QC υποστηρίζεται ή όχι από μια SSCD ([1]).

Στο πλαίσιο των εν λόγω προδιαγραφών, όταν η χρήση του είναι ΑΠΑΡΑΙΤΗΤΗ, π.χ. για υπηρεσίες CA/QC, ΘΑ ΠΡΕΠΕΙ ΝΑ χρησιμοποιηθεί και να δομηθεί ένα προαιρετικό πεδίο πληροφοριών «Service information extensions» («Sie»), σύμφωνα με την επέκταση «Αναγνωρίσεις», η οποία ορίζεται στο ETSI TS 102 231, παράρτημα L.3.1, ως σειρά μιας ή περισσοτέρων πλειάδων, καθεμία από τις οποίες παρέχει:

— (φίλτρα) Πληροφορίες, οι οποίες θα χρησιμοποιηθούν για την περαιτέρω αναγνώριση στην αναγνωρισμένη υπηρεσία πιστοποίησης «Sdi» την υπηρεσία εκείνη (δηλαδή το σύνολο αναγνωρισμένων πιστοποιητικών), για την οποία απαιτούνται/παρέχονται επιπλέον πληροφορίες, όσον αφορά την παρουσία ή την απουσία υποστήριξης από SSCD (ή/και την έκδοση υπέρ νομικού προσώπου) και

— Τις συσχετιζόμενες πληροφορίες («προσδιοριστές») σχετικά με το αν αυτό το περαιτέρω αναγνωρισμένο σύνολο υπηρεσιών αναγνωρισμένων πιστοποιητικών υποστηρίζεται από μια SSCD ή όχι (όταν αυτές οι πληροφορίες είναι «QCSSCDStatusAsInCert», αυτό σημαίνει ότι αυτές οι συσχετιζόμενες πληροφορίες αποτελούν μέρος του QC βάσει τυποποιημένης μορφής με δυνατότητα επεξεργασίας από μηχανή του ETSI ([2]), ή/και τις πληροφορίες όσον αφορά το γεγονός ότι τα εν λόγω QC εκδίδονται υπέρ νομικών προσώπων (εξ ορισμού πρέπει να θεωρείται ότι εκδίδονται μόνο υπέρ φυσικών προσώπων).

— **QCWithSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCWithSSCD): σημαίνει ότι ο CSP διασφαλίζει και το κράτος μέλος (ο φορέας εποπτείας ή ο φορέας διαπίστευσής του, αντίστοιχα) ελέγχει (μοντέλο εποπτείας) ή διερευνά (μοντέλο διαπίστευσης) ότι οποιαδήποτε QC, τα οποία εκδίδονται στο πλαίσιο της υπηρεσίας (QCA) που ορίζεται στο πεδίο «Service digital identity» (διάταξη 5.5.3) και ορίζεται περαιτέρω από τις προαναφερθείσες πληροφορίες (φίλτρα), οι οποίες χρησιμοποιούνται για την περαιτέρω αναγνώριση στο πλαίσιο της καθοριζόμενης από το «Sdi» υπηρεσίας πιστοποίησης του ακριβούς συνόλου αναγνωρισμένων πιστοποιητικών για τα οποία απαιτούνται οι εν λόγω επιπρόσθετες πληροφορίες όσον αφορά την παρουσία ή την απουσία υποστήριξης **ΥΠΟΣΤΗΡΙΖΟΝΤΑΙ** από μια SSCD (δηλαδή ότι το ιδιωτικό κλειδί που συσχετίζεται με το δημόσιο κλειδί του πιστοποιητικού αποθηκεύεται σε μια ασφαλή διάταξη δημιουργίας υπογραφών, σύμφωνα με το παράρτημα III της Οδηγίας 1999/93/ΕΚ),

([1]) Βλέπε ενότητα 2.2 του παρόντος εγγράφου.

([2]) Αυτό αναφέρεται σε ένα κατάλληλο συνδυασμό της δήλωσης QcCompliance που ορίζεται από το ETSI, δηλώσεων QcSSCD [ETSI TS 101 862] ή ενός QCP/QCP + OID καθοριζόμενου από το ETSI [ETSI TS 101 456].

▼C1

— **QCNoSSCD** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCNoSSCD): σημαίνει ότι ο CSP διασφαλίζει και το κράτος μέλος (ο φορέας εποπτείας ή ο φορέας διαπίστευσής του, αντίστοιχα) ελέγχει (μοντέλο εποπτείας) ή διερευνά (μοντέλο διαπίστευσης) ότι οποιαδήποτε QC, τα οποία εκδίδονται στο πλαίσιο της υπηρεσίας (RootCA/QC ή CA/QC) που ορίζεται στο πεδίο «Service digital identity» (διάταξη 5.5.3) και ορίζεται περαιτέρω από τις προαναφερθείσες πληροφορίες (φίλτρα), οι οποίες χρησιμοποιούνται για την περαιτέρω αναγνώριση στο πλαίσιο της καθοριζόμενης από το «Sdi» υπηρεσίας πιστοποίησης του ακριβούς συνόλου αναγνωρισμένων πιστοποιητικών για τα οποία απαιτούνται οι εν λόγω επιπρόσθετες πληροφορίες όσον αφορά την παρουσία ή την απουσία υποστήριξης **ΔΕΝ ΥΠΟΣΤΗΡΙΖΟΝΤΑΙ** από μια SSCD (δηλαδή ότι το ιδιωτικό κλειδί που συσχετίζεται με το δημόσιο κλειδί του πιστοποιητικού **δεν** αποθηκεύεται σε μια ασφαλή διάταξη δημιουργίας υπογραφών, σύμφωνα με το παράρτημα ΙΙΙ της Οδηγίας 1999/93/ΕΚ).

— **QCSSCDStatusAsInCert** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCSSCDStatusAsInCert): σημαίνει ότι ο CSP διασφαλίζει και το κράτος μέλος (ο φορέας εποπτείας ή ο φορέας διαπίστευσής του, αντίστοιχα) ελέγχει (μοντέλο εποπτείας) ή διερευνά (μοντέλο διαπίστευσης) ότι οποιαδήποτε QC, τα οποία εκδίδονται στο πλαίσιο της υπηρεσίας (CA/QC) που ορίζεται στο πεδίο «Service digital identity» (διάταξη 5.5.3) και ορίζεται περαιτέρω από τις προαναφερθείσες πληροφορίες (φίλτρα), οι οποίες χρησιμοποιούνται για την περαιτέρω αναγνώριση στο πλαίσιο της καθοριζόμενης από το «Sdi» υπηρεσίας πιστοποίησης του ακριβούς συνόλου αναγνωρισμένων πιστοποιητικών για τα οποία απαιτούνται οι εν λόγω επιπρόσθετες πληροφορίες όσον αφορά την παρουσία ή την απουσία υποστήριξης ΘΑ ΠΡΕΠΕΙ ΝΑ περιέχουν τις πληροφορίες με δυνατότητα επεξεργασίας με μηχανικά μέσα που υποδεικνύουν αν το QC υποστηρίζεται από μια SSCD,

— **QCForLegalPerson** (http://uri.etsi.org/TrstSvc/eSigDir-1999-93-EC-TrustedList/SvcInfoExt/QCForLegalPerson): σημαίνει ότι ο CSP διασφαλίζει και το κράτος μέλος (ο φορέας εποπτείας ή ο φορέας διαπίστευσής του, αντίστοιχα) ελέγχει (μοντέλο εποπτείας) ή διερευνά (μοντέλο διαπίστευσης) ότι οποιαδήποτε QC, τα οποία εκδίδονται στο πλαίσιο της υπηρεσίας (QCA) που ορίζεται στο πεδίο «Service digital identity» (διάταξη 5.5.3) και ορίζεται περαιτέρω από τις προαναφερθείσες πληροφορίες (φίλτρα), οι οποίες χρησιμοποιούνται για την περαιτέρω αναγνώριση στο πλαίσιο της καθοριζόμενης από το «Sdi» υπηρεσίας πιστοποίησης του ακριβούς συνόλου αναγνωρισμένων πιστοποιητικών για τα οποία απαιτούνται οι εν λόγω επιπρόσθετες πληροφορίες όσον αφορά την έκδοση υπέρ νομικού προσώπου **ΕΚΔΙΔΟΝΤΑΙ** υπέρ νομικών προσώπων,

Οι προσδιοριστές αυτοί πρέπει να χρησιμοποιούνται μόνο ως επεκτάσεις αν ο τύπος της υπηρεσίας είναι http://uri.etsi.org/TrstSvc/Svctype/CA/QC.

Το πεδίο αυτό αφορά ειδικά την εφαρμογή (ASN.1 ή XML) και ΠΡΕΠΕΙ ΝΑ συμμορφώνεται με τις προδιαγραφές που παρέχονται στο ETSI TS 102 231, παράρτημα L.3.1.

▼M1

Στο πλαίσιο μιας εφαρμογής XML, το ειδικό περιεχόμενο των εν λόγω επιπρόσθετων πληροφοριών πρέπει να κωδικοποιηθεί, χρησιμοποιώντας τα αρχεία xsd που παρέχονται στο παράρτημα Γ του ETSI TS 102 231.

▼C1

Service Approval History

Το πεδίο αυτό είναι ΠΡΟΑΙΡΕΤΙΚΟ αλλά ΠΡΕΠΕΙ ΝΑ υπάρχει αν η «Historical information period» (διάταξη 5.3.12) δεν είναι μηδενική. Έτσι, στο πλαίσιο των εν λόγω προδιαγραφών, το σχήμα ΠΡΕΠΕΙ ΝΑ διατηρεί πληροφορίες ιστορικού. Σε περίπτωση που πρέπει να διατηρούνται πληροφορίες ιστορικού, αλλά η υπηρεσία δεν έχει ιστορικό πριν από την τρέχουσα κατάσταση (δηλαδή ο υπεύθυνος του σχήματος δεν είχε διατηρήσει την αρχική κατάσταση καταγραφής ούτε πληροφορίες ιστορικού) το εν λόγω πεδίο ΘΑ ΠΡΕΠΕΙ ΝΑ αφήνεται κενό. Διαφορετικά, για κάθε αλλαγή στην τρέχουσα κατάσταση της υπηρεσίας TSP που σημειώθηκε εντός της περιόδου πληροφοριών ιστορικού, όπως καθορίζεται στο ETSI TS 102 231 διάταξη 5.3.12, οι πληροφορίες για την προηγούμενη κατάσταση έγκρισης ΘΑ ΠΡΕΠΕΙ ΝΑ παρέχονται σε φθίνουσα σειρά ημερομηνίας και ώρας αλλαγής κατάστασης (δηλαδή της ημερομηνίας και της ώρας έναρξης ισχύος της μετέπειτα κατάστασης έγκρισης).

▼C1

Αυτό ΘΑ ΠΡΕΠΕΙ ΝΑ αποτελεί μια σειρά πληροφοριών ιστορικού όπως ορίζεται παρακάτω.

▼C2

TSP(1) Service(1) History(1)

▼C1

Service type identifier (διάταξη 5.6.1)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει το αναγνωριστικό του τύπου υπηρεσίας, με τη μορφή και την έννοια με την οποία χρησιμοποιείται στο πεδίο «TSP Service Information – Service type identifier» (διάταξη 5.5.1).

Service name (διάταξη 5.6.2)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζεται η ονομασία υπό την οποία ο CSP παρέσχε την υπηρεσία που ορίζεται στο πεδίο «TSP Service Information – Service type identifier» (διάταξη 5.5.1) με τη μορφή και την έννοια με την οποία χρησιμοποιείται στο «TSP Service Information – Service name» (διάταξη 5.5.2). Αυτή η διάταξη δεν απαιτεί να είναι η ονομασία η ίδια με εκείνη που ορίζεται στη διάταξη 5.5.2. Μια αλλαγή της ονομασίας ΔΥΝΑΤΑΙ ΝΑ οφείλεται στις περιστάσεις που απαιτούν νέα κατάσταση.

▼M1

Service digital identity (διάταξη 5.6.3)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΚΑΘΟΡΙΖΕΙ τουλάχιστον μια απεικόνιση του ψηφιακού αναγνωριστικού (π.χ. X.509v3 πιστοποιητικό) που χρησιμοποιείται στο πεδίο «TSP Service Information – Service digital identity» (διάταξη 5.5.3), με την ίδια μορφή και έννοια όπως ορίζεται στο ETSI TS 102 231, διάταξη 5.5.3.

Σημείωση: Για μια τιμή πιστοποιητικού X.509v3 που χρησιμοποιείται στο πεδίο «Sdi» διάταξη 5.5.3 μιας υπηρεσίας, πρέπει να υπάρχει μόνον μια μεμονωμένη καταχώριση υπηρεσίας στον κατάλογο εμπίστευσης ανά τιμή «Sti:Sie/-additionalServiceInformation». Οι πληροφορίες «Sdi» (διάταξη 5.6.3) που χρησιμοποιούνται στις πληροφορίες ιστορικού έγκρισης υπηρεσίας σε σύνδεση με μια καταχώριση υπηρεσίας και οι πληροφορίες «Sdi» (διάταξη 5.5.3) που χρησιμοποιούνται στην εν λόγω καταχώριση υπηρεσίας ΠΡΕΠΕΙ να έχουν σχέση με την ίδια τιμή πιστοποιητικού X.509v3. Όταν αλλάξει το «Sdi» μιας καταγεγραμμένης υπηρεσίας (π.χ. ανανέωση ή αλλαγή κλειδιού ενός πιστοποιητικού X.509v3 για π.χ. ένα CA/PKC ή CA/QC) ή δημιουργηθεί νέο «Sdi» για τέτοιου είδους υπηρεσία, ακόμη και αν οι τιμές είναι ίδιες για τα συναφή «Sti», «Sn», και [«Sie»], αυτό σημαίνει ότι ο Scheme Operator ΠΡΕΠΕΙ να δημιουργήσει μια διαφορετική καταχώριση υπηρεσίας από την προηγούμενη.

▼C1

Service previous status (διάταξη 5.6.4)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει το αναγνωριστικό της προηγούμενης κατάστασης της υπηρεσίας, με τη μορφή και την έννοια με την οποία χρησιμοποιείται στο πεδίο «TSP Service Information – Service current status» (διάταξη 5.5.4).

Previous status starting date and time (διάταξη 5.6.5)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει την ημερομηνία και την ώρα κατά την οποία τέθηκε σε ισχύ η προηγούμενη εν λόγω κατάσταση, με τη μορφή και την έννοια με την οποία χρησιμοποιείται στο πεδίο «TSP Service Information – Service current status starting date and time» (διάταξη 5.5.5).

Service information extensions (διάταξη 5.6.6)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΔΥΝΑΤΑΙ ΝΑ χρησιμοποιηθεί από τους υπεύθυνους του σχήματος για να παράσχουν ειδικές πληροφορίες για την υπηρεσία, με τη μορφή και την έννοια με την οποία χρησιμοποιείται στο πεδίο «TSP Service Information – Service information extensions» (διάταξη 5.5.9).

▼C2

TSP(1) Service(1) History(2)

Το ίδιο για το TSP(1) Service(1) History(2) (πριν από το History 1)

…

TSP(1) Service(2)

Το ίδιο για το TSP(1) Service 2 (όπως ισχύει)

TSP(1) Service(2) History(1)

…

TSP(2) Information

Το ίδιο για το TSP 2 (όπως ισχύει)

Το ίδιο για το TSP 2 Service 1

Το ίδιο για το TSP 2 Service 1 History 1

…

▼M1

Signed TSL

Η αναγνώσιμη από άνθρωπο TSL εφαρμογή του καταλόγου εμπίστευσης, το οποίο θεσπίζεται υπό τις παρούσες προδιαγραφές και ιδίως το κεφάλαιο IV, φέρει την υπογραφή του «Scheme operator name» (διάταξη 5.3.4), προκειμένου να διασφαλιστεί η αυθεντικότητα και η ακεραιότητά του ([1]). Η μορφή της υπογραφής είναι PAdES μέρος 3 [ETSI TS 102 778-3 ([2])] αλλά ΜΠΟΡΕΙ να είναι PAdES μέρος 2 [ETSI TS 102 778-2 ([3])] στο πλαίσιο του ειδικού αξιόπιστου μοντέλου που θεσπίστηκε μέσω της δημοσίευσης των πιστοποιητικών που χρησιμοποιούνται για την υπογραφή των καταλόγων εμπίστευσης.

Η μηχανικά επεξεργάσιμη TSL εφαρμογή του καταλόγου εμπίστευσης, το οποίο θεσπίζεται υπό τις παρούσες προδιαγραφές, φέρει την υπογραφή του «Scheme operator name» (διάταξη 5.3.4), προκειμένου να διασφαλιστεί η αυθεντικότητα και η ακεραιότητά του. Η μορφή της μηχανικά επεξεργάσιμης TSL εφαρμογής του καταλόγου εμπίστευσης, η οποία θεσπίζεται υπό τις παρούσες προδιαγραφές, είναι XML και συμμορφώνεται με τις προδιαγραφές που αναφέρονται στα παραρτήματα Β και Γ του ETSI TS 102 231.

Η μορφή της υπογραφής ΠΡΕΠΕΙ να είναι XAdES BES ή EPES όπως ορίζεται από τις προδιαγραφές ETSI TS 101 903 για εφαρμογές XML. Αυτή η εφαρμογή ηλεκτρονικής υπογραφής πληροί τις απαιτήσεις που αναφέρονται στο παράρτημα Β του ETSI TS 102 231 ([4]). Επιπλέον γενικές απαιτήσεις όσον αφορά την υπογραφή αναγράφονται στις παρακάτω ενότητες.

▼C1

Scheme identification (διάταξη 5.7.2)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει μια παραπομπή την οποία θα αναθέτει ο υπεύθυνος του σχήματος, η οποία να ορίζει με μονοσήμαντο τρόπο το σχήμα που περιγράφεται στις παρούσες προδιαγραφές και στον καθιερωμένο TSL, και ΠΡΕΠΕΙ ΝΑ συμπεριλαμβάνεται κατά τον υπολογισμό της υπογραφής. Αναμένεται ότι θα είναι μια στοιχειοσειρά χαρακτήρων ή δυαδικών ψηφίων.

([1]) Αν η αναγνώσιμη από άνθρωπο TSL εφαρμογή του καταλόγου εμπίστευσης δεν είναι υπογεγραμμένη, η αυθεντικότητα και η ακεραιότητα ΠΡΕΠΕΙ να εξασφαλίζονται από κατάλληλο δίαυλο κοινοποίησης με ισότιμο επίπεδο ασφάλειας. Χρήση του TLS (IETF RFC 5246: «The Transport Layer Security (TLS) Protocol Version 1.2») συνιστάται για τον σκοπό αυτό και το αποτύπωμα του πιστοποιητικού του διαύλου TLS ΠΡΕΠΕΙ τα κράτη μέλη να θέτουν στη διάθεση εκτός ζώνης των χρηστών TSL.

([2]) ETSI TS 102 778-3 — Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced — PAdES-BES and PAdES-EPES Profiles.

([3]) ETSI TS 102 778-2 — Electronic Signatures and Infrastructures (ESI): PDF Advanced Electronic Signature Profiles; Part 2: PAdES Basic — Profile based on ISO 32000-1.

([4]) Είναι υποχρεωτικό να προστατεύεται το πιστοποιητικό υπογραφής του υπεύθυνου σχήματος με την υπογραφή με έναν από τους τρόπους που καθορίζονται στο ETSI TS 101 903 και το ds:keyInfo πρέπει να περιέχει τη σχετική σειρά πιστοποιητικού, αν υπάρχει.

▼M1

Στο πλαίσιο των εν λόγω προδιαγραφών, η παραπομπή που ανατέθηκε αποτελεί παράθεση του πεδίου «TSL type» (διάταξη 5.3.3), του πεδίου «Scheme name» (διάταξη 5.3.6) και της τιμής της επέκτασης SubjectKeyIdentifier του πιστοποιητικού που χρησιμοποιεί ο υπεύθυνος του σχήματος για να υπογράψει ηλεκτρονικά το TSL.

▼C1

Signature algorithm identifier (διάταξη 5.7.3)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ καθορίζει τον κρυπτογραφικό αλγόριθμο που χρησιμοποιήθηκε για τη δημιουργία της υπογραφής. Ανάλογα με τον χρησιμοποιούμενο αλγόριθμο, το πεδίο αυτό ΔΥΝΑΤΑΙ να απαιτεί επιπλέον παραμέτρους. Το πεδίο αυτό ΠΡΕΠΕΙ ΝΑ συμπεριλαμβάνεται στον υπολογισμό της υπογραφής.

Signature value (διάταξη 5.7.4)

Το πεδίο αυτό ΑΠΑΙΤΕΙΤΑΙ και ΘΑ ΠΡΕΠΕΙ ΝΑ συμπεριλαμβάνει την πραγματική τιμή της ψηφιακής υπογραφής. Όλα τα πεδία του TSL (εκτός από την ίδια την τιμή της υπογραφής) ΠΡΕΠΕΙ να συμπεριλαμβάνονται στον υπολογισμό της υπογραφής.

TSL extensions (διάταξη 5.8)

Επέκταση **expiredCertsRevocationInfo** (διάταξη 5.8.1)

Η επέκταση αυτή είναι ΠΡΟΑΙΡΕΤΙΚΗ. Όταν χρησιμοποιείται ΠΡΕΠΕΙ ΝΑ συμμορφώνεται με τις προδιαγραφές του ETSI TS 102 231, διάταξη 5.8.1.

Επέκταση **additionalServiceInformation** (διάταξη 5.8.2)

Αυτή η ΠΡΟΑΙΡΕΤΙΚΗ επέκταση, όταν χρησιμοποιείται, ΠΡΕΠΕΙ ΝΑ χρησιμοποιείται μόνο σε επίπεδο υπηρεσίας και μόνο στο πεδίο που ορίζεται στη διάταξη 5.5.9 («Επέκταση πληροφοριών υπηρεσίας»). Χρησιμοποιείται για να παράσχει επιπλέον πληροφορίες για μια υπηρεσία. ΘΑ ΠΡΕΠΕΙ ΝΑ αποτελεί αλληλουχία μιας ή περισσότερων πλειάδων, καθεμιά από τις οποίες θα παρέχει:

α) ένα URI το οποίο θα ορίζει τις επιπλέον πληροφορίες, π.χ.:

— ένα URI το οποίο θα υποδεικνύει κάποιο εθνικά καθορισμένο ειδικό προσδιοριστή για μια παροχή εποπτευόμενου/διαπιστευμένου αδειοδοτικού υπηρεσίας εμπιστοσύνης, π.χ.

— ένα καθορισμένο επίπεδο διαβάθμισης ασφάλειας/ποιότητας όσον αφορά το εθνικό σχήμα εποπτείας/διαπίστευσης για τους CSP που δεν εκδίδουν QC (π.χ. RGS */**/*** στα γαλλικά, ειδική κατάσταση «εποπτείας» που ορίζεται από την εθνική νομοθεσία για καθορισμένους CSP που εκδίδουν QC στα γερμανικά), βλέπε Σημείωση (4) του πεδίου «Service current status» – διάταξη 5.5.4,

— ή μια καθορισμένη νομική κατάσταση για μια παροχή εποπτευόμενου/διαπιστευμένου αδειοδοτικού υπηρεσίας εμπιστοσύνης (π.χ. ένα εθνικά καθορισμένο «αναγνωρισμένο TST» όπως στα γερμανικά ή στα ουγγρικά),

— ή την έννοια ενός καθορισμένου αναγνωριστικού πολιτικής, το οποίο υπάρχει σε ένα πιστοποιητικό X.509v3 και παρέχεται στο πεδίο «Sdi».

— ή ένα εγγεγραμμένο URI όπως καθορίζεται στο πεδίο «Αναγνωριστικό τύπου υπηρεσίας», διάταξη 5.5.1, προκειμένου να καθοριστεί περαιτέρω η συμμετοχή της αναγνωρισμένης υπηρεσίας βάσει «Sti» ως βασική υπηρεσία ενός παρόχου υπηρεσιών πιστοποίησης που εκδίδει QC (π.χ. OCSP-QC, CRL-QC, και RootCA-QC)·

β) έναν προαιρετικό αλγόριθμο ο οποίος περιέχει την τιμή serviceInformation, με την έννοια που ορίζεται στο σχήμα (π.χ. *, ** ή ***)·

γ) τυχόν επιπλέον πληροφορίες που παρέχονται σε μια μορφή ειδική για το σχήμα.

▼**M1**

Η τροποποίηση του URI οδηγεί σε πληροφορίες με δυνατότητα ανάγνωσης (τουλάχιστον στα EN και ενδεχομένως σε μία ή περισσότερες εθνικές γλώσσες) τα οποία θεωρούνται κατάλληλα και επαρκή για να μπορεί ένα συμβαλλόμενο μέρος να κατανοήσει την επέκταση και ειδικά για την εξήγηση της έννοιας των δεδομένων URI, με την οποία θα καθορίζονται οι δυνατές τιμές για το serviceInformation και τι σημαίνει κάθε τιμή.

Qualifications Extension (διάταξη L.3.1)

Περιγραφή: Το πεδίο αυτό είναι ΠΡΟΑΙΡΕΤΙΚΟ αλλά ΠΡΕΠΕΙ να υπάρχει όταν η χρήση του είναι ΑΠΑΡΑΙΤΗΤΗ, π.χ. για υπηρεσίες RootCA/QC ή CA/QC, και όταν:

— οι πληροφορίες που παρέχονται στο πεδίο «Ψηφιακό αναγνωριστικό υπηρεσίας» δεν αρκούν για να ταυτοποιήσουν με σαφήνεια τα αναγνωρισμένα πιστοποιητικά που εκδίδονται από την εν λόγω υπηρεσία,

— οι πληροφορίες που υπάρχουν στα σχετικά αναγνωρισμένα πιστοποιητικά δεν επιτρέπουν αναγνώριση με μηχανικά μέσα επεξεργασίας των στοιχείων όσον αφορά το αν το QC υποστηρίζεται από SSCD.

Όταν χρησιμοποιείται, αυτή η επέκταση επιπέδου υπηρεσίας ΠΡΕΠΕΙ ΝΑ χρησιμοποιείται μόνο στο πεδίο που ορίζεται στο «Service information extension» (διάταξη 5.5.9) και συμμορφώνεται με τις προδιαγραφές που καθορίζονται στο παράρτημα L.3.1 του ETSI TS 102 231.

TakenOverBy Extension (διάταξη L.3.2)

Περιγραφή: Η επέκταση είναι ΠΡΟΑΙΡΕΤΙΚΗ αλλά ΠΡΕΠΕΙ να είναι εμφανής όταν μια υπηρεσία που ανήκε πριν στη νομική αρμοδιότητα ενός CSP αναλαμβάνεται από άλλο TSP και χρησιμεύει στην επίσημη δήλωση της νομικής αρμοδιότητας μιας υπηρεσίας και παρέχει τη δυνατότητα στο λογισμικό επαλήθευσης να παρουσιάσει στο χρήστη κάποια νομική λεπτομέρεια. Οι πληροφορίες που παρέχονται στην εν λόγω επέκταση είναι συναφείς με τη σχετική χρήση της διάταξης 5.5.6 και συμμορφώνονται με τις προδιαγραφές στο παράρτημα L.3.2 του ETSI TS 102 231.

▼**M1**

ΚΕΦΑΛΑΙΟ II

Κατά την κατάρτιση των καταλόγων εμπίστευσής τους, τα κράτη μέλη θα χρησιμοποιούν:

τους κωδικούς των γλωσσών στο κάτω τετραγωνίδιο και τους κωδικούς των χωρών στο επάνω τετραγωνίδιο·

Τους κωδικούς γλωσσών και χωρών σύμφωνα με τον πίνακα που παρατίθεται παρακάτω·

Όταν υπάρχει λατινική γραφή (με το σωστό της κωδικό γλώσσας) προστίθεται ο μεταγραμματισμός στη λατινική γραφή με τους αντίστοιχους κωδικούς γλώσσας που διευκρινίζονται στον παρακάτω πίνακα.

Σύντομη επωνυμία (στη γλώσσα πηγή)	Σύντομη επωνυμία (στα αγγλικά)	Κωδικός χώρας	Κωδικός γλώσσας	Σημειώσεις	Transliterati on in Latin script
Belgique/België	Belgium	BE	nl, fr, de		
България (*)	Bulgaria	BG	bg		bg-Latn
Česká republika	Czech Republic	CZ	cs		
Danmark	Denmark	DK	da		
Deutschland	Germany	DE	de		
Eesti	Estonia	EE	et		
Éire/Ireland	Ireland	IE	ga, en		
Ελλάδα (*)	Greece	EL	el	Κωδικός χώρας που συνιστάται από την ΕΕ	el-Latn
España	Spain	ES	es	καθώς και Catalan (ca), Basque (eu), Galician (gl)	
France	France	FR	fr		
Italia	Italy	IT	it		
Κύπρος/Kıbrıs (*)	Cyprus	CY	el, tr		el-Latn
Latvija	Latvia	LV	lv		
Lietuva	Lithuania	LT	lt		
Luxembourg	Luxembourg	LU	fr, de, lb		
Magyarország	Hungary	HU	hu		
Malta	Malta	MT	mt, en		
Nederland	Netherlands	NL	nl		
Österreich	Austria	AT	de		
Polska	Poland	PL	pl		
Portugal	Portugal	PT	pt		
România	Romania	RO	ro		

▼**M1**

Σύντομη επωνυμία (στη γλώσσα πηγή)	Σύντομη επωνυμία (στα αγγλικά)	Κωδικός χώρας	Κωδικός γλώσσας	Σημειώσεις	Transliterati on in Latin script
Slovenija	Slovenia	SI	sl		
Slovensko	Slovakia	SK	sk		
Suomi/Finland	Finland	FI	fi, sv		
Sverige	Sweden	SE	sv		
United Kingdom	United Kingdom	UK	en	Κωδικός χώρας που συνιστάται από την ΕΕ	
Ísland	Iceland	IS	is		
Liechtenstein	Liechtenstein	LI	de		
Norge/Noreg	Norway	NO	no, nb, nn		

(*) Μεταγραμματισμός με λατινικά ψηφία: България = Bulgaria· Ελλάδα = Elláda· Κύπρος = Kýpros.

———————

▼C1

ΚΕΦΑΛΑΙΟ IV

ΠΡΟΔΙΑΓΡΑΦΕΣ ΓΙΑ ΤΗ ΜΟΡΦΗ ΜΕ ΔΥΝΑΤΟΤΗΤΑ ΑΝΑΓΝΩΣΗΣ ΑΠΟ ΑΝΘΡΩΠΟ ΤΗΣ ΕΦΑΡΜΟΓΗΣ TSL ΤΟΥ ΚΑΤΑΛΟΓΟΥ ΕΜΠΙΣΤΕΥΣΗΣ

Μια μορφή με δυνατότητα ανάγνωσης από άνθρωπο (Human Readable - HR) της εφαρμογής TSL του καταλόγου εμπίστευσης ΠΡΕΠΕΙ ΝΑ είναι διαθέσιμη στο κοινό και προσβάσιμη με ηλεκτρονικά μέσα. ΠΡΟΤΕΙΝΕΤΑΙ να παρέχεται με τη μορφή εγγράφου Portable Document Format (PDF) σύμφωνα με το ISO 32000, το οποίο ΠΡΕΠΕΙ να φέρει μορφοποίηση, σύμφωνα με το προφίλ PDF/A (ISO 19005).

Το περιεχόμενο μιας μορφής HR βάσει PDF/A της εφαρμογής TSL του καταλόγου εμπίστευσης ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ συμμορφώνεται με τις παρακάτω απαιτήσεις:

▼M1

— Ο τίτλος της αναγνώσιμης από άνθρωπο μορφής των καταλόγων εμπίστευσης κατασκευάζεται ως συνένωση των ακόλουθων στοιχείων:

  — προαιρετικά εικόνα της εθνικής σημαίας του κράτους μέλους,

  — κενός χώρος,

  — το ακρωνύμιο της χώρας στη γλώσσα/γλώσσες-πηγή (όπως προβλέπονται στην πρώτη στήλη του πίνακα του κεφαλαίου ΙΙ),

  — κενός χώρος,

  — «(»,

  — το ακρωνύμιο της χώρας στα αγγλικά (όπως προβλέπονται στη δεύτερη του πίνακα του κεφαλαίου ΙΙ) εντός παρενθέσεων,

  — «):» ως δεύτερη παρένθεση και ως διαχωριστικό,

  — κενός χώρος,

  — «Trusted List»,

  — προαιρετικά λογότυπο του φορέα διαχείρισης του σχήματος του κράτους μέλους.

▼C1

— Η δομή της μορφής HR ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ αντιστοιχεί στο λογικό μοντέλο που περιγράφεται στην ενότητα 5.1.2 του ETSI TS 102 231,

— Κάθε υπάρχον πεδίο ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ προβάλλεται και να παρέχει:

  — Τον τίτλο του πεδίου (π.χ. «Αναγνωριστικό τύπου υπηρεσίας»),

  — Την τιμή του πεδίου (π.χ. «CA/QC»),

  — Την έννοια (περιγραφή) της τιμής του πεδίου, όταν ισχύει, και ειδικά όπως προβλέπεται στο παράρτημα D του ETSI TS 102 231 ή στις παρούσες προδιαγραφές για τα καταγεγραμμένα URI (π.χ. «Μια αρχή πιστοποίησης που εκδίδει πιστοποιητικά δημοσίου κλειδιού»),

  — Πολλαπλές εκδόσεις σε διάφορες εθνικές γλώσσες, όπως προβλέπεται στην εφαρμογή TSL του καταλόγου εμπίστευσης, όταν ισχύουν.

— Τα παρακάτω πεδία και οι αντίστοιχες τιμές των ψηφιακών πιστοποιητικών που υπάρχουν στο πεδίο «Ψηφιακό αναγνωριστικό υπηρεσίας» ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ εμφανίζονται τουλάχιστον στη μορφή HR:

  — Έκδοση

  — Αύξων αριθμός

  — Αλγόριθμος υπογραφής

  — Εκδότης

  — Ισχύει από

  — Ισχύει μέχρι

  — Αντικείμενο

▼C1

— Δημόσιο κλειδί

— Πολιτικές πιστοποιητικού

— Αναγνωριστικό κλειδιού υποκειμένου

— Σημεία διανομής CRL

— Αναγνωριστικό κλειδιού αρχής

— Χρήση κλειδιού

— Βασικοί περιορισμοί

— Αλγόριθμος ψηφιακής σφραγίδας

— Ψηφιακή σφραγίδα

— Η μορφή HR ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ μπορεί να εκτυπωθεί εύκολα

— Η μορφή HR ΔΥΝΑΤΑΙ ΝΑ φέρει ηλεκτρονική υπογραφή. Όταν υπογράφεται, ΠΡΕΠΕΙ ΝΑ υπογράφεται από τον υπεύθυνο σχήματος, σύμφωνα με τις ίδιες προδιαγραφές υπογραφής που ισχύουν και για την εφαρμογή TSL του καταλόγου εμπίστευσης.