

## ΕΚΤΕΛΕΣΤΙΚΗ ΑΠΟΦΑΣΗ ΤΗΣ ΕΠΙΤΡΟΠΗΣ

της 14ης Οκτωβρίου 2013

για την τροποποίηση της απόφασης 2009/767/ΕΚ σχετικά με την κατάρτιση, την τήρηση και τη δημοσίευση καταλόγων εμπιστευσης για παρόχους υπηρεσιών πιστοποίησης οι οποίοι εποπτεύονται/διαπιστεύονται από τα κράτη μέλη

[κοινοποιηθείσα υπό τον αριθμό C(2013) 6543]

(Κείμενο που παρουσιάζει ενδιαφέρον για τον ΕΟΧ)

(2013/662/ΕΕ)

Η ΕΥΡΩΠΑΪΚΗ ΕΠΙΤΡΟΠΗ,

Έχοντας υπόψη τη Συνθήκη για τη λειτουργία της Ευρωπαϊκής Ένωσης,

Έχοντας υπόψη την οδηγία 2006/123/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 12ης Δεκεμβρίου 2006, σχετικά με τις υπηρεσίες στην εσωτερική αγορά <sup>(1)</sup>, και ιδίως το άρθρο 8 παράγραφος 3,

Εκτιμώντας τα ακόλουθα:

- (1) Η απόφαση 2009/767/ΕΚ της Επιτροπής, της 16ης Οκτωβρίου 2009, σχετικά με 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 <sup>(2)</sup>, υποχρεώνει τα κράτη μέλη να καθιστούν διαθέσιμες τις πληροφορίες που απαιτούνται για την επικύρωση προηγμένων ηλεκτρονικών υπογραφών που υποστηρίζονται από αναγνωρισμένο πιστοποιητικό. Αυτά τα στοιχεία πρέπει να διατίθενται με ομοιόμορφο τρόπο στους αποκαλούμενους «καταλόγους εμπιστευσης» που περιέχουν πληροφορίες σχετικά με τους παρόχους υπηρεσιών πιστοποίησης οι οποίοι εκδίδουν αναγνωρισμένα πιστοποιητικά για το κοινό σύμφωνα με την οδηγία 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές <sup>(3)</sup>, και οι οποίοι εποπτεύονται/διαπιστεύονται από το εκάστοτε κράτος μέλος.
- (2) Η πρακτική εμπειρία από την εφαρμογή της απόφασης 2009/767/ΕΚ από τα κράτη μέλη κατέδειξε ότι είναι απαραίτητο να γίνουν ορισμένες βελτιώσεις προκειμένου να μεγιστοποιηθούν τα οφέλη των καταλόγων εμπιστευσης. Επιπλέον, το Ευρωπαϊκό Ινστιτούτο Τηλεπικοινωνιακών Προτύπων (ETSI) δημοσίευσε νέες τεχνικές προδιαγραφές για τους καταλόγους εμπιστευσης (TS 119 612), οι οποίες βασίζονται στις προδιαγραφές που περιλαμβάνονται επί του παρόντος στο παράρτημα της απόφασης αλλά, ταυτόχρονα, επιφέρουν ορισμένες βελτιώσεις στις υφιστάμενες προδιαγραφές.
- (3) Ως εκ τούτου, η απόφαση 2009/767/ΕΚ θα πρέπει να τροποποιηθεί ώστε να παραπέμπει στις τεχνικές προδιαγραφές

119 612 του ETSI και να ενσωματώσει τις αλλαγές που θεωρούνται απαραίτητες για τη βελτίωση και τη διευκόλυνση της εφαρμογής και χρήσης των καταλόγων εμπιστευσης.

- (4) Προκειμένου να μπορέσουν τα κράτη μέλη να προβούν στις απαιτούμενες τεχνικές αλλαγές στους επίκαιρους καταλόγους εμπιστευσης, ενδείκνυται η έναρξη εφαρμογής της παρούσας απόφασης από την 1η Φεβρουαρίου 2014.
- (5) Τα μέτρα που προβλέπει η παρούσα απόφαση είναι σύμφωνα με τη γνώμη της επιτροπής για την οδηγία παροχής υπηρεσιών,

ΕΞΕΔΩΣΕ ΤΗΝ ΠΑΡΟΥΣΑ ΑΠΟΦΑΣΗ:

Άρθρο 1

**Τροποποιήσεις της απόφασης 2009/767/ΕΚ**

Η απόφαση 2009/767/ΕΚ τροποποιείται ως εξής:

1) Το άρθρο 2 τροποποιείται ως εξής:

- α) Οι παράγραφοι 1, 2 και 2α αντικαθίστανται από το ακόλουθο κείμενο:

«1. Κάθε κράτος μέλος κατάρτιζει, τηρεί και δημοσιεύει, σύμφωνα με τις τεχνικές προδιαγραφές που ορίζονται στο παράρτημα, “κατάλογο εμπιστευσης”, ο οποίος περιέχει, ως ελάχιστη προϋπόθεση, πληροφορίες που αφορούν τους παρόχους υπηρεσιών πιστοποίησης οι οποίοι εκδίδουν αναγνωρισμένα πιστοποιητικά για το κοινό και εποπτεύονται/διαπιστεύονται από το εκάστοτε κράτος μέλος..

2. Τα κράτη μέλη κατάρτιζουν και δημοσιεύουν μια μηχανικά επεξεργάσιμη μορφή του καταλόγου εμπιστευσης, σύμφωνα με τις προδιαγραφές που ορίζονται στο παράρτημα. Εάν ένα κράτος μέλος επιλέξει να δημοσιεύει σε αναγνώσιμη από άνθρωπο μορφή τον κατάλογο εμπιστευσης του, η εν λόγω μορφή του καταλόγου εμπιστευσης συμμορφώνεται με τις προδιαγραφές που ορίζονται στο παράρτημα.

2α. Τα κράτη μέλη υπογράφουν ηλεκτρονικά τη μηχανικά επεξεργάσιμη μορφή των καταλόγων εμπιστευσης τους προκειμένου να διασφαλίζεται η αυθεντικότητα και η ακεραιότητά τους. Εάν ένα κράτος μέλος δημοσιεύει αναγνώσιμη από άνθρωπο μορφή του καταλόγου εμπιστευσης, μεριμνά ώστε η εν λόγω μορφή του καταλόγου εμπιστευσης να περιέχει τα ίδια δεδομένα με τη μηχανικά επεξεργασμένη μορφή και την υπογράφει ηλεκτρονικά με το ίδιο πιστοποιητικό που χρησιμοποιείται για τη μηχανικά επεξεργασμένη μορφή.»

<sup>(1)</sup> ΕΕ L 376 της 27.12.2006, σ. 36.

<sup>(2)</sup> ΕΕ L 274 της 20.10.2009, σ. 36.

<sup>(3)</sup> ΕΕ L 13 της 19.1.2000, σ. 12.

β) Εισάγεται η ακόλουθη παράγραφος 2β:

«2β. Τα κράτη μέλη μεριμνούν ώστε η μηχανικά επεξεργασμένη μορφή των καταλόγων εμπιστευσις τους να είναι προσβάσιμη στον τόπο δημοσίευσής της οποιαδήποτε στιγμή και χωρίς διακοπή, εκτός από τις περιπτώσεις που πραγματοποιούνται εργασίες συντήρησης.»

γ) Η παράγραφος 3 αντικαθίσταται από το ακόλουθο κείμενο:

«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 μηχανικά επεξεργάσιμης μορφής καταλόγου εμπιστευσις·

β) τον τόπο δημοσίευσης της μηχανικά επεξεργάσιμης μορφής του καταλόγου εμπιστευσις·

γ) δύο ή περισσότερα πιστοποιητικά δημόσιου κλειδιού του υπεύθυνου σχήματος, με μετατιθέμενες περιόδους ισχύος τουλάχιστον τριών μηνών, που αντιστοιχούν στα ιδιωτικά κλειδιά που μπορούν να χρησιμοποιηθούν για την ηλεκτρονική υπογραφή της μηχανικά επεξεργάσιμης μορφής του καταλόγου εμπιστευσις·

δ) τυχόν αλλαγές σχετικά με τις πληροφορίες που αναφέρονται στα στοιχεία α), β) και γ).».

δ) Εισάγεται η ακόλουθη παράγραφος 3α:

«3α. Εάν ένα κράτος μέλος δημοσιεύει αναγνώσιμη από άνθρωπο μορφή του καταλόγου εμπιστευσις, οι πληροφορίες που αναφέρονται στην παράγραφο 3 κοινοποιούνται και για την αναγνώσιμη από άνθρωπο μορφή.».

2) Το παράρτημα αντικαθίσταται από το παράρτημα του παρόντος κανονισμού.

*Άρθρο 2*

### **Εφαρμογή**

Η παρούσα απόφαση εφαρμόζεται από την 1η Φεβρουαρίου 2014.

*Άρθρο 3*

### **Αποδέκτες**

Η παρούσα απόφαση απευθύνεται στα κράτη μέλη.

Βρυξέλλες, 14 Οκτωβρίου 2013.

Για την Επιτροπή

Michel BARNIER

Μέλος της Επιτροπής

## ΠΑΡΑΡΤΗΜΑ

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

## ΓΕΝΙΚΕΣ ΑΠΑΙΤΗΣΕΙΣ

## 1. Εισαγωγή

Σκοπός του κοινού σχεδίου τύπου «Κατάλογος εμπιστευσης 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<sup>(1)</sup> (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.

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)<sup>(2)</sup> τις οποίες υποστηρίζει ένα αναγνωρισμένο πιστοποιητικό<sup>(3)</sup> <sup>(4)</sup>.

Στις υποχρεωτικές πληροφορίες του καταλόγου εμπιστευσης πρέπει να περιλαμβάνονται, κατ' ελάχιστον, πληροφορίες για τους εποπτευόμενους/διαπιστευμένους CSP που εκδίδουν αναγνωρισμένα πιστοποιητικά (Qualified Certificate — QC)<sup>(5)</sup> σύμφωνα με τις διατάξεις της οδηγίας 1999/93/ΕΚ [άρθρο 3 παράγραφος 2 και 3 και άρθρο 7 παράγραφος 1 στοιχείο α)], συμπεριλαμβανομένων, όταν δεν αποτελούν μέρος των QC, πληροφοριών σχετικά με τα QC που υποστηρίζουν ηλεκτρονική υπογραφή και σχετικά με το αν η υπογραφή δημιουργείται ή όχι μέσω μιας ασφαλούς διάταξης δημιουργίας υπογραφών (Secure Signature Creation Device — SSCD)<sup>(6)</sup>.

Ο κατάλογος εμπιστευσης μπορεί να συμπεριλαμβάνει εθελοντικά και σε εθνική βάση επιπλέον πληροφορίες σχετικά με άλλους CSP που δεν εκδίδουν QC αλλά παρέχουν υπηρεσίες σχετικά με τις ηλεκτρονικές υπογραφές (π.χ. CSP που παρέχουν υπηρεσίες χρονοσφράγισης και εκδίδουν αδειοδοτικά χρονοσφράγισης, CSP που εκδίδουν μη αναγνωρισμένα πιστοποιητικά κ.λπ.), υπό την προϋπόθεση ότι είτε διαπιστεύονται/εποπτεύονται με παρόμοιο τρόπο όπως οι CSP που εκδίδουν QC είτε εγκρίνονται βάσει διαφορετικού εθνικού σχήματος έγκρισης. Τα εθνικά σχήματα έγκρισης μπορεί σε ορισμένα κράτη μέλη να διαφέρουν από τα σχήματα εποπτείας ή εθελοντικής διαπίστευσης που ισχύουν για τους CSP που εκδίδουν QC όσον αφορά τις ισχύουσες απαιτήσεις και/ή τον αρμόδιο οργανισμό. Οι όροι «διαπιστευμένος» και/ή «εποπτευόμενος» στις παρούσες προδιαγραφές καλύπτουν επίσης τα εθνικά σχήματα έγκρισης, αλλά θα παρέχονται πρόσθετες πληροφορίες σχετικά με τη φύση τυχόν εθνικών σχημάτων από το κάθε κράτος μέλος στον οικείο κατάλογο εμπιστευσης, συμπεριλαμβανομένων διευκρινίσεων σχετικά με τις ενδεχόμενες διαφορές με τα σχήματα διαπίστευσης/εποπτείας που ισχύουν σε CSP που εκδίδουν QC.

Το κοινό σχεδίο τύπου βασίζεται στις προδιαγραφές TS 119 612 v1.1.1 του ETSI<sup>(7)</sup> (στο εξής θα αναφέρονται ως ETSI TS 119 612), οι οποίες έχουν ως αντικείμενο την κατάρτιση, τη δημοσίευση, τον τόπο, την πρόσβαση, την επαλήθευση ταυτότητας και την ακεραιότητα καταλόγων τέτοιου είδους.

## 2. Δομή του κοινού σχεδίου τύπου για τον κατάλογο εμπιστευσης

Το κοινό σχεδίο τύπου για έναν κατάλογο εμπιστευσης κράτους μέλους είναι δομημένο σύμφωνα με τις προδιαγραφές TS 119 612 στις παρακάτω κατηγορίες πληροφοριών:

1. μια ετικέτα καταλόγου εμπιστευσης, η οποία θα διευκολύνει την ταυτοποίηση του καταλόγου εμπιστευσης κατά τις ηλεκτρονικές αναζητήσεις·
2. πληροφορίες σχετικά με τον κατάλογο εμπιστευσης και το σχήμα έκδοσής του·
3. μια αλληλουχία πεδίων που περιέχουν 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 δεν περιέχει τίποτα, δηλώνοντας την απουσία εποπτευόμενου ή διαπιστευμένου CSP στο οικείο κράτος μέλος για τους σκοπούς του καταλόγου εμπιστευσης)·
4. για κάθε καταγεγραμμένο CSP, τα λεπτομερή στοιχεία σχετικά με τις συγκεκριμένες υπηρεσίες εμπιστευσης που προσφέρει, των οποίων η τρέχουσα κατάσταση καταγράφεται στον κατάλογο εμπιστευσης, παρέχονται ως αλληλουχία πεδίων που ταυτοποιούν με αδιαμφισβήτητο τρόπο εποπτευόμενες/διαπιστευμένες υπηρεσίες πιστοποίησης που παρέχει ο CSP και την τρέχουσα κατάστασή τους (αυτή η αλληλουχία πρέπει να έχει τουλάχιστον μία καταχώριση)·

<sup>(1)</sup> Όπως ορίζονται στο άρθρο 2 παράγραφος 11 της οδηγίας 1999/93/ΕΚ.

<sup>(2)</sup> Όπως ορίζονται στο άρθρο 2 παράγραφος 2 της οδηγίας 1999/93/ΕΚ.

<sup>(3)</sup> Για μια AdES που υποστηρίζεται από ένα QC χρησιμοποιείται το ακρόνυμο «AdES<sub>QC</sub>» στο σύνολο του παρόντος εγγράφου.

<sup>(4)</sup> Επισημαίνεται ότι υπάρχουν πολλές ηλεκτρονικές υπηρεσίες που βασίζονται σε απλές AdES, των οποίων η διασυνοριακή χρήση θα μπορούσε επίσης να διευκολυνθεί, 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 εμπιστευσης κάθε κράτους μέλους.

<sup>(5)</sup> Όπως ορίζονται στο άρθρο 2 παράγραφος 10 της οδηγίας 1999/93/ΕΚ.

<sup>(6)</sup> Όπως ορίζεται στο άρθρο 2 παράγραφος 6 της οδηγίας 1999/93/ΕΚ.

<sup>(7)</sup> ETSI TS 119 612 v1.1.1 (2013-06) — Ηλεκτρονικές υπογραφές και υποδομές (Electronic Signatures and Infrastructures — ESI)-κατάλογοι εμπιστευσης.

5. για κάθε καταγεγραμμένη εποπτευόμενη/διαπιστευμένη υπηρεσία πιστοποίησης, τις πληροφορίες για το ιστορικό της κατάστασης αυτής, κατά περίπτωση·
6. την υπογραφή που χρησιμοποιείται στον κατάλογο εμπιστευσης.

Στο πλαίσιο ενός CSP που εκδίδει QC, η δομή του καταλόγου εμπιστευσης και, ειδικότερα, το μέρος των πληροφοριών υπηρεσιών (όπως αναφέρεται στο σημείο 4 παραπάνω) επιτρέπει την παροχή συμπληρωματικών πληροφοριών σε επεκτάσεις πληροφοριών υπηρεσίας ως επανόρθωση για τις καταστάσεις όπου διατίθενται ανεπαρκείς (μηχανικά επεξεργασμένες) πληροφορίες στο αναγνωρισμένο πιστοποιητικό σχετικά με την κατάσταση «αναγνώρισης» του, την ενδεχόμενη υποστήριξή του από μια SSCD και ειδικά προκειμένου να αντιμετωπιστεί το πρόσθετο γεγονός ότι οι περισσότεροι από τους (εμπορικούς) CSP χρησιμοποιούν μια ενιαία αναγνωρισμένη εκδίδουσα αρχή πιστοποίησης (CA) για την έκδοση πολλών τύπων πιστοποιητικών για οντότητες-τελικούς αποδέκτες, αναγνωρισμένων και μη.

Στο πλαίσιο των υπηρεσιών έκδοσης πιστοποιητικών (CA), ο αριθμός των καταχωρίσεων υπηρεσιών στον κατάλογο για έναν CSP μπορεί να μειωθεί στην περίπτωση που υπάρχουν μία ή περισσότερες υπηρεσίες CA ανώτερης βαθμίδας εντός της υποδομής δημόσιου κλειδιού (Public Key Infrastructure — PKI) του CSP (π.χ. στο πλαίσιο μιας ιεραρχίας CA από μια CA βάσης μέχρι αρκετές εκδίδουσες CA) καταγράφοντας αυτές τις υπηρεσίες CA ανώτερης βαθμίδας και όχι τις υπηρεσίες CA που εκδίδουν πιστοποιητικά για οντότητες-τελικούς αποδέκτες (π.χ. καταγραφή μόνο της CA βάσης του CSP). Ωστόσο, στις περιπτώσεις αυτές, οι πληροφορίες για την κατάσταση αφορούν ολόκληρη την ιεραρχία των υπηρεσιών CA κάτω από την καταγεγραμμένη υπηρεσία και πρέπει να τηρηθεί και να εξασφαλιστεί η αρχή διασφάλισης του αδιαμφισβήτητου δεσμού μεταξύ μιας υπηρεσίας πιστοποίησης CSP<sub>QC</sub> και του συνόλου των πιστοποιητικών που προορίζονται να αναγνωριστούν ως QC.

### 2.1. Περιγραφή των πληροφοριών σε κάθε κατηγορία

#### 1. Ετικέτα καταλόγου εμπιστευσης

#### 2. Πληροφορίες σχετικά με τον κατάλογο εμπιστευσης και το σχήμα έκδοσής του

Στη συγκεκριμένη κατηγορία, εντάσσονται οι παρακάτω πληροφορίες:

- **αναγνωριστικό έκδοσης μορφής** καταλόγου εμπιστευσης,
- **αριθμός αλληλουχίας (ή έκδοσης)** καταλόγου εμπιστευσης,
- **πληροφορίες τύπου του** καταλόγου εμπιστευσης (π.χ. για αναγνώριση ότι ο εν λόγω κατάλογος εμπιστευσης 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/EK),
- **πληροφορίες για τον υπεύθυνο σχήματος (κάτοχο)** του καταλόγου εμπιστευσης (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 εμπιστευσης),
- **πληροφορίες σχετικά με το υπάρχον/υπάρχοντα σχήμα/σχήματα εποπτείας/διαπίστευσης** με τα οποία σχετίζεται ο κατάλογος εμπιστευσης, 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 και/ή νομική σημείωση, αστική ευθύνη, αρμοδιότητες** όσον αφορά τον κατάλογο εμπιστευσης,
- **ημερομηνία και ώρα έκδοσης** του καταλόγου εμπιστευσης,
- **επόμενη προγραμματισμένη επικαιροποίηση** του καταλόγου εμπιστευσης.

#### 3. Αδιαμφισβήτητες πληροφορίες ταυτότητας σχετικά με κάθε εποπτευόμενο/διαπιστευμένο CSP στο πλαίσιο του σχήματος

Αυτό το σύνολο πληροφοριών περιλαμβάνει τουλάχιστον τα εξής:

- την επωνυμία του οργανισμού του CSP όπως χρησιμοποιείται στις επίσημες καταγραφές στα μητρώα (συμπεριλαμβανομένου του αναγνωριστικού 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 συμπεριλαμβάνονται είτε απευθείας είτε μέσω παραπομπής σε τόπο από όπου είναι δυνατή η μεταφόρτωση των εν λόγω επιπλέον πληροφοριών.

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

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

- Service type identifier: αναγνωριστικό του τύπου της υπηρεσίας πιστοποίησης (π.χ. αναγνωριστικό το οποίο δηλώνει ότι η εποπτευόμενη/διαπιστευμένη υπηρεσία πιστοποίησης του CSP είναι μια αρχή πιστοποίησης που εκδίδει QC),
- Service (trade) name: (εμπορική) επωνυμία της εν λόγω υπηρεσίας πιστοποίησης,
- Service digital identity: αδιαμφισβήτητο μοναδικό αναγνωριστικό της υπηρεσίας πιστοποίησης,
- Service current status: αναγνωριστικό της τρέχουσας κατάστασης της υπηρεσίας,
- Η ημερομηνία και ώρα έναρξης της τρέχουσας κατάστασης,
- Service information extension, κατά περίπτωση: επιπλέον πληροφορίες σχετικά με την υπηρεσία (π.χ. που συμπεριλαμβάνονται απευθείας ή μέσω παραπομπής σε τόπο από όπου είναι δυνατή η μεταφόρτωση των πληροφοριών): πληροφορίες καθορισμού υπηρεσίας παρεχόμενες από τον υπεύθυνο σχήματος, πληροφορίες πρόσβασης όσον αφορά την υπηρεσία, πληροφορίες καθορισμού υπηρεσίας παρεχόμενες από τον CSP και επεκτάσεις πληροφοριών υπηρεσίας. Π.χ. για υπηρεσίες CA/QC, μια προαιρετική σειρά πλειάδων πληροφοριών, όπου κάθε πλειάδα παρέχει:
  - ο κριτήρια τα οποία θα χρησιμοποιούνται για την περαιτέρω αναγνώριση (φιλτράρισμα), στο πλαίσιο της αναγνωρισμένης υπηρεσίας εμπιστευσης, του ακριβούς συνόλου αποτελεσμάτων υπηρεσίας (π.χ. του συνόλου (αναγνωρισμένων) πιστοποιητικών) για την οποία απαιτούνται/παρέχονται επιπλέον πληροφορίες όσον αφορά την κατάσταση της, τη δήλωση της υποστήριξης από SSCD και/ή την έκδοση υπέρ νομικού προσώπου και
  - ο τους συνδεδεμένους «προσδιοριστές» που παρέχουν πληροφορίες σχετικά με το εάν το σύνολο των αποτελεσμάτων υπηρεσίας ταυτοποιεί πιστοποιητικά που πρέπει να θεωρούνται αναγνωρισμένα και/ή εάν τα ταυτοποιημένα αναγνωρισμένα πιστοποιητικά από την υπηρεσία αυτήν υποστηρίζονται από SSCD, και/ή πληροφορίες σχετικά με το εάν τα QC εκδίδονται υπέρ νομικού προσώπου (εξ ορισμού πρέπει να θεωρείται ότι εκδίδονται υπέρ φυσικών προσώπων).

5. Για κάθε καταγεγραμμένη υπηρεσία πιστοποίησης, πληροφορίες ιστορικού για την κατάσταση της.

6. Μια υπογραφή υπολογισμένη για σκοπούς επαλήθευσης της ταυτότητας σε όλα τα πεδία του καταλόγου εμπιστευσης (trusted list, TL), εκτός από την ίδια την τιμή της υπογραφής.

### 3. Κατευθυντήριες γραμμές για την επεξεργασία καταχωρίσεων στον κατάλογο εμπιστευσης

- 3.1. Πληροφορίες για την κατάσταση εποπτευόμενων/διαπιστευμένων υπηρεσιών πιστοποίησης και των παρόχων τους σε έναν ενιαίο κατάλογο

Ο κατάλογος εμπιστευσης ενός κράτους μέλους είναι 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/EK».

Ένας τέτοιος κατάλογος εμπιστευσης είναι το μόνο μέσο που πρέπει να χρησιμοποιεί το οικείο κράτος μέλος για την παροχή πληροφοριών σχετικά με την κατάσταση εποπτείας/διαπίστευσης των υπηρεσιών πιστοποίησης και των παρόχων τους:

- **όλων των παρόχων υπηρεσιών πιστοποίησης**, όπως ορίζεται ο πάροχος υπηρεσιών πιστοποίησης στο άρθρο 2 παράγραφος 11 της οδηγίας 1999/93/EK, δηλαδή «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 της οδηγίας 1999/93/EK.

Αν εξεταστούν οι ορισμοί και οι διατάξεις που ορίζονται στην οδηγία 1999/93/EK, ιδίως όσον αφορά τους συναφείς CSP και τα συστήματα εποπτείας/εθελοντικής διαπίστευσης τους, μπορεί να γίνει διάκριση σε δύο ομάδες CSP: τους CSP που εκδίδουν QC για το κοινό (CSP<sub>QC</sub>), και τους CSP που δεν εκδίδουν QC για το κοινό, αλλά 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/EK, 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, ιδίως εκείνες που ορίζονται στο άρθρο 3 παράγραφος 3, το άρθρο 8 παράγραφος 1, το άρθρο 11, στην αιτιολογική σκέψη 13 [αντίστοιχα, άρθρο 2 παράγραφος 13, άρθρο 3 παράγραφος 2, άρθρο 7 παράγραφος 1 στοιχείο α), άρθρο 8 παράγραφος 1, άρθρο 11, αιτιολογικές σκέψεις 4, 11, 12 και 13].
- **CSP που δεν εκδίδουν QC:**
  - Μπορούν να εμπίπτουν σε ένα σύστημα «εθελοντικής διαπίστευσης» (όπως ορίζεται στην οδηγία 1999/93/ΕΚ και σε συμμόρφωση με αυτήν) και/ή 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 εν λόγω οδηγία και ενδεχομένως με τις εθνικές διατάξεις όσον αφορά την παροχή υπηρεσιών πιστοποίησης (κατά την έννοια του άρθρου 2 παράγραφος 11 της οδηγίας 1999/93/ΕΚ).
  - Ορισμένα από τα φυσικά ή ψηφιακά (λογικά) αντικείμενα που δημιουργούνται ή εκδίδονται ως αποτέλεσμα της παροχής μιας υπηρεσίας πιστοποίησης μπορεί να δικαιούνται ειδική «αναγνώριση» βάσει της συμμόρφωσής τους με τις διατάξεις και τις απαιτήσεις που ορίζονται σε εθνικό επίπεδο, αλλά η έννοια αυτής της «αναγνώρισης» ενδέχεται να περιορίζεται αποκλειστικά σε εθνικό επίπεδο.

Πρέπει να καταρτίζεται και να τηρείται μόνο ένας ενιαίος κατάλογος εμπιστευσης ανά κράτος μέλος, προκειμένου να δηλώνεται η κατάσταση εποπτείας και/ή διαπίστευσης των υπηρεσιών πιστοποίησης από τους CSP που εποπτεύονται/διαπιστεύονται από το κράτος μέλος. Ο κατάλογος εμπιστευσης περιλαμβάνει τουλάχιστον τους CSP που εκδίδουν QC. Ο κατάλογος εμπιστευσης μπορεί επίσης να δηλώνει την κατάσταση άλλων υπηρεσιών πιστοποίησης που εποπτεύονται ή διαπιστεύονται στο πλαίσιο ενός εθνικά καθορισμένου σχήματος έγκρισης.

### 3.2. Ενιαίο σύνολο τιμών κατάστασης εποπτείας/διαπίστευσης

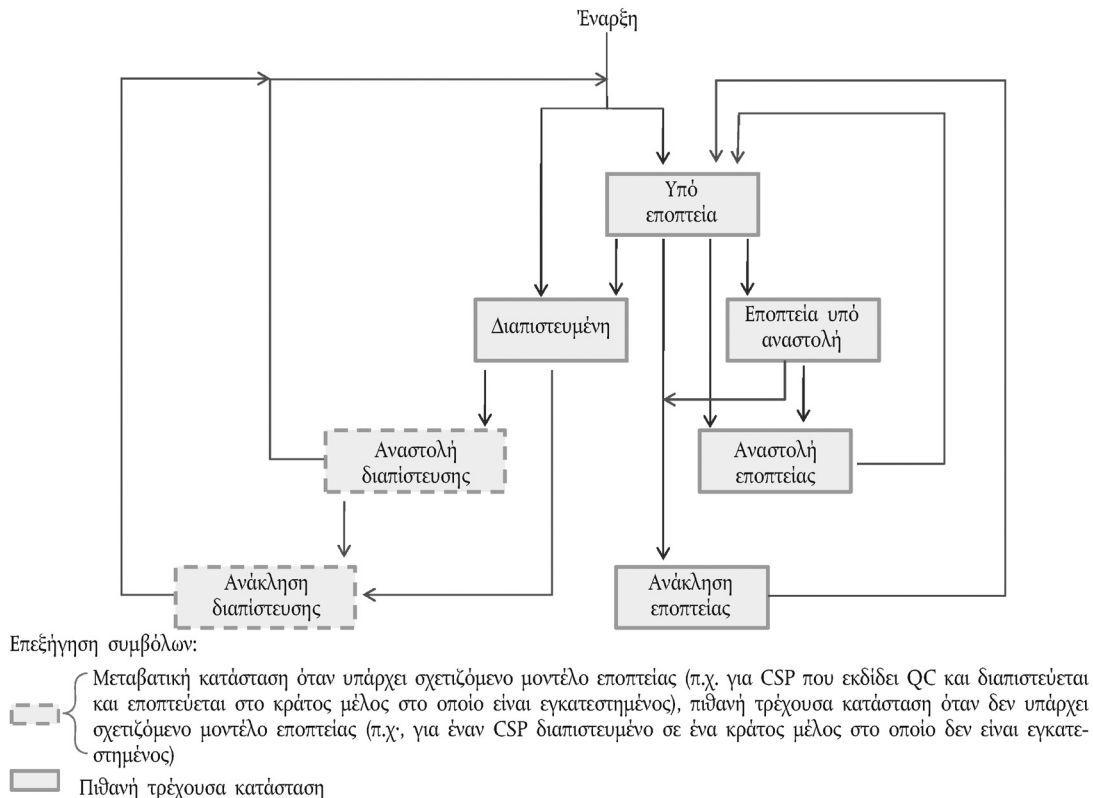
Στον κατάλογο εμπιστευσης, το εάν η υπηρεσία υπόκειται επί του παρόντος σε «εποπτεία» ή σε «διαπίστευση» δηλώνεται από την τιμή της τρέχουσας κατάστασής της. Επιπλέον, μια κατάσταση εποπτείας ή διαπίστευσης μπορεί να είναι θετική [«under supervision» (υπό εποπτεία), «accredited» (διαπιστευμένη), «supervision in cessation» (εποπτεία υπό αναστολή)], να δηλώνει αναστολή [«supervision ceased» (αναστολή εποπτείας), «accreditation ceased» (αναστολή διαπίστευσης)] ή ακόμη και ανάκληση [«supervision revoked» (ανάκληση εποπτείας), «accreditation revoked» (ανάκληση διαπίστευσης)] και να οριστεί στην αντίστοιχη τιμή. Σε όλη τη διάρκεια της ζωής της, η ίδια υπηρεσία πιστοποίησης μπορεί να μεταβαίνει από κατάσταση εποπτείας σε κατάσταση διαπίστευσης και αντίστροφα <sup>(1)</sup>.

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 που είναι εγκατεστημένος σε ένα κράτος μέλος και παρέχει μια υπηρεσία πιστοποίησης που αρχικά εποπτεύεται από το κράτος μέλος (φορέας εποπτείας), μπορεί, μετά την πάροδο ορισμένου χρονικού διαστήματος, να αποφασίσει να προβεί σε εθελοντική διαπίστευση για την υπηρεσία πιστοποίησης που εποπτεύεται επί του παρόντος. Αντίστροφα, 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 και/ή οικονομικούς λόγους.

Διάγραμμα 1

## Αναμενόμενη ροή καταστάσεων εποπτείας/διαπίστευσης για μία ενιαία υπηρεσία CSP



Όταν είναι εγκατεστημένη σε ένα κράτος μέλος, μια υπηρεσία πιστοποίησης που εκδίδει QC πρέπει να εποπτεύεται (από το κράτος μέλος στο οποίο είναι εγκατεστημένη) και δύναται να διαπιστευθεί εθελοντικά. Η κατάσταση μιας τέτοιας υπηρεσίας όταν συγκαταλέγεται σε έναν κατάλογο εμπιστευσης πρέπει να λάβει μια από τις προαναφερθείσες καταστάσεις ως «τιμή τρέχουσας κατάστασης» σύμφωνα με την πραγματική κατάστασή της και η κατάσταση της πρέπει να αλλάζει, κατά περίπτωση, βάσει της ροής κατάστασης που απεικονίζεται παραπάνω. Ωστόσο, οι τιμές «Accreditation ceased» (Αναστολή διαπίστευσης) και «Accreditation revoked» (Ανάκληση διαπίστευσης) πρέπει να είναι και οι δύο τιμές «μεταβατικής κατάστασης» όταν η αντίστοιχη υπηρεσία CSP<sub>QC</sub> συγκαταλέγεται στον κατάλογο εμπιστευσης του κράτους μέλους στο οποίο είναι εγκατεστημένη, καθώς μια τέτοια υπηρεσία πρέπει να εποπτεύεται εξ ορισμού (ακόμη και όταν δεν είναι πλέον διαπιστευμένη)· όταν η αντίστοιχη υπηρεσία συγκαταλέγεται (είναι διαπιστευμένη) σε άλλο κράτος μέλος από αυτό όπου είναι εγκατεστημένη, αυτές οι τιμές μπορεί να είναι οι τελικές.

Τα κράτη μέλη που θεσπίζουν ή έχουν θεσπίσει «αναγνωρισμένο σχήμα/αναγνωρισμένα σχήματα έγκρισης», τα οποία εφαρμόζονται σε εθνική βάση για την εποπτεία της συμμόρφωσης υπηρεσιών από CSP που **δεν** εκδίδουν QC σύμφωνα με τις διατάξεις της οδηγίας 1999/93/ΕΚ και ενδεχομένως με τις εθνικές διατάξεις σχετικά με την παροχή υπηρεσιών πιστοποίησης (κατά την έννοια του άρθρου 2 παράγραφος 11 της οδηγίας 1999/93/ΕΚ), πρέπει να κατατάξουν το/τα εν λόγω σχήμα/σχήματα στις δύο παρακάτω κατηγορίες:

- «εθελοντική διαπίστευση», όπως ορίζεται από την οδηγία 1999/93/ΕΚ και διέπεται από τις διατάξεις της [άρθρο 2 παράγραφος 13, άρθρο 3 παράγραφος 2, άρθρο 7 παράγραφος 1 στοιχείο α), άρθρο 8 παράγραφος 1, άρθρο 11, αιτιολογικές σκέψεις 4, 11, 12 και 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.

Επομένως, μια υπηρεσία πιστοποίησης που δεν εκδίδει αναγνωρισμένα πιστοποιητικά δύναται να εποπτεύεται ή να διαπιστεύεται εθελοντικά. Η κατάσταση μιας τέτοιας υπηρεσίας όταν συγκαταλέγεται σε έναν κατάλογο εμπιστευσης πρέπει να λάβει μία από τις παραπάνω καταστάσεις ως «τιμή τρέχουσας κατάστασης» (βλέπε το διάγραμμα 1) σύμφωνα με την πραγματική κατάστασή της και πρέπει να εξελίσσεται, κατά περίπτωση, βάσει της ροής κατάστασης που απεικονίζεται παραπάνω.

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

- πληροφορίες σχετικά με το σύστημα εποπτείας που ισχύει για κάθε CSP<sub>QC</sub>.
- πληροφορίες, όταν υπάρχουν, για το εθνικό σχήμα «εθελοντικής διαπίστευσης» που ισχύει για κάθε CSP<sub>QC</sub>.
- 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 κείρας 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 καταλόγου εμπιστευσης όσον αφορά τις υπηρεσίες των CSP που δεν εκδίδουν QC, τα προαναφερθέντα σύνολα πληροφοριών πρέπει να παρέχονται σε επίπεδο καταλόγου εμπιστευσης μέσω της χρήσης του «Scheme information URI» (URI πληροφοριών σχήματος) (διάταξη 5.3.7 — πληροφορίες που παρέχουν τα κράτη μέλη), του «Scheme type/community/rules» (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 «TSL policy/legal notice» (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).

Πρόσθετες πληροφορίες «αναγνώρισης» που ορίζονται στο επίπεδο των εθνικών συστημάτων εποπτείας/διαπίστευσης για τους CSP που δεν εκδίδουν QC μπορούν να παρέχονται στο επίπεδο υπηρεσιών όταν υπάρχουν και απαιτούνται (π.χ. για να γίνει διάκριση μεταξύ πολλών επιπέδων ποιότητας/ασφάλειας) μέσω της χρήσης της τιμής «additionalServiceInformation Extension» (διάταξη 5.5.9.4) στο πλαίσιο της «Service information extensions» (Επεκτάσεις πληροφοριών υπηρεσίας) (διάταξη 5.5.9). Περαιτέρω πληροφορίες σχετικά με τις αντίστοιχες τεχνικές προδιαγραφές παρέχονται στις αναλυτικές προδιαγραφές στο κεφάλαιο I.

Παρότι ενδέχεται ξεχωριστοί 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 και να επικαιροποιείται αναλόγως η κατάσταση εποπτείας/διαπίστευσης της.

### 3.3. Καταχωρίσεις καταλόγου εμπιστευσης με στόχο τη διευκόλυνση της επικύρωσης των προηγμένων ηλεκτρονικών υπογραφών (QES) και των προηγμένων ηλεκτρονικών υπογραφών που υποστηρίζονται από αναγνωρισμένο πιστοποιητικό (AdES<sub>QC</sub>)

Το πιο κρίσιμο μέρος της δημιουργίας του καταλόγου εμπιστευσης είναι η κατάρτιση του υποχρεωτικού του μέρους, δηλαδή του «Καταλόγου υπηρεσιών» ανά CSP που εκδίδει QC, προκειμένου να παρουσιάζεται ορθά η ακριβής κατάσταση κάθε υπηρεσίας πιστοποίησης που εκδίδει QC και να διασφαλίζεται ότι οι πληροφορίες που παρέχονται μέσω κάθε καταχώρισης επαρκούν για τη διευκόλυνση της επικύρωσης των QES και των AdES<sub>QC</sub> (σε συνδυασμό με το περιεχόμενο του QC για την οντότητα-τελικό αποδέκτη το οποίο εκδίδεται από τον CSP στο πλαίσιο της υπηρεσίας πιστοποίησης που αναγράφεται στην εν λόγω καταχώριση).

Στις απαραίτητες πληροφορίες ενδέχεται να συμπεριλαμβάνονται κι άλλες πληροφορίες εκτός από την «Service digital identity» (Ψηφιακή ταυτότητα υπηρεσίας) μιας ενιαίας CA (βάσης) και συγκεκριμένα πληροφορίες που ορίζουν την κατάσταση QC των πιστοποιητικών που εκδίδονται από την εν λόγω υπηρεσία CA και πληροφορίες για το αν οι υποστηριζόμενες υπογραφές δημιουργούνται από μια SSCD ή όχι. Επομένως, ο φορέας ενός κράτους μέλους που είναι υπεύθυνος για την κατάρτιση, την επεξεργασία και την τήρηση του καταλόγου εμπιστευσης πρέπει να λαμβάνει υπόψη το τρέχον προφίλ και το περιεχόμενο πιστοποιητικού κάθε εκδιδόμενου QC, ανά υπηρεσία CSP<sub>QC</sub> που συμπεριλαμβάνεται στον κατάλογο εμπιστευσης.

Ιδανικά, κάθε εκδιδόμενο QC θα πρέπει να συμπεριλαμβάνει την οριζόμενη από το ETSI δήλωση QcCompliance<sup>(1)</sup> όταν εκφράζεται ο ισχυρισμός ότι είναι QC και θα πρέπει να συμπεριλαμβάνει την οριζόμενη από το ETSI δήλωση QcSSCD όταν εκφράζεται ο ισχυρισμός ότι υποστηρίζεται από μια SSCD για τη δημιουργία ηλεκτρονικών υπογραφών και/ή ότι κάθε εκδιδόμενο QC συμπεριλαμβάνει ένα από τα QCP/QCP+, τα αναγνωριστικά αντικείμενα πολιτικής πιστοποιητικού (OID), τα οποία ορίζονται στις τεχνικές προδιαγραφές ETSI EN 319 411-2<sup>(2)</sup>. Το γεγονός ότι οι CSP που εκδίδουν QC χρησιμοποιούν διαφορετικά πρότυπα ως αναφορές, το ευρύ πεδίο ερμηνείας των εν λόγω προτύπων, καθώς και η μη επίγνωση της ύπαρξης και του προηγούμενου ορισμένων κανονιστικών τεχνικών προδιαγραφών ή προτύπων είχαν ως αποτέλεσμα να διαπιστώνονται διαφορές στο πραγματικό περιεχόμενο των QC που εκδίδονται επί του παρόντος (π.χ. η χρήση ή η μη χρήση των εν λόγω δηλώσεων QcStatements που ορίζονται στο ETSI) και, κατά συνέπεια, να μην επιτρέπεται στον αποδέκτη να βασίζεται απλά στο πιστοποιητικό του υπογράφοντος (και στη συνδεδεμένη αλυσίδα/διαδρομή) για να αξιολογήσει, τουλάχιστον με μηχανικά αναγνώσιμο τρόπο, αν για το πιστοποιητικό που υποστηρίζει ηλεκτρονική υπογραφή εκφράζεται ο ισχυρισμός ότι αποτελεί QC και αν το πιστοποιητικό αυτό συνδέεται με μια SSCD μέσω της οποίας δημιουργήθηκε η ηλεκτρονική υπογραφή.

<sup>(1)</sup> Ανατρέξτε στο ETSI EN 319 412-5 (Ηλεκτρονικές Υπογραφές και Υποδομές (ESI)- Προφίλ για παρόχους υπηρεσιών εμπιστευσης που εκδίδουν πιστοποιητικά, Μέρος 5: προφίλ επέκτασης για αναγνωρισμένο πιστοποιητικό) για τον ορισμό με τέτοιας δήλωσης.

<sup>(2)</sup> ETSI EN 319 411-2 — Ηλεκτρονικές Υπογραφές και Υποδομές (ESI)- Προφίλ για παρόχους υπηρεσιών εμπιστευσης που εκδίδουν πιστοποιητικά, Μέρος 2: Απαιτήσεις πολιτικής για τις αρχές πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά.



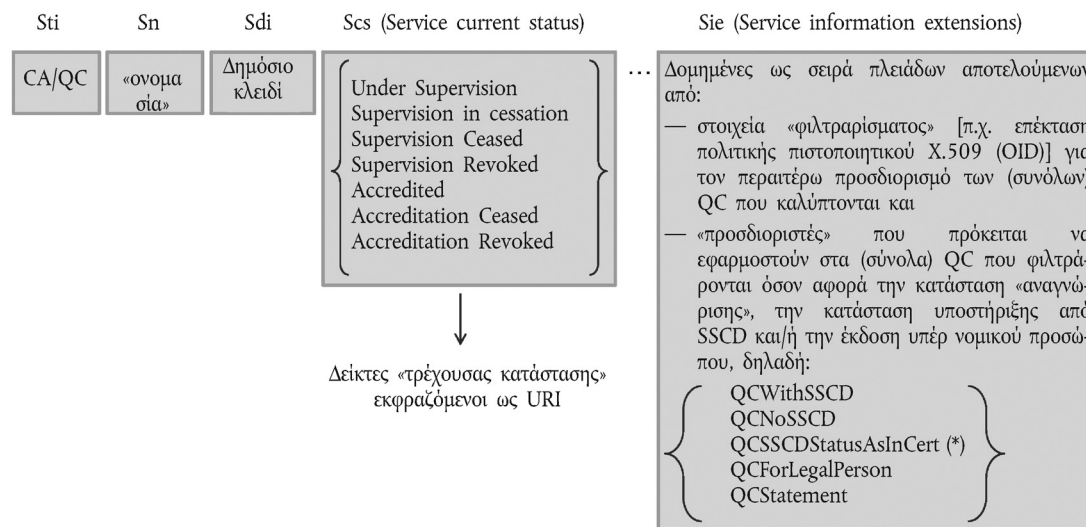
Η συμπλήρωση των πεδίων της καταχώρισης υπηρεσίας «Αναγνωριστικό τύπου υπηρεσίας» (Service type identifier — «Sti»), «Όνομασία υπηρεσίας» (Service name — «Sn») και «Ψηφιακή ταυτότητα υπηρεσίας» (Service digital identity — «Sdi») στον κατάλογο εμπιστευσης με τις πληροφορίες που παρέχονται από το πεδίο «Επεκτάσεις πληροφοριών υπηρεσίας» (Service information extensions — «Sie») επιτρέπει τον πλήρη καθορισμό ενός συγκεκριμένου τύπου αναγνωρισμένου πιστοποιητικού που εκδίδεται από μια καταγεγραμμένη υπηρεσία πιστοποίησης CSP που εκδίδει QC και παρέχει πληροφορίες σχετικά με το αν υποστηρίζεται ή όχι από SSCD (όταν οι πληροφορίες αυτές λείπουν από το εκδιδόμενο QC). Με αυτήν την καταχώριση συνδέονται πληροφορίες για μια συγκεκριμένη «Τρέχουσα κατάσταση υπηρεσίας» (Service current status — «Scs»). Αυτό απεικονίζεται στο διάγραμμα 2 που ακολουθεί.

Η καταγραφή μιας υπηρεσίας παρέχοντας απλά το «Sdi» μιας CA (βάσης) σημαίνει ότι διασφαλίζεται (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 (ιεραρχίας) CA (βάσης) περιέχει αρκετές οριζόμενες από το ETSI και μηχανικά επεξεργασίες πληροφορίες ώστε να αξιολογείται αν πρόκειται για QC ή αν υποστηρίζεται από SSCD. Σε περίπτωση, για παράδειγμα, που η τελευταία πρόταση δεν ισχύει (π.χ. αν δεν υπάρχει στο QC μηχανικά επεξεργασίμη δήλωση τυποποιημένη βάσει του ETSI σχετικά με το αν υποστηρίζεται από SSCD), τότε καταγράφοντας μόνο το «Sdi» της εν λόγω CA (βάσης) το μόνο συμπέρασμα που μπορεί να εξαχθεί είναι ότι τα QC που εκδόθηκαν σύμφωνα με την εν λόγω ιεραρχία CA (βάσης) δεν υποστηρίζονται από καμία SSCD. Για να δηλωθεί ότι τα εν λόγω QC πρέπει να θεωρείται ότι υποστηρίζονται από SSCD, θα πρέπει να χρησιμοποιηθεί το πεδίο «Sie» (κάτι που δηλώνει επίσης ότι για αυτές τις πληροφορίες παρέχει εγγυήσεις ο CSP που εκδίδει QC και εποπτεύεται/διαπιστεύεται από τον φορέα εποπτείας ή διαπίστευσης αντίστοιχα).

Διάγραμμα 2

**Καταχώριση υπηρεσίας καταγεγραμμένου CSP που εκδίδει QC στον κατάλογο εμπιστευσης**  
**Γενικές αρχές — Κανόνες επεξεργασίας — Καταχωρίσεις CSP<sub>QC</sub> (καταγεγραμμένες υπηρεσίες)**

Καταχώριση υπηρεσίας για καταγεγραμμένο CSP<sub>QC</sub>:



(\*) η ένδειξη αυτή σημαίνει ότι οι εν λόγω πληροφορίες είναι βέβαιο ότι περιλαμβάνονται σε οποιοδήποτε QC που εκδίδει CA/QC και προσδιορίζεται από Sdi-[Sie] (εάν δεν υπάρχει τίποτα στο QC, τότε πρόκειται για NoSSCD)

Οι παρούσες τεχνικές προδιαγραφές του κοινού σχεδιασμού του καταλόγου εμπιστευσης επιτρέπουν τη χρήση ενός συνδυασμού πέντε κυρίων μερών πληροφοριών στην καταχώριση της υπηρεσίας:

- το «Αναγνωριστικό τύπου υπηρεσίας» (Service type identifier — «Sti»), π.χ. με το οποίο αναγνωρίζεται μια CA που εκδίδει QC («CA/QC»).
- την «Όνομασία υπηρεσίας» (Service name, «Sn»).
- τις πληροφορίες «Ψηφιακή ταυτότητα υπηρεσίας» (Service digital identity — «Sdi»), οι οποίες ταυτοποιούν μια καταγεγραμμένη υπηρεσία, π.χ. το δημόσιο κλειδί (κατ' ελάχιστον) μιας CA που εκδίδει QC.

- για υπηρεσίες CA/QC, προαιρετικές πληροφορίες «Επέκταση πληροφοριών υπηρεσίας» (Service information extension — «Sie»), οι οποίες επιτρέπουν να συμπεριληφθούν αρκετά στοιχεία πληροφοριών σχετικών με τη συγκεκριμένη υπηρεσία και αφορούν την κατάσταση ανάκλησης πιστοποιητικών που έχουν λήξει, πρόσθετα χαρακτηριστικά QC, εξαγορά ενός CSP από άλλον CSP, καθώς και άλλες πρόσθετες πληροφορίες υπηρεσίας. Για παράδειγμα, τα πρόσθετα χαρακτηριστικά των QC δηλώνονται με μια αλληλουχία μιας ή περισσότερων πλειάδων, καθεμία από τις οποίες παρέχει:
  - κριτήρια τα οποία χρησιμοποιούνται για την περαιτέρω αναγνώριση (φιλτράρισμα) στο πεδίο «Sdi» του ακριβούς συνόλου αναγνωρισμένων πιστοποιητικών για τα οποία απαιτούνται/παρέχονται επιπλέον πληροφορίες, όσον αφορά την ένδειξη της κατάστασης «αναγνώρισης», την υποστήριξη από SSCD και/ή την έκδοση υπέρ νομικού προσώπου και
  - τις συνδεδεμένες πληροφορίες («προσδιοριστές») σχετικά με το αν αυτό το σύνολο αναγνωρισμένων πιστοποιητικών πρέπει να θεωρείται «αναγνωρισμένο», υποστηρίζεται ή όχι από μια SSCD ή σχετικά με το αν οι εν λόγω συνδεδεμένες πληροφορίες αποτελούν μέρος του QC βάσει τυποποιημένης μηχανικά επεξεργάσιμης μορφής, και/ή 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).
- 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.

#### 3.4. Κατευθυντήριες γραμμές επεξεργασίας και χρήσης για τις καταχωρίσεις υπηρεσιών CSP<sub>QC</sub>

Οι γενικές κατευθυντήριες γραμμές επεξεργασίας είναι οι εξής:

1. Αν διασφαλίζεται [η εγγύηση παρέχεται από τον CSP<sub>QC</sub> 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 τη δήλωση QcSSCD και/ή το QCP + αναγνωριστικό αντικειμένου (Object Identifier — OID), τότε η χρήση ενός κατάλληλου «Sdi» αρκεί και το πεδίο «Sie» μπορεί να χρησιμοποιηθεί προαιρετικά και δεν είναι απαραίτητο να περιέχει πληροφορίες υποστήριξης από SSCD.
2. Αν διασφαλίζεται (η εγγύηση παρέχεται από τον CSP<sub>QC</sub> και εποπτεύεται/διαπιστεύεται από τον SB/AB) ότι, για μια καταγεγραμμένη υπηρεσία που προσδιορίζεται με «Sdi», οποιοδήποτε QC που δεν υποστηρίζεται από μια SSCD περιέχει τη δήλωση συμμόρφωσης QcCompliance και/ή το QCP OID, και δεν περιλαμβάνει τη δήλωση QcSSCD ή το QCP + OID, τότε η χρήση ενός κατάλληλου «Sdi» αρκεί και το πεδίο «Sie» μπορεί να χρησιμοποιηθεί προαιρετικά και δεν είναι απαραίτητο να περιέχει πληροφορίες υποστήριξης από SSCD (πράγμα που σημαίνει ότι δεν υποστηρίζεται από SSCD).
3. Αν διασφαλίζεται (η εγγύηση παρέχεται από τον CSP<sub>QC</sub> και εποπτεύεται/διαπιστεύεται από τον SB/AB) ότι, για μια καταγεγραμμένη υπηρεσία που προσδιορίζεται με «Sdi», οποιοδήποτε QC περιέχει τη δήλωση συμμόρφωσης QcCompliance, και ορισμένα από αυτά τα QC πρέπει να υποστηρίζονται από SSCD, ενώ κάποια άλλα όχι (π.χ. μπορεί να γίνει αυτή η διάκριση μέσω διαφορετικών OID πολιτικής πιστοποιητικού ανά CSP ή μέσω άλλων πληροφοριών για κάθε CSP στο QC, άμεσα ή έμμεσα, με ή χωρίς δυνατότητα επεξεργασίας με μηχανικά μέσα), αλλά ένα πιστοποιητικό που υποστηρίζεται από SSCD δεν περιέχει ΟΥΤΕ τη δήλωση QcSSCD ΟΥΤΕ το QCP(+) OID του ETSI, τότε η χρήση ενός κατάλληλου «Sdi» ενδέχεται να μην αρκεί ΚΑΙ πρέπει να χρησιμοποιηθεί το πεδίο «Sie» για να παράσχει ρητές πληροφορίες υποστήριξης από SSCD, καθώς και μια πιθανή επέκταση πληροφοριών για την αναγνώριση του καλυπτόμενου συνόλου πιστοποιητικών. Για αυτό ενδέχεται να απαιτηθεί να συμπεριληφθούν διαφορετικές «τιμές πληροφοριών υποστήριξης από SSCD» για το ίδιο «Sdi», όταν γίνεται χρήση του πεδίου «Sie».
4. Αν διασφαλίζεται (η εγγύηση παρέχεται από τον CSP<sub>QC</sub> και εποπτεύεται/διαπιστεύεται από τον SB/AB) ότι, για μια καταγεγραμμένη υπηρεσία η οποία προσδιορίζεται με «Sdi», οποιοδήποτε QC δεν περιέχει δήλωση συμμόρφωσης QcCompliance, QCP OID, δήλωση QcSSCD, ή QCP + OID, αλλά διασφαλίζεται ότι ορισμένα από αυτά τα πιστοποιητικά για οντότητες-τελικούς αποδέκτες που εκδίδονται βάσει του εν λόγω «Sdi» πρέπει να είναι QC και/ή να υποστηρίζονται από SSCD, ενώ κάποια άλλα όχι (π.χ. μπορεί να γίνει αυτή η διάκριση μέσω διαφορετικών OID πολιτικών πιστοποιητικού ανά CSP<sub>QC</sub> ή μέσω άλλων πληροφοριών για κάθε CSP<sub>QC</sub> στο QC, άμεσα ή έμμεσα, με ή χωρίς δυνατότητα επεξεργασίας με μηχανικά μέσα), τότε η χρήση ενός κατάλληλου «Sdi» δεν θα αρκεί ΚΑΙ πρέπει να χρησιμοποιηθεί το πεδίο «Sie» για να συμπεριληφθούν ρητές πληροφορίες αναγνώρισης. Γι' αυτό ενδέχεται να απαιτηθεί να συμπεριληφθούν διαφορετικές «τιμές πληροφοριών με υποστήριξη από SSCD» για το ίδιο «Sdi», όταν γίνεται χρήση του πεδίου «Sie».

Ως γενική εξ' ορισμού αρχή, για έναν CSP ο οποίος είναι καταγεγραμμένος στον κατάλογο εμπιστευσης, πρέπει να υπάρχει μια καταχώριση υπηρεσίας ανά δημόσιο κλειδί για μια υπηρεσία πιστοποίησης τύπου CA/QC, δηλαδή ανά αρχή πιστοποίησης που εκδίδει (άμεσα) QC. Σε ορισμένες εξαιρετικές περιπτώσεις και υπό προσεκτικά ρυθμιζόμενες συνθήκες, ο φορέας εποπτείας/διαπίστευσης ενός κράτους μέλους δύναται να αποφασίσει να χρησιμοποιήσει, ως το «Sdi» μιας ενιαίας καταχώρισης στον

κατάλογο υπηρεσιών αυτού του καταγεγραμμένου CSP, το δημόσιο κλειδί μιας CA βάσης ή ανώτερου επιπέδου στο πλαίσιο της PKI του CSP (π.χ. στο πλαίσιο μιας ιεραρχίας CSP με CA από μια CA βάσης μέχρι αρκετές εκδίδουσες CA), αντί να παραθέτει όλες τις κατώτερες ιεραρχικά υπηρεσίες εκδίδουσών CA (δηλαδή καταγραφή μιας αρχής πιστοποίησης η οποία δεν εκδίδει άμεσα QC για οντότητες-τελικούς αποδέκτες, αλλά η οποία πιστοποιεί μια ιεραρχία CA μέχρι εκείνες τις CA που εκδίδουν QC για οντότητες - τελικούς αποδέκτες). Οι συνέπειες (πλεονεκτήματα και μειονεκτήματα) της χρήσης του εν λόγω δημόσιου κλειδιού CA βάσης ή ανώτερου επιπέδου ως τιμής «Sdi» σε μια καταχώριση υπηρεσίας στον κατάλογο εμπιστευσης πρέπει να λαμβάνονται σοβαρά υπόψη από τα κράτη μέλη όταν την επιλέγουν. Επιπλέον, χρησιμοποιώντας αυτήν 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. Για παράδειγμα, στο πλαίσιο ενός CSP<sub>QC</sub> που χρησιμοποιεί μία CA βάσης, στο πλαίσιο της οποίας πολλές CA εκδίδουν τόσο αναγνωρισμένα όσο και μη αναγνωρισμένα QCs, 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 CA βάσης θα σήμαινε μόνο, βάσει των κανόνων που εξηγήθηκαν παραπάνω, ότι κανένα QC που εκδίδεται υπό την εν λόγω CA βάσης δεν υποστηρίζεται από SSCD. Αν υπάρχουν QC που υποστηρίζονται πράγματι από SSCD, χωρίς όμως να περιλαμβάνεται μηχανικά επεξεργάσιμη δήλωση που να αναφέρει αυτήν την υποστήριξη στα πιστοποιητικά, συνιστάται θερμά να χρησιμοποιείται η δήλωση QcSSCD στα QC που θα εκδοθούν μελλοντικά. Εν τω μεταξύ (μέχρι τη λήξη του τελευταίου QC που δεν περιέχει αυτές τις πληροφορίες), στον κατάλογο εμπιστευσης θα πρέπει να χρησιμοποιείται το πεδίο «Sie» και το συνδεδεμένο «Επέκταση προσδιορισμών» (Qualifications Extension), π.χ. παρέχοντας πληροφορίες φιλτραρίσματος για την αναγνώριση ομάδας/ομάδων πιστοποιητικών μέσω της χρήσης ειδικού/ειδικών OID που καθορίζονται από τον CSP<sub>QC</sub>, τα οποία χρησιμοποιεί ενδεχομένως ο CSP<sub>QC</sub> για να κάνει διάκριση ανάμεσα στους διάφορους τύπους QC (ορισμένα από τα οποία υποστηρίζονται από SSCD, ενώ ορισμένα άλλα όχι) και τις συνδεδεμένες ρητές «πληροφορίες υποστήριξης SSCD» για τα πιστοποιητικά που αναγνωρίζονται (φιλτράρονται) μέσω της χρήσης «Προσδιοριστών».

**Οι γενικές κατευθυντήριες γραμμές χρήσης** για τις εφαρμογές, τις υπηρεσίες ή τα προϊόντα που αφορούν τις ηλεκτρονικές υπογραφές και βασίζονται σε έναν κατάλογο διαπίστευσης σύμφωνο 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 CA με αναγνωριστικό «Sdi» (παρομοίως στο πλαίσιο της ιεραρχίας CA η οποία ξεκινά από την CA βάσης με αναγνωριστικό «Sdi»), όλα τα εκδιδόμενα πιστοποιητικά για οντότητες-τελικούς αποδέκτες είναι QC, **εφόσον** υποστηρίζεται ότι είναι τέτοια στο πιστοποιητικό μέσω της χρήσης κατάλληλης μηχανικά επεξεργάσιμης QcStatement (δηλαδή, QcCompliance) και/ή QCP(+) OID που ορίζονται από το ETSI (και αυτό διασφαλίζεται από τον φορέα εποπτείας/ διαπίστευσης, βλέπε παραπάνω τις «γενικές κατευθυντήριες γραμμές επεξεργασίας»).

*Σημείωση:* Σε περίπτωση που δεν υπάρχουν πληροφορίες «Sie» «Επέκταση προσδιορισμών» ή σε περίπτωση που ένα πιστοποιητικό για οντότητες-τελικούς αποδέκτες το οποίο υποστηρίζεται ότι είναι QC δεν αναγνωρίζεται πλέον μέσω σχετικής καταχώρισης «Sie» «Επέκταση προσδιορισμών», τότε οι μηχανικά επεξεργάσιμες πληροφορίες που βρίσκονται στο QC θεωρούνται, βάσει εποπτείας/διαπίστευσης, ακριβείς. Αυτό σημαίνει ότι η χρήση (ή μη χρήση) των κατάλληλων δηλώσεων QcStatements (δηλαδή, QcCompliance, QcSSCD) και/ή QCP(+) OID που ορίζονται από το ETSI διασφαλίζεται ότι συμφωνεί με αυτό που υποστηρίζει ο CSP<sub>QC</sub>.

- **και AN** υπάρχουν πληροφορίες «Sie» «Επέκταση προσδιορισμών», τότε εκτός από τον παραπάνω εξ ορισμού κανόνα ερμηνείας χρήσης, τα πιστοποιητικά που ορίζονται μέσω της χρήσης των εν λόγω πληροφοριών «Sie» «Επέκταση προσδιορισμών», η οποία βασίζεται στην αρχή της αλληλουχίας φίλτρων που προσδιορίζουν περαιτέρω ένα σύνολο πιστοποιητικών, πρέπει να εξετάζονται σύμφωνα με τους συσχετιζόμενους προσδιοριστές παρέχοντας ορισμένες επιπλέον πληροφορίες όσον αφορά την κατάσταση αναγνώρισης, την «υποστήριξη από SSCD» και/ή το «νομικό πρόσωπο ως υποκείμενο» (π.χ. τα πιστοποιητικά που περιέχουν συγκεκριμένο αναγνωριστικό αντικείμενο στην επέκταση της πολιτικής πιστοποιητικού και/ή έχουν συγκεκριμένη σχηματομορφή «Χρήσης κλειδιού» και/ή φιλτράρονται μέσω της χρήσης συγκεκριμένης τιμής η οποία εμφανίζεται σε ένα συγκεκριμένο πεδίο ή επέκταση του πιστοποιητικού κ.λπ.). Οι προσδιοριστές αυτοί αποτελούν μέρος του παρακάτω συνόλου «Προσδιοριστών», οι οποίοι χρησιμοποιούνται για να επανορθώσουν την έλλειψη πληροφοριών στο αντίστοιχο περιεχόμενο του QC και οι οποίοι χρησιμοποιούνται αντίστοιχα:

- για να δηλώσουν την κατάσταση αναγνώρισης: «QcStatement», η οποία σημαίνει ότι το/τα προσδιοριζόμενο/-α πιστοποιητικό/-ά είναι αναγνωρισμένα·

KAI/H

- για να δηλώσουν τη φύση της υποστήριξης από SSCD

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

- τιμή προσδιοριστή «QCNoSSCD», η οποία σημαίνει ότι 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·

KAI/H

— για να δηλώσουν έκδοση υπέρ νομικού προσώπου:

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

### 3.5. Υπηρεσίες που υποστηρίζουν υπηρεσίες «CA/QC», αλλά δεν αποτελούν μέρος των «CA/QC» «Sdi»

Η κατάσταση εγκυρότητας πιστοποιητικού που σχετίζεται με τα QC για τα οποία οι πληροφορίες κατάστασης εγκυρότητας πιστοποιητικού (π.χ. CRL και αποκρίσεις OCSP) υπογράφεται από οντότητα της οποίας το ιδιωτικό κλειδί δεν είναι πιστοποιημένο βάσει διαδρομής πιστοποίησης που καταλήγει σε καταγεγραμμένη CA που εκδίδει QC («CA/QC») συμπεριλαμβάνεται στον κατάλογο εμπιστευσης καταγράφοντας αυτές τις υπηρεσίες κατάστασης εγκυρότητας πιστοποιητικού ως τέτοιες στον TL (δηλαδή, με τύπο υπηρεσίας «OCSP/QC» ή «CRL/QC» αντίστοιχα), καθώς οι εν λόγω υπηρεσίες μπορούν να θεωρηθούν μέρος των εποπτευόμενων/διαπιστευμένων «αναγνωρισμένων» υπηρεσιών που έχουν σχέση με την παροχή υπηρεσιών πιστοποίησης QC. Ασφαλώς, οι αποκρίτες 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 «έγκυροι» 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»).

Ο κατάλογος εμπιστευσης περιλαμβάνει υπηρεσίες κατάστασης εγκυρότητας πιστοποιητικού όταν δεν υπάρχουν σχετικές πληροφορίες για τον τόπο αυτών των υπηρεσιών στα πιστοποιητικά για οντότητα-τελικό αποδέκτη τα οποία αφορούν οι υπηρεσίες κατάστασης εγκυρότητας πιστοποιητικού.

## 4. Ορισμοί και συντομογραφίες

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

Όρος	Ακρώνυμο	Ορισμός
Πάροχος υπηρεσιών πιστοποίησης	CSP	Όπως ορίζεται στο άρθρο 2 παράγραφος 11 της οδηγίας 1999/93/ΕΚ.
Αρχή πιστοποίησης	CA	1. πάροχος υπηρεσιών πιστοποίησης που δημιουργεί και χορηγεί πιστοποιητικά δημοσίου κλειδιού ή 2. τεχνική υπηρεσία δημιουργίας πιστοποιητικών που χρησιμοποιείται από έναν πάροχο υπηρεσιών πιστοποίησης που δημιουργεί και χορηγεί πιστοποιητικά δημοσίου κλειδιού. <i>ΣΗΜΕΙΩΣΗ:</i> Βλέπε τη διάταξη 4 του EN 319 411-2 (1) για περαιτέρω διευκρινίσεις σχετικά με την έννοια της αρχής πιστοποίησης.
Αρχή πιστοποίησης που εκδίδει αναγνωρισμένα πιστοποιητικά	CA/QC	Μια CA που 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 παράγραφος 9 της οδηγίας 1999/93/ΕΚ.
Αναγνωρισμένο πιστοποιητικό	QC	Όπως ορίζεται στο άρθρο 2 παράγραφος 10 της οδηγίας 1999/93/ΕΚ.
Υπογραφή	Υπογραφή	Όπως ορίζεται στο άρθρο 2 παράγραφος 3 της οδηγίας 1999/93/ΕΚ.
Εποπτεία	Εποπτεία	Αναφέρεται στην εποπτεία που προβλέπεται στο άρθρο 3 παράγραφος 3 της οδηγίας 1999/93/ΕΚ. Η οδηγία 1999/93/ΕΚ επιβάλλει στα κράτη μέλη να καθιερώσουν κατάλληλο σύστημα που καθιστά δυνατή την εποπτεία των εγκατεστημένων στο έδαφός τους CSP που εκδίδουν αναγνωρισμένα πιστοποιητικά για το κοινό, διασφαλίζοντας την εποπτεία της συμμόρφωσης προς τις διατάξεις της εν λόγω οδηγίας.
Εθελοντική διαπίστευση	Διαπίστευση	Όπως ορίζεται στο άρθρο 2 παράγραφος 13 της οδηγίας 1999/93/ΕΚ.
Κατάλογος εμπιστευσης	TL	Προσδιορίζει τον κατάλογο που δηλώνει 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.

Όρος	Ακρόνυμο	Ορισμός
Κατάλογος κατάστασης υπηρεσιών εμπιστευσης	TSL	Μορφή υπογεγραμμένου καταλόγου ο οποίος χρησιμοποιείται ως βάση για την παρουσίαση πληροφοριών για την κατάσταση των υπηρεσιών εμπιστευσης σύμφωνα με τις προδιαγραφές του ETSI TS 119 612.
Υπηρεσία εμπιστευσης		Υπηρεσία η οποία αυξάνει την αξιοπιστία των ηλεκτρονικών συναλλαγών και την εμπιστοσύνη σε αυτές (συνήθως, όχι όμως απαραίτητα, με χρήση τεχνικών κρυπτογραφίας ή με συμπερίληψη απόρρητου υλικού) (ETSI TS 119 612). <b>ΣΗΜΕΙΩΣΗ:</b> Ο συγκεκριμένος όρος είναι ευρύτερος από την υπηρεσία πιστοποίησης που εκδίδει πιστοποιητικά ή παρέχει άλλες υπηρεσίες σχετικές με τις ηλεκτρονικές υπογραφές.
Πάροχος υπηρεσιών εμπιστευσης	TSP	Φορέας ο οποίος παρέχει μία ή περισσότερες (ηλεκτρονικές) υπηρεσίες εμπιστευσης (ο όρος αυτός είναι ευρύτερος από τον «CSP»).
Αδειοδοτικό υπηρεσίας εμπιστευσης	TrST	Φυσικό ή ψηφιακό (λογικό) αντικείμενο το οποίο δημιουργείται ή εκδίδεται ως αποτέλεσμα της χρήσης μιας υπηρεσίας εμπιστευσης. Παραδείγματα ψηφιακών TrST είναι τα πιστοποιητικά, οι κατάλογοι ανάκλησης πιστοποιητικών (CRL), τα αδειοδοτικά χρονοσφράγισσης (TST) και οι αποκρίσεις πρωτοκόλλου κατάστασης πιστοποιητικού με σύνδεση (OCSP).
Αναγνωρισμένη ηλεκτρονική υπογραφή	QES	Μια AdES η οποία υποστηρίζεται από QC και η οποία δημιουργείται από μια ασφαλή διάταξη δημιουργίας υπογραφών, όπως ορίζεται στο άρθρο 2 της οδηγίας 1999/93/ΕΚ.
Προηγμένη ηλεκτρονική υπογραφή	AdES	Όπως ορίζεται στο άρθρο 2 παράγραφος 2 της οδηγίας 1999/93/ΕΚ.
Προηγμένη ηλεκτρονική υπογραφή που υποστηρίζεται από αναγνωρισμένο πιστοποιητικό	AdES <sub>QC</sub>	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 υπογραφών	SSCD	Όπως ορίζεται στο άρθρο 2 παράγραφος 6 της οδηγίας 1999/93/ΕΚ.

(<sup>1</sup>) EN 319 411-2: Ηλεκτρονικές Υπογραφές και Υποδομές (ESU)· Απαιτήσεις πολιτικής και ασφάλειας για παρόχους υπηρεσιών εμπιστευσης που εκδίδουν πιστοποιητικά· Μέρος 2: Απαιτήσεις πολιτικής για τις αρχές πιστοποίησης που εκδίδουν αναγνωρισμένα πιστοποιητικά.

Στα επόμενα κεφάλαια, οι λέξεις-κλειδιά «ΠΡΕΠΕΙ ΝΑ», «ΔΕΝ ΠΡΕΠΕΙ ΝΑ», «ΑΠΑΙΤΕΙΤΑΙ ΝΑ», «ΘΑ ΠΡΕΠΕΙ ΝΑ», «ΔΕΝ ΘΑ ΠΡΕΠΕΙ ΝΑ», «ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ», «ΔΕΝ ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ», «ΣΥΝΙΣΤΑΤΑΙ ΝΑ», «ΔΥΝΑΤΑΙ/ΔΥΝΑΝΤΑΙ ΝΑ» και «ΠΡΟΑΙΡΕΤΙΚΑ» πρέπει να ερμηνεύονται όπως περιγράφεται στο RFC (αίτηση για σχολιασμό) 2119 (<sup>1</sup>).

## ΚΕΦΑΛΑΙΟ I

### ΑΝΑΛΥΤΙΚΕΣ ΠΡΟΔΙΑΓΡΑΦΕΣ ΤΟΥ ΚΟΙΝΟΥ ΣΧΕΔΙΟΤΥΠΟΥ ΓΙΑ ΤΟΝ «ΚΑΤΑΛΟΓΟ ΕΜΠΙΣΤΕΥΣΗΣ ΕΠΙΟΠΤΕΥΟΜΕΝΩΝ/ΔΙΑΠΙΣΤΕΥΜΕΝΩΝ ΠΑΡΟΧΩΝ ΥΠΗΡΕΣΙΩΝ ΠΙΣΤΟΠΟΙΗΣΗΣ»

Οι παρούσες προδιαγραφές βασίζονται στις προδιαγραφές και τις απαιτήσεις που παρατίθενται στο ETSI TS 119 612 v1.1.1 (στο εξής θα αναφέρεται ως ETSI TS 119 612).

Όταν δεν αναφέρεται συγκεκριμένη απαίτηση στις παρούσες προδιαγραφές, ΘΑ ΠΡΕΠΕΙ ΝΑ ισχύουν εξ ολοκλήρου οι προδιαγραφές του ETSI TS 119 612 διατάξεις 5 και 6. Όταν αναφέρονται συγκεκριμένες απαιτήσεις στις παρούσες προδιαγραφές, ΘΑ ΠΡΕΠΕΙ ΝΑ υπερισχύουν των αντίστοιχων απαιτήσεων του ETSI TS 119 612. Σε περίπτωση αποκλίσεων μεταξύ των παρούσων προδιαγραφών και αυτών του ETSI TS 119 612, κανονιστική ισχύ ΘΑ ΠΡΕΠΕΙ ΝΑ έχουν οι παρούσες προδιαγραφές.

#### **Scheme operator name** (διάταξη 5.3.4)

Το πεδίο αυτό ΘΑ ΠΡΕΠΕΙ ΝΑ υπάρχει και ΘΑ ΠΡΕΠΕΙ ΝΑ συμμορφώνεται με τις προδιαγραφές του TS 119 612 διάταξη 5.3.4.

(<sup>1</sup>) IETF RFC 2119: «Λέξεις-κλειδιά για χρήση στην αίτηση για σχολιασμό προκειμένου να δηλωθούν τα επίπεδα συμμόρφωσης».

Μια χώρα ΔΥΝΑΤΑΙ ΝΑ διαθέτει χωριστούς φορείς εποπτείας και διαπίστευσης και ακόμη και συμπληρωματικούς φορείς για τυχόν σχετικές επιχειρησιακές δραστηριότητες. Εναπόκειται στο κάθε κράτος μέλος να ορίσει τον υπεύθυνο σχήματος του καταλόγου εμπιστευσης του. Αναμένεται ότι ο φορέας εποπτείας, ο φορέας διαπίστευσης και ο υπεύθυνος σχήματος (όταν εμφανίζονται ως χωριστοί φορείς) θα αναλαμβάνουν 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 καταλόγου εμπιστευσης, συμπεριλαμβανομένων των πληροφοριών που αφορούν ειδικά το σχήμα, οι οποίες ορίζονται στο πεδίο «Scheme information URI» (URI πληροφοριών σχήματος) (διάταξη 5.3.7).

#### **Scheme name** (διάταξη 5.3.6)

Το πεδίο αυτό ΘΑ ΠΡΕΠΕΙ ΝΑ υπάρχει και ΘΑ ΠΡΕΠΕΙ ΝΑ συμμορφώνεται με τις προδιαγραφές του TS 119 612 διάταξη 5.3.6 όπου ΘΑ ΠΡΕΠΕΙ ΝΑ χρησιμοποιείται η ακόλουθη επωνυμία για το σχήμα:

«EN\_name\_value» = «Κατάλογος κατάστασης εποπτείας/διαπίστευσης των υπηρεσιών πιστοποίησης από παρόχους υπηρεσιών πιστοποίησης οι οποίοι εποπτεύονται/διαπιστεύονται από τον υπεύθυνο σχήματος του εκάστοτε κράτος μέλος ως προς τη συμμόρφωση με τις σχετικές διατάξεις της οδηγίας 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές».

#### **Scheme information URI** (διάταξη 5.3.7)

Το πεδίο αυτό ΘΑ ΠΡΕΠΕΙ ΝΑ υπάρχει και ΘΑ ΠΡΕΠΕΙ ΝΑ συμμορφώνεται με τις προδιαγραφές του TS 119 612 διάταξη 5.3.7, όπου οι «κατάλληλες πληροφορίες για το σχήμα» ΘΑ ΠΡΕΠΕΙ ΝΑ συμπεριλαμβάνουν τουλάχιστον:

- Εισαγωγικές πληροφορίες που είναι κοινές σε όλα τα κράτη μέλη όσον αφορά το πεδίο εφαρμογής και το πλαίσιο του καταλόγου εμπιστευσης και το υπάρχον σχήμα/τα υπάρχοντα σχήματα εποπτείας/διαπίστευσης. Το κοινό κείμενο που πρέπει να χρησιμοποιείται παρατίθεται παρακάτω, όπου η στοιχειοσειρά «[ονομασία του οικείου κράτους μέλους]» ΘΑ ΠΡΕΠΕΙ ΝΑ αντικαθίσταται από την ονομασία του οικείου κράτους μέλους:

«Ο παρών κατάλογος είναι ο "Κατάλογος εμπιστευσης εποπτευόμενων/διαπιστευμένων παρόχων υπηρεσιών πιστοποίησης" που παρέχει πληροφορίες σχετικά με την κατάσταση εποπτείας/διαπίστευσης των υπηρεσιών πιστοποίησης από τους παρόχους υπηρεσιών πιστοποίησης (CSP) οι οποίοι εποπτεύονται/διαπιστεύονται από την/το [ονομασία του οικείου κράτους μέλους] ως προς τη συμμόρφωση με τις σχετικές διατάξεις της οδηγίας 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.

Ο κατάλογος εμπιστευσης αποσκοπεί στα εξής:

- στην καταγραφή και την παροχή αξιόπιστων πληροφοριών σχετικά με την κατάσταση εποπτείας/διαπίστευσης των υπηρεσιών πιστοποίησης από παρόχους υπηρεσιών πιστοποίησης οι οποίοι εποπτεύονται/είναι διαπιστευμένοι από τη/το [ονομασία του οικείου κράτους μέλους] ως προς τη συμμόρφωση με τις σχετικές διατάξεις της οδηγίας 1999/93/ΕΚ.
- στην παροχή της δυνατότητας για επικύρωση εμπιστευσης των ηλεκτρονικών υπογραφών που υποστηρίζονται από τις εποπτευόμενες/διαπιστούμενες υπηρεσίες πιστοποίησης που εγγράφονται στον κατάλογο από τους καταγεγραμμένους CSP.

Ο κατάλογος εμπιστευσης ενός κράτους μέλους παρέχει, ως ελάχιστη προϋπόθεση, πληροφορίες για τους εποπτευόμενους/διαπιστευμένους CSP που εκδίδουν αναγνωρισμένα πιστοποιητικά σύμφωνα με τις διατάξεις που ορίζονται στην οδηγία 1999/93/ΕΚ [άρθρο 3 παράγραφος 2 και 3 και άρθρο 7 παράγραφος 1 στοιχείο α)], συμπεριλαμβανομένων, όταν δεν αποτελούν μέρος των QC, πληροφοριών σχετικά με τα QC που υποστηρίζουν την ηλεκτρονική υπογραφή και σχετικά με το αν η υπογραφή δημιουργείται μέσω ασφαλούς διάταξης δημιουργίας υπογραφών.

Οι CSP οι οποίοι εκδίδουν αναγνωρισμένα πιστοποιητικά (Qualified Certificates -QC) που παρατίθενται εδώ εποπτεύονται από την/το [ονομασία του οικείου κράτους μέλους] και μπορούν επίσης να διαπιστευθούν ως προς τη συμμόρφωση με τις διατάξεις που ορίζονται στην οδηγία 1999/93/ΕΚ, συμπεριλαμβανομένης της συμμόρφωσης με τις απαιτήσεις του παραρτήματος I (απαιτήσεις για τα QC) και τις απαιτήσεις του παραρτήματος II (απαιτήσεις για τους CSP που εκδίδουν QC). Το ισχύον σύστημα "εποπτείας" (αντίστοιχα, σύστημα "εθελοντικής διαπίστευσης") ορίζεται και πρέπει να πληροί τις σχετικές απαιτήσεις της οδηγίας 1999/93/ΕΚ, ιδίως εκείνες που ορίζονται στο άρθρο 3 παράγραφος 3, το άρθρο 8 παράγραφος 1, το άρθρο 11 [αντίστοιχα, στο άρθρο 2 παράγραφος 13, το άρθρο 3 παράγραφος 2, το άρθρο 7 παράγραφος 1 στοιχείο α), το άρθρο 8 παράγραφος 1, το άρθρο 11].

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

— Συγκεκριμένες πληροφορίες σχετικά με το υπάρχον σχήμα/τα υπάρχοντα σχήματα εποπτείας/διαπίστευσης, και συγκεκριμένα (!):

- πληροφορίες σχετικά με το σχήμα εποπτείας που ισχύει για κάθε CSP<sub>QC</sub>.
- πληροφορίες, όταν υπάρχουν, για το εθνικό σχήμα εθελοντικής διαπίστευσης που ισχύει για κάθε CSP<sub>QC</sub>.
- 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 προαναφερθέν σχήμα:

- 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 τεθούν υπό εποπτεία/να διαπιστευθούν·
  - πληροφορίες σχετικά με τα κριτήρια βάσει των οποίων εποπτεύονται/διαπιστεύονται οι CSP.
- Συγκεκριμένες πληροφορίες, όταν υπάρχουν, για τους ειδικούς «προσδιορισμούς» που μπορεί να δικαιούνται να λάβουν ορισμένα φυσικά ή ψηφιακά (λογικά) αντικείμενα που δημιουργούνται ή εκδίδονται ως αποτέλεσμα της παροχής μιας υπηρεσίας πιστοποίησης, βάσει της συμμόρφωσής τους με τις διατάξεις και τις απαιτήσεις που ορίζονται σε εθνικό επίπεδο, συμπεριλαμβανομένων της έννοιας ενός τέτοιου «προσδιορισμού» και των σχετικών εθνικών διατάξεων και απαιτήσεων.

Επιπλέον ειδικές πληροφορίες ανά κράτος μέλος για το σχήμα ΔΥΝΑΤΑΙ ΝΑ παρέχονται εθελοντικά, όπως:

- πληροφορίες σχετικά με τα κριτήρια και τους κανόνες που χρησιμοποιούνται για την επιλογή υπεύθυνων για την εποπτεία/τη διαπίστευση και ορίζουν πώς οι υπεύθυνοι αυτοί εποπτεύουν (ελέγχουν)/διαπιστεύουν (διερευνούν) τους CSP·
- λοιπά στοιχεία επικοινωνίας και γενικές πληροφορίες που ισχύουν για τη λειτουργία του σχήματος.

#### **Scheme type/community/rules** (διάταξη 5.3.9)

Το πεδίο αυτό ΘΑ ΠΡΕΠΕΙ ΝΑ υπάρχει, ΘΑ ΠΡΕΠΕΙ ΝΑ συμμορφώνεται με τις προδιαγραφές του TS 119 612 ρήτρα 5.3.9 και ΘΑ ΠΡΕΠΕΙ ΝΑ συμπεριλαμβάνει τουλάχιστον δύο URI:

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

URI: <http://uri.etsi.org/TrstSvc/TrustedList/schemerules/EUcommon>

Περιγραφικό κείμενο:

#### *«Συμμετοχή σε ένα σχήμα*

Κάθε κράτος μέλος πρέπει να δημιουργήσει έναν "Κατάλογο εμπιστευσης εποπτευόμενων/διαπιστευμένων παρόχων υπηρεσιών πιστοποίησης" που παρέχει πληροφορίες σχετικά με την κατάσταση εποπτείας/διαπίστευσης των υπηρεσιών πιστοποίησης από τους παρόχους υπηρεσιών πιστοποίησης (CSP) οι οποίοι εποπτεύονται/διαπιστεύονται από το οικείο κράτος μέλος ως προς τη συμμόρφωση με τις σχετικές διατάξεις της οδηγίας 1999/93/ΕΚ του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου, της 13ης Δεκεμβρίου 1999, σχετικά με το κοινοτικό πλαίσιο για ηλεκτρονικές υπογραφές.

Η παρούσα εφαρμογή των εν λόγω καταλόγων εμπιστευσης πρέπει επίσης να αναφέρεται στον κατάλογο συνδέσμων (δεικτών) προς τον κατάλογο εμπιστευσης κάθε κράτους μέλους, ο οποίος καταρτίζεται από την Ευρωπαϊκή Επιτροπή.

#### *Πολιτική/κανόνες για την αξιολόγηση των καταγεγραμμένων υπηρεσιών*

Ο κατάλογος εμπιστευσης ενός κράτους μέλους πρέπει να παρέχει, ως ελάχιστη προϋπόθεση, πληροφορίες για τους εποπτευόμενους/διαπιστευμένους CSP που εκδίδουν αναγνωρισμένα πιστοποιητικά σύμφωνα με τις διατάξεις που ορίζονται στην οδηγία 1999/93/ΕΚ [άρθρο 3 παράγραφος 2 και 3 και άρθρο 7 παράγραφος 1 στοιχείο α)], συμπεριλαμβανομένων πληροφοριών σχετικά με τα αναγνωρισμένα πιστοποιητικά (QC) που υποστηρίζουν την ηλεκτρονική υπογραφή και σχετικά με το αν η υπογραφή δημιουργείται μέσω μιας ασφαλούς διάταξης δημιουργίας υπογραφών.

(<sup>1</sup>) Τα δυο τελευταία σύνολα πληροφοριών είναι καίριας 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 για τους CSP που δεν εκδίδουν QC. Τα εν λόγω σύνολα πληροφοριών θα πρέπει να παρέχονται σε επίπεδο καταλόγου εμπιστευσης 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), και 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 εθνικά συστήματα εποπτείας/διαπίστευσης για τους CSP που δεν εκδίδουν QC μπορούν να παρέχονται σε επίπεδο υπηρεσίας, όταν υπάρχουν και όταν είναι απαραίτητες (π.χ. για να γίνεται διάκριση μεταξύ πολλών επιπέδων ποιότητας/ασφάλειας) μέσω της χρήσης του «URI καθορισμού υπηρεσίας σχήματος» (διάταξη 5.5.6).

Οι CSP που εκδίδουν αναγνωρισμένα πιστοποιητικά (QC) πρέπει να εποπτεύονται από το κράτος μέλος όπου είναι εγκατεστημένοι (αν είναι εγκατεστημένοι σε κράτος μέλος) και δύνανται επίσης να είναι διαπιστευμένοι ως προς τη συμμόρφωση με τις διατάξεις της οδηγίας 1999/93/EK, συμπεριλαμβανομένης της συμμόρφωσης με τις απαιτήσεις του παραρτήματος I (απαιτήσεις για τα QC), και με τις απαιτήσεις 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/EK, ιδίως εκείνες που ορίζονται στο άρθρο 3 παράγραφος 3, το άρθρο 8 παράγραφος 1, το άρθρο 11 [αντίστοιχα, στο άρθρο 2 παράγραφος 13, το άρθρο 3 παράγραφος 2, το άρθρο 7 παράγραφος 1 στοιχείο α), το άρθρο 8 παράγραφος 1, το άρθρο 11].

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

Οι CSP που δεν εκδίδουν QC, αλλά παρέχουν βοηθητικές υπηρεσίες, μπορούν να εμπίπτουν σε ένα σύστημα "εθελοντικής διαπίστευσης" (όπως ορίζεται στην οδηγία 1999/93/EK και σε συμμόρφωση με αυτήν) και/ή στο πλαίσιο ενός εθνικά καθορισμένου "αναγνωρισμένου σχήματος έγκρισης", που εφαρμόζεται σε εθνική βάση για την εποπτεία της συμμόρφωσης με τις διατάξεις που ορίζονται στην οδηγία 1999/93/EK και ενδεχομένως με τις εθνικές διατάξεις όσον αφορά την παροχή υπηρεσιών πιστοποίησης (κατά την έννοια του άρθρου 2 παράγραφος 11 της οδηγίας 1999/93/EK). Ορισμένα από τα φυσικά ή ψηφιακά (λογικά) αντικείμενα που δημιουργούνται ή εκδίδονται ως αποτέλεσμα της παροχής μιας υπηρεσίας πιστοποίησης μπορεί να δικαιούνται ειδική "αναγνώριση" βάσει της συμμόρφωσής τους με τις διατάξεις και τις απαιτήσεις που ορίζονται σε εθνικό επίπεδο, αλλά η έννοια αυτής της "αναγνώρισης" ενδέχεται να περιορίζεται αποκλειστικά στο εθνικό επίπεδο.

#### Ερμηνεία του καταλόγου εμπιστευσης

Οι **γενικές κατευθυντήριες γραμμές χρήσης** για τις εφαρμογές, τις υπηρεσίες ή τα προϊόντα που αφορούν ηλεκτρονικές υπογραφές και βασίζονται σε έναν κατάλογο εμπιστευσης, σύμφωνα με το παράρτημα της απόφασης της Επιτροπής [παραπομπή στην παρούσα απόφαση] είναι οι εξής:

Μια καταχώριση "CA/QC" "Αναγνωριστικό τύπου υπηρεσίας" ("Sti") (παρομοίως μια καταχώριση CA/QC που αναγνωρίζεται περαιτέρω ότι αποτελεί "RootCA/QC" μέσω της χρήσης της επέκτασης "Επέκταση πληροφοριών υπηρεσίας" "Sie" additionalServiceInformation)

- δηλώνει ότι από την CA με αναγνωριστικό "Ψηφιακό αναγνωριστικό υπηρεσίας" ("Sdi") (παρομοίως με ιεραρχία CA η οποία ξεκινά από την CA βάσης με αναγνωριστικό "Sdi") από τον αντίστοιχο CSP (βλέπε συσχετιζόμενα πεδία πληροφοριών TSP) όλα τα εκδιδόμενα πιστοποιητικά για οντότητα-τελικό αποδέκτη είναι αναγνωρισμένα πιστοποιητικά (QC) **εφόσον** υποστηρίζεται ότι είναι τέτοια στο πιστοποιητικό μέσω της χρήσης κατάλληλων δηλώσεων QcStatements που ορίζονται μέσω του EN 319 412-5 (δηλαδή, QcCompliance, QcSSCD κ.λπ.) και/ή των αναγνωριστικών QCP(+) OID που ορίζονται στο EN 319 411-2 (και αυτό διασφαλίζεται από τον εκδίδοντα CSP και διασφαλίζεται από τον φορέα εποπτείας/διαπίστευσης του κράτους μέλους).

*Σημείωση:* Σε περίπτωση που δεν υπάρχουν πληροφορίες "Sie" "Επέκταση προσδιορισμών" ή σε περίπτωση που ένα πιστοποιητικό για οντότητες-τελικούς αποδέκτες το οποίο υποστηρίζεται ότι είναι QC δεν αναγνωρίζεται πλέον μέσω σχετικών πληροφοριών "Sie" "Επέκταση προσδιορισμών", τότε οι μηχανικά επεξεργασίμες πληροφορίες που βρίσκονται στο QC θεωρούνται, βάσει εποπτείας/διαπίστευσης, ακριβείς. Αυτό σημαίνει ότι η χρήση (ή η μη χρήση) των κατάλληλων δηλώσεων QcStatements που καθορίζονται βάσει του ETSI (δηλαδή, QcCompliance, QcSSCD κ.λπ.) και/ή των αναγνωριστικών QCP(+) OID που καθορίζονται βάσει του ETSI διασφαλίζεται ότι συμφωνεί με αυτό που υποστηρίζει ο CSP που εκδίδει QC.

- **και αν** υπάρχουν πληροφορίες "Sie" "Επέκταση προσδιορισμών", τότε εκτός από τον παραπάνω εξ ορισμού κανόνα ερμηνείας χρήσης, τα πιστοποιητικά που ορίζονται μέσω της χρήσης των εν λόγω πληροφοριών "Sie" "Επέκταση προσδιορισμών", η οποία βασίζεται στην αρχή μιας αλληλουχίας "φίλτρων" που προσδιορίζουν περαιτέρω ένα σύνολο πιστοποιητικών, πρέπει να εξετάζονται σύμφωνα με τους συσχετιζόμενους προσδιοριστές παρέχοντας ορισμένες επιπλέον πληροφορίες όσον αφορά την κατάσταση αναγνώρισης, την "υποστήριξη από SS CD" και/ή το "νομικό πρόσωπο ως υποκείμενο" (π.χ. τα πιστοποιητικά που περιέχουν συγκεκριμένο αναγνωριστικό αντικείμενο στην επέκταση της πολιτικής πιστοποιητικού και/ή έχουν συγκεκριμένη σχηματομορφή "Χρήσης κλειδιού" και/ή φιλτράρονται μέσω της χρήσης συγκεκριμένης τιμής η οποία εμφανίζεται σε ένα συγκεκριμένο πεδίο ή επέκταση του πιστοποιητικού κ.λπ.). Οι προσδιοριστές αυτοί αποτελούν μέρος του παρακάτω συνόλου "προσδιοριστών", οι οποίοι χρησιμοποιούνται για να επανορθώσουν την έλλειψη πληροφοριών στο αντίστοιχο περιεχόμενο του QC και οι οποίοι χρησιμοποιούνται αντίστοιχα:

- ο για να δηλώσουν την κατάσταση αναγνώρισης: "QCStatement", η οποία σημαίνει ότι το/τα προσδιοριζόμενο/-α πιστοποιητικό/-ά είναι αναγνωρισμένα:



- για να δηλώσουν τη φύση της υποστήριξης από SSCD:
  - τιμή προσδιοριστή "QCWithSSCD", η οποία σημαίνει ότι το "QC υποστηρίζεται από SSCD", ή
  - τιμή προσδιοριστή "QCNoSSCD", η οποία σημαίνει ότι 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.

#### ΚΑΙ/Η

- για να δηλώσουν έκδοση υπέρ νομικού προσώπου:
  - τιμή προσδιοριστή "QCForLegalPerson", η οποία σημαίνει ότι "το πιστοποιητικό εκδόθηκε υπέρ νομικού προσώπου".

Ο γενικός κανόνας ερμηνείας για οποιαδήποτε άλλη καταχώριση τύπου "Sti" είναι ότι η καταγεγραμμένη υπηρεσία που ονομάζεται βάσει της τιμής πεδίου "Sn" και αναγνωρίζεται κατά μονοσήμαντο τρόπο βάσει της τιμής πεδίου "Sdi" έχει τρέχουσα κατάσταση εποπτείας/διαπίστευσης σύμφωνα με την τιμή πεδίου "Scs" από την ημερομηνία που υποδεικνύεται στο "Current status starting date and time" (Ημερομηνία και ώρα έναρξης της τρέχουσας κατάστασης). Ενδέχεται να εντοπιστούν ειδικοί κανόνες ερμηνείας για οποιοδήποτε επιπλέον πληροφορίες όσον αφορά μια καταγεγραμμένη υπηρεσία (π.χ. πεδίο "Service Information Extensions" (Επεκτάσεις πληροφοριών υπηρεσίας), όταν ισχύει, στο ειδικό URI ανά κράτος μέλος, ως μέρος του υπάρχοντος πεδίου "Scheme type/community/rules" (Τύπος σχήματος/κοινότητες/κανόνες).

Ανατρέξτε στις τεχνικές προδιαγραφές για ένα κοινό σχεδιάγραμμα για τον "Κατάλογο εμπιστευσης εποπτευόμενων/διαπιστευμένων παρόχων υπηρεσιών πιστοποίησης" στο παράρτημα της απόφασης 2009/767/EK της Επιτροπής για περαιτέρω λεπτομέρειες σχετικά με τα πεδία, την περιγραφή και την έννοια των καταλόγων εμπιστευσης των κρατών μελών.».

- Ένα URI ειδικά για τον κατάλογο εμπιστευσης κάθε 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/TrustedList/schemerules/CC> όπου CC = ο κωδικός χώρας ISO 3166-1 <sup>(1)</sup> 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 αξιολογούνται 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 του καταλόγου εμπιστευσης όσον αφορά τις υπηρεσίες πιστοποίησης που δεν σχετίζονται με την έκδοση QC. Αυτό μπορεί να χρησιμοποιηθεί για να δηλώσει πιθανή λεπτομερή ανάλυση των εθνικών συστημάτων εποπτείας/διαπίστευσης που σχετίζονται με τους CSP που δεν εκδίδουν QC και το πώς χρησιμοποιούνται για τον σκοπό αυτόν τα πεδία «Scheme service definition URI» (URI καθορισμού υπηρεσίας σχήματος) (διάταξη 5.5.6) και «Service information extension» (επέκταση πληροφοριών υπηρεσίας) (διάταξη 5.5.9).

Τα κράτη μέλη ΔΥΝΑΝΤΑΙ ΝΑ ορίσουν και να χρησιμοποιούν πρόσθετα URI από το παραπάνω αποκλειστικό ανά κράτος μέλος URI (δηλαδή, URI τα οποία καθορίζονται από αυτό το ιεραρχικά αποκλειστικό URI).

#### TSL policy/legal notice (διάταξη 5.3.11)

Το πεδίο αυτό ΘΑ ΠΡΕΠΕΙ ΝΑ υπάρχει και ΘΑ ΠΡΕΠΕΙ ΝΑ συμμορφώνεται με τις προδιαγραφές του TS 119 612 ρήτρα 5.3.11, όπου η πολιτική/νομική σημείωση σχετικά με το νομικό καθεστώς του σχήματος ή τις νομικές απαιτήσεις που πληροί το σχήμα υπό τη δικαιοδοσία στην οποία είναι εγκατεστημένο το σχήμα και/ή τυχόν περιορισμούς και όρους βάσει των οποίων ο κατάλογος εμπιστευσης τηρείται και δημοσιεύονται ΘΑ ΠΡΕΠΕΙ ΝΑ είναι μια πολύγλωσση στοιχειοσειρά (απλό κείμενο), αποτελούμενη από δύο μέρη:

1. Ένα πρώτο υποχρεωτικό μέρος, κοινό για τους καταλόγους εμπιστευσης όλων των κρατών μελών (με υποχρεωτική γλώσσα τα αγγλικά του Ηνωμένου Βασιλείου και ενδεχομένως μία ή περισσότερες εθνικές γλώσσες), το οποίο δηλώνει ότι το ισχύον νομικό πλαίσιο είναι η οδηγία 1999/93/EK και η αντίστοιχη εφαρμογή της στους νόμους του κράτους μέλους που δηλώνεται 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 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.

<sup>(1)</sup> ISO 3166-1:2006: «Κωδικοί αναπαράστασης των ονομασιών των χωρών και των υποδιαίρεσών τους — Μέρος 1: Κωδικοί χωρών».

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

Το ισχύον νομικό πλαίσιο για την παρούσα εφαρμογή TSL του καταλόγου εμπιστευσης 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].

2. Ένα δεύτερο προαιρετικό μέρος, ειδικό για κάθε κατάλογο εμπιστευσης (με υποχρεωτική γλώσσα τα αγγλικά του Ηνωμένου Βασιλείου και ενδεχομένως μία ή περισσότερες εθνικές γλώσσες), το οποίο περιέχει παραπομπές σε συγκεκριμένα ισχύοντα εθνικά νομικά πλαίσια (π.χ. συγκεκριμένα όσον αφορά εθνικά σχήματα εποπτείας/διαπίστευσης για CSP που δεν εκδίδουν QC).

## ΚΕΦΑΛΑΙΟ II

### ΣΥΝΕΧΕΙΑ ΤΩΝ ΚΑΤΑΛΟΓΩΝ ΕΜΠΙΣΤΕΥΣΗΣ

Τα πιστοποιητικά που πρόκειται να κοινοποιηθούν στην Επιτροπή δυνάμει του άρθρου 3 στοιχείο γ) της παρούσας απόφασης ΘΑ ΠΡΕΠΕΙ ΝΑ εκδίδονται κατά τέτοιο τρόπο ώστε:

- να μεσολαβεί διάστημα τουλάχιστον τριών μηνών μεταξύ των ημερομηνιών ισχύος τους,
- να δημιουργούνται σε νέα ζεύγη κλειδιών καθώς δεν επιτρέπεται η εκ νέου πιστοποίηση χρησιμοποιημένου ζεύγους κλειδιών.

Σε περίπτωση αποκάλυψης ή κατάργησης ΕΝΟΣ από τα ιδιωτικά κλειδιά που αντιστοιχούν στο δημόσιο κλειδί που θα μπορούσε να χρησιμοποιηθεί για την επικύρωση της υπογραφής του καταλόγου εμπιστευσης και έχει κοινοποιηθεί στην Επιτροπή και δημοσιευτεί στους κεντρικούς καταλόγους δεικτών της Επιτροπής, τα κράτη μέλη ΘΑ ΠΡΕΠΕΙ ΝΑ:

- επανεκδίδουν, χωρίς καθυστέρηση, νέο κατάλογο εμπιστευσης με το μη παραβιασμένο ιδιωτικό κλειδί σε περίπτωση που ο δημοσιευμένος κατάλογος εμπιστευσης υπογράφηκε με παραβιασμένο ή καταργημένο ιδιωτικό κλειδί·
- γνωστοποιούν άμεσα στην Επιτροπή τον νέο κατάλογο πιστοποιητικών δημόσιων κλειδιών που αντιστοιχούν στα ιδιωτικά κλειδιά που θα μπορούσαν να χρησιμοποιηθούν για την υπογραφή του καταλόγου εμπιστευσης.

Σε περίπτωση αποκάλυψης ή κατάργησης ΟΛΩΝ των ιδιωτικών κλειδιών που αντιστοιχούν στα δημόσια κλειδιά που θα μπορούσαν να χρησιμοποιηθούν για την επικύρωση της υπογραφής του καταλόγου εμπιστευσης και έχουν κοινοποιηθεί στην Επιτροπή και δημοσιευτεί στους κεντρικούς καταλόγους δεικτών της Επιτροπής, τα κράτη μέλη ΘΑ ΠΡΕΠΕΙ ΝΑ:

- δημιουργήσουν νέα ζεύγη κλειδιών που θα μπορούσαν να χρησιμοποιηθούν για την υπογραφή του καταλόγου εμπιστευσης και των αντίστοιχων πιστοποιητικών δημόσιου κλειδιού·
- επανεκδώσουν, χωρίς καθυστέρηση, νέο κατάλογο εμπιστευσης υπογεγραμμένο με ένα από αυτά τα νέα ιδιωτικά κλειδιά, του οποίου το αντίστοιχο πιστοποιητικό δημόσιου κλειδιού πρόκειται να κοινοποιηθεί·
- να ενημερώσουν άμεσα την Επιτροπή για τον νέο κατάλογο πιστοποιητικών δημόσιων κλειδιών που αντιστοιχούν στα ιδιωτικά κλειδιά που θα μπορούσαν να χρησιμοποιηθούν για την υπογραφή του καταλόγου εμπιστευσης.

## ΚΕΦΑΛΑΙΟ III

### ΠΡΟΔΙΑΓΡΑΦΕΣ ΓΙΑ ΤΗΝ ΑΝΑΓΝΩΣΙΜΗ ΑΠΟ ΑΝΘΡΩΠΟ ΜΟΡΦΗ ΤΟΥ ΚΑΤΑΛΟΓΟΥ ΕΜΠΙΣΤΕΥΣΗΣ

Μια αναγνώσιμη από άνθρωπο μορφή του καταλόγου εμπιστευσης που δημιουργείται και δημοσιεύεται ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ παρέχεται με τη μορφή εγγράφου Portable Document Format (PDF) σύμφωνα με το ISO 32000<sup>(1)</sup>, το οποίο ΠΡΕΠΕΙ να φέρει μορφοποίηση, σύμφωνα με το προφίλ PDF/A [ISO 19005<sup>(2)</sup>].

Το περιεχόμενο μιας αναγνώσιμης από άνθρωπο μορφής βάσει PDF/A του καταλόγου εμπιστευσης ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ συμμορφώνεται με τις παρακάτω απαιτήσεις:

- Η δομή της μορφής HR ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ αντιστοιχεί στο λογικό μοντέλο που περιγράφεται στο TS 119 612.
- 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 (π.χ. «Μια αρχή πιστοποίησης που εκδίδει πιστοποιητικά δημοσίου κλειδιού»·
  - πολλαπλές εκδόσεις σε διάφορες εθνικές γλώσσες, όπως προβλέπεται στον κατάλογο εμπιστευσης, όταν ισχύουν.

<sup>(1)</sup> ISO 32000-1:2008: Διαχείριση εγγράφων — Μορφή φορητού εγγράφου — Μέρος 1: PDF 1.7.

<sup>(2)</sup> ISO 19005-2:2011: Διαχείριση εγγράφων — Ηλεκτρονική μορφή αρχείου του εγγράφου για μακροχρόνια διατήρηση — Μέρος 2: Χρήση του ISO 32000-1 (PDF/A-2).

- Τα παρακάτω πεδία και οι αντίστοιχες τιμές των ψηφιακών πιστοποιητικών που υπάρχουν στο πεδίο «Ψηφιακή ταυτότητα υπηρεσίας» ΠΡΟΤΕΙΝΕΤΑΙ ΝΑ εμφανίζονται τουλάχιστον στη μορφή HR:
- έκδοση
  - αύξων αριθμός
  - αλγόριθμος υπογραφής
  - εκδότης
  - ισχύει από
  - ισχύει μέχρι
  - αντικείμενο
  - 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 ΠΡΕΠΕΙ ΝΑ υπογράφεται από τον υπεύθυνο σχήματος, σύμφωνα με το βασικό προφίλ υπογραφών PAdES <sup>(1)</sup>.
- 

<sup>(1)</sup> ETSI TS 103 172 (Μάρτιος 2012) — Ηλεκτρονικές υπογραφές και υποδομές (ES)· βασικό προφίλ PAdES.