



Βρυξέλλες, 5 Νοεμβρίου 2018
(OR. en)

Διοργανικός φάκελος:
2018/0339(NLE)

13711/18
ADD 1

TRANS 488

ΣΗΜΕΙΩΜΑ

Αποστολέας: Γενική Γραμματεία του Συμβουλίου

Αποδέκτης: Αντιπροσωπίες

αριθ. προηγ. εγγρ.: ST 13711/18 TRANS 448

Αριθ. εγγρ. Επιτρ.: ST 12727/18 TRANS 426 + ADD 1

Θέμα: Απόφαση του Συμβουλίου σχετικά με τη θέση που πρέπει να ληφθεί, εξ ονόματος της Ευρωπαϊκής Ένωσης, στην ομάδα εμπειρογνομόνων της Οικονομικής Επιτροπής των Ηνωμένων Εθνών για την Ευρώπη για την ευρωπαϊκή συμφωνία περί της εργασίας των πληρωμάτων οχημάτων που εκτελούν διεθνείς οδικές μεταφορές

Προσάρτημα της προαναφερόμενης απόφασης του Συμβουλίου.

Νέο προσάρτημα της AETR

Προσάρτημα 4

Προδιαγραφές του TACHOnet

1. Πεδίο εφαρμογής και σκοπός
 - 1.1. Στο παρόν προσάρτημα καθορίζονται οι όροι και οι προϋποθέσεις σύνδεσης των συμβαλλομένων μερών της AETR με το TACHOnet μέσω του eDelivery.
 - 1.2. Τα συμβαλλόμενα μέρη που συνδέονται με το TACHOnet μέσω του eDelivery συμμορφώνονται με τις διατάξεις του παρόντος προσαρτήματος.
2. Ορισμοί
 - α) «συμβαλλόμενο μέρος» ή «μέρος»: οποιοδήποτε συμβαλλόμενο μέρος της AETR.
 - β) «eDelivery»: η υπηρεσία που έχει αναπτύξει η Ευρωπαϊκή Επιτροπή η οποία καθιστά δυνατή τη μετάδοση δεδομένων μεταξύ τρίτων μερών με ηλεκτρονικά μέσα και παρέχει τεκμήρια σχετικά με τον χειρισμό των μεταδιδόμενων δεδομένων, καθώς και απόδειξη της αποστολής και της παραλαβής των δεδομένων, και προστατεύει τα μεταδιδόμενα δεδομένα από τον κίνδυνο μη εξουσιοδοτημένης μεταβολής τους.
 - γ) «TACHOnet»: το σύστημα ηλεκτρονικής ανταλλαγής πληροφοριών μεταξύ των συμβαλλομένων μερών σχετικών με τις κάρτες οδηγού κατά το άρθρο 31 παράγραφος 2 του κανονισμού (ΕΕ) αριθ. 165/2014.
 - δ) «κεντρικός κόμβος»: το σύστημα πληροφοριών που καθιστά δυνατή την αποστολή μηνυμάτων TACHOnet μεταξύ των αιτούντων συμβαλλομένων μερών και των αποκρινόμενων συμβαλλομένων μερών.
 - ε) «αιτούν συμβαλλόμενο μέρος»: το συμβαλλόμενο μέρος που αποστέλλει αίτηση ή κοινοποίηση στο TACHOnet, η οποία κατόπιν δρομολογείται από τον κεντρικό κόμβο στο ενδεδειγμένο αποκρινόμενο συμβαλλόμενο μέρος.

- στ) «αποκρινόμενο συμβαλλόμενο μέρος»: το συμβαλλόμενο μέρος στο οποίο απευθύνεται αίτηση ή κοινοποίηση με το TACHOnet·
- ζ) «εκδίδουσα αρχή καρτών» ή «CIA»: η οντότητα που έχει εξουσιοδοτηθεί από συμβαλλόμενο μέρος να εκδίδει και να διαχειρίζεται κάρτες ταχογράφου.

3. Γενικές αρμοδιότητες

- 3.1. Κανένα συμβαλλόμενο μέρος δεν δύναται να συνάψει συμφωνίες πρόσβασης στο TACHOnet εξ ονόματος άλλου συμβαλλομένου μέρους ή να εκπροσωπήσει κατά άλλον τρόπο το άλλο συμβαλλόμενο μέρος βάσει του παρόντος προσαρτήματος. Κανένα συμβαλλόμενο μέρος δεν ενεργεί ως υπεργολάβος του άλλου συμβαλλομένου μέρους στις λειτουργίες που αναφέρονται στο παρόν προσάρτημα.
- 3.2. Τα συμβαλλόμενα μέρη παρέχουν πρόσβαση στα εθνικά τους μητρώα καρτών οδηγού μέσω του TACHOnet, με τον τρόπο και στο επίπεδο εξυπηρέτησης που καθορίζονται στο υποπροσάρτημα 4.6.
- 3.3. Εάν τα συμβαλλόμενα μέρη παρατηρήσουν διαταραχές ή σφάλματα εντός του πεδίου αρμοδιότητάς τους που μπορούν να θέσουν σε κίνδυνο την πλήρη και ομαλή λειτουργία του TACHOnet, τις κοινοποιούν αμοιβαία χωρίς καθυστέρηση.
- 3.4. Κάθε συμβαλλόμενο μέρος ορίζει στη Γραμματεία της AETR τα πρόσωπα επικοινωνίας για το TACHOnet. Κάθε αλλαγή των σημείων επαφής επισημαίνεται γραπτώς στη Γραμματεία της AETR.

4. Δοκιμές σύνδεσης με το TACHOnet

- 4.1. Η σύνδεση συμβαλλομένου μέρους με το TACHOnet ολοκληρώνεται μετά την επιτυχή περάτωση των δοκιμών σύνδεσης, ενσωμάτωσης και επιδόσεων σύμφωνα με τις οδηγίες της Ευρωπαϊκής Επιτροπής και υπό την επίβλεψή της.
- 4.2. Σε περίπτωση αποτυχίας των προκαταρκτικών δοκιμών, η Ευρωπαϊκή Επιτροπή μπορεί να αναστείλει το στάδιο δοκιμής. Οι δοκιμές επαναλαμβάνονται όταν το συμβαλλόμενο μέρος κοινοποιήσει στην Ευρωπαϊκή Επιτροπή ότι προέβη στις αναγκαίες τεχνικές βελτιώσεις σε εθνικό επίπεδο που επιτρέπουν την επιτυχή διεξαγωγή των προκαταρκτικών δοκιμών.

- 4.3. Οι προκαταρκτικές δοκιμές είναι μέγιστης διάρκειας έξι μηνών.
5. Αρχιτεκτονική εμπιστευσης
- 5.1. Η εμπιστευτικότητα, η ακεραιότητα και η μη αποκήρυξη των μηνυμάτων του TACHOnet διασφαλίζεται με την αρχιτεκτονική εμπιστευσης του TACHOnet.
- 5.2. Η αρχιτεκτονική εμπιστευσης του TACHOnet βασίζεται σε υπηρεσία υποδομής δημόσιου κλειδιού (PKI) που έχει δημιουργήσει η Ευρωπαϊκή Επιτροπή, της οποίας οι απαιτήσεις καθορίζονται στα υποπροσάρτηματα 4.8 και 4.9.
- 5.3. Στην αρχιτεκτονική εμπιστευσης του TACHOnet παρεμβαίνουν οι ακόλουθες οντότητες:
- α) Η αρχή πιστοποίησης, αρμόδια για την παραγωγή των ψηφιακών πιστοποιητικών τα οποία παραδίδει η αρχή καταχώρισης στις εθνικές αρχές των συμβαλλομένων μερών (μέσω των εμπιστευμένων ταχυδρόμων που έχουν ορίσει), καθώς και για τη δημιουργία της τεχνικής υποδομής για την έκδοση, την ανάκληση και την ανανέωση ψηφιακών πιστοποιητικών.
 - β) Ο κάτοχος τομέα, αρμόδιος για τη λειτουργία του κεντρικού κόμβου που αναφέρεται στο υποπροσάρτημα 4.1 και για την επικύρωση και τον συντονισμό της αρχιτεκτονικής εμπιστευσης του TACHOnet.
 - γ) Η αρχή καταχώρισης, αρμόδια για την καταχώριση και την έγκριση των αιτήσεων έκδοσης, ανάκλησης και ανανέωσης ψηφιακών πιστοποιητικών, και για την εξακρίβωση της ταυτότητας των εμπιστευμένων ταχυδρόμων.
 - δ) Ο εμπιστευμένος ταχυδρόμος είναι το πρόσωπο που έχουν ορίσει οι εθνικές αρχές και είναι αρμόδιο για την παράδοση του δημόσιου κλειδιού στην αρχή καταχώρισης και για την παραλαβή του σχετικού πιστοποιητικού που παράγει η αρχή πιστοποίησης.
 - ε) Η εθνική αρχή συμβαλλομένου μέρους, η οποία:
 - (i) παράγει τα ιδιωτικά κλειδιά και τα αντίστοιχα δημόσια κλειδιά που πρέπει να περιέχουν τα πιστοποιητικά που παράγει η αρχή πιστοποίησης.

(ii) αιτείται τα ψηφιακά πιστοποιητικά από την αρχή πιστοποίησης·

(iii) ορίζει τον εμπιστευμένο ταχυδρόμο.

5.4. Η αρχή πιστοποίησης και η αρχή καταχώρισης ορίζονται από την Ευρωπαϊκή Επιτροπή.

5.5. Κάθε συμβαλλόμενο μέρος που συνδέεται με το TACHOnet οφείλει να αιτηθεί την έκδοση ψηφιακού πιστοποιητικού σύμφωνα με το υποπροσάρτημα 4.9 για να υπογράψει και να κρυπτογραφεί μηνύματα στο TACHOnet.

5.6. Πιστοποιητικό είναι δυνατόν να ανακληθεί σύμφωνα με το υποπροσάρτημα 4.9.

6. Προστασία δεδομένων και εμπιστευτικότητα

6.1. Τα συμβαλλόμενα μέρη, σύμφωνα με το δίκαιο προστασίας δεδομένων σε διεθνές και εθνικό επίπεδο, και ιδίως σύμφωνα με τη σύμβαση για την προστασία του ατόμου από την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα, λαμβάνουν όλα τα αναγκαία τεχνικά και οργανωτικά μέτρα ώστε να εγγυώνται την ασφάλεια των δεδομένων του TACHOnet και να αποτρέπουν την αλλοίωση ή την απώλειά τους, ή τη μη εξουσιοδοτημένη επεξεργασία τους ή τη μη εξουσιοδοτημένη πρόσβαση στα δεδομένα αυτά (ιδίως όσον αφορά τη γνησιότητα, την εμπιστευτικότητα των δεδομένων, την ιχνηλασιμότητα, την ακεραιότητα, τη διαθεσιμότητα και τη μη αποκήρυξη και την ασφάλεια των μηνυμάτων).

6.2. Κάθε συμβαλλόμενο μέρος προστατεύει τα οικεία εθνικά συστήματα από παράνομη χρήση, κακόβουλους κωδικούς, ιούς, επισυνδέσεις υπολογιστή, παραβιάσεις και παράνομες παραποιήσεις δεδομένων και άλλες παρεμφερείς ενέργειες τρίτων. Τα συμβαλλόμενα μέρη συμφωνούν στην καταβολή εμπορικά εύλογων προσπαθειών για να αποφεύγεται η μετάδοση ιών, ωρολογιακών βομβών, σκουληκιών ή παρόμοιων στοιχείων ή κάθε ρουτίνα προγραμματισμού υπολογιστή που ενδέχεται να παρεμβληθεί στα μηχανογραφικά συστήματα άλλου συμβαλλομένου μέρους.

7. Κόστος

7.1. Τα συμβαλλόμενα μέρη αναλαμβάνουν το κόστος ανάπτυξης και λειτουργίας των οικείων συστημάτων δεδομένων και διαδικασιών που απαιτούνται για την εκπλήρωση των υποχρεώσεών τους σύμφωνα με το παρόν προσάρτημα.

- 7.2. Οι υπηρεσίες που προσδιορίζονται στο υποπροσάρτημα 4.1 και παρέχονται από τον κεντρικό κόμβο διατίθενται δωρεάν.
8. Υπεργολαβία
- 8.1. Τα συμβαλλόμενα μέρη μπορούν να αναθέτουν υπεργολαβικά οποιαδήποτε υπηρεσία για την οποία είναι αρμόδια δυνάμει του παρόντος προσαρτήματος.
- 8.2. Η εν λόγω υπεργολαβική ανάθεση δεν απαλλάσσει το συμβαλλόμενο μέρος από την ευθύνη κατά το παρόν προσάρτημα, ούτε από την ευθύνη για το ενδεδειγμένο επίπεδο εξυπηρέτησης σύμφωνα με το υποπροσάρτημα 4.6.

Γενικές πτυχές του TACHOnet

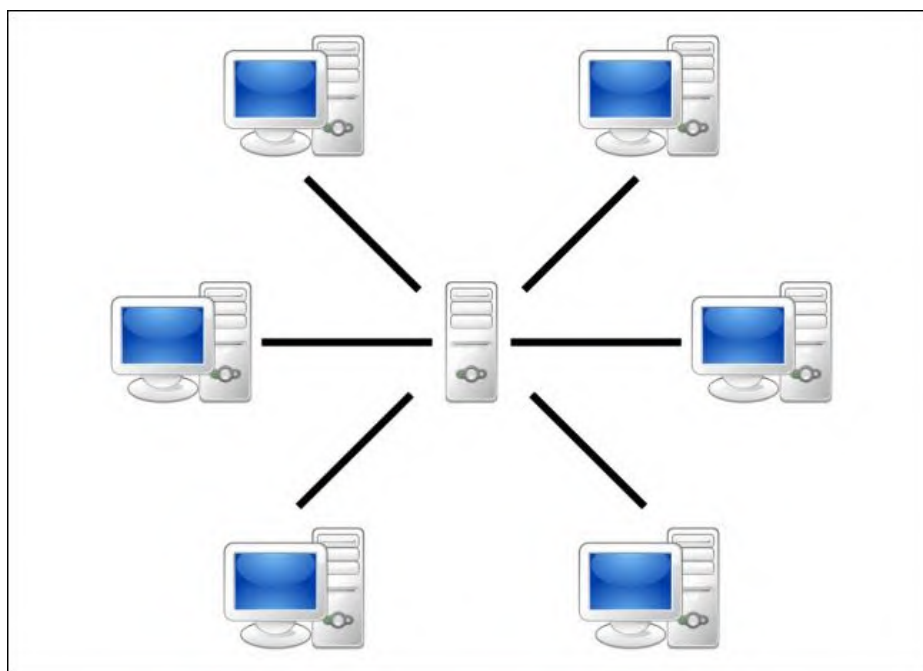
1. Γενική περιγραφή

Το TACHOnet είναι ένα σύστημα ηλεκτρονικής ανταλλαγής πληροφοριών μεταξύ των συμβαλλομένων μερών της AETR σχετικά με τις κάρτες οδηγού. Το TACHOnet δρομολογεί τις αιτήσεις παροχής πληροφοριών των αιτούντων συμβαλλομένων μερών στα αποκρινόμενα συμβαλλόμενα μέρη, καθώς και τις αποκρίσεις αυτών στα αιτούντα συμβαλλόμενα μέρη. Τα συμβαλλόμενα μέρη που συμμετέχουν στο TACHOnet οφείλουν να συνδέουν τα οικεία εθνικά μητρώα καρτών οδηγού με το σύστημα.

2. Αρχιτεκτονική

Το σύστημα ανταλλαγής μηνυμάτων TACHOnet απαρτίζεται από τα ακόλουθα μέρη:

- 2.1. Έναν κεντρικό κόμβο ο οποίος έχει τη δυνατότητα να παραλαμβάνει αίτηση από τον αιτούν συμβαλλόμενο μέρος, να το επικυρώνει και να το επεξεργάζεται διαβιβάζοντάς το στα αποκρινόμενα συμβαλλόμενα μέρη. Ο κεντρικός κόμβος αναμένει απόκριση από κάθε αποκρινόμενο συμβαλλόμενο μέρος, ενοποιεί όλες τις αποκρίσεις και διαβιβάζει την ενοποιημένη απόκριση στο αιτούν συμβαλλόμενο μέρος.
- 2.2. Τα εθνικά συστήματα των συμβαλλομένων μερών, τα οποία διαθέτουν διεπαφή που έχει τη δυνατότητα τόσο να αποστέλλει αιτήσεις στον κεντρικό κόμβο, όσο και να παραλαμβάνει τις σχετικές αποκρίσεις. Τα εθνικά συστήματα δύνανται να χρησιμοποιούν ιδιόκτητο ή εμπορικό λογισμικό για τη μετάδοση και την παραλαβή μηνυμάτων από τον κεντρικό κόμβο.



3. Διαχείριση

- 3.1. Η διαχείριση του κεντρικού κόμβου ασκείται από την Ευρωπαϊκή Επιτροπή, η οποία είναι υπεύθυνη για την τεχνική λειτουργία και τη συντήρηση του κεντρικού κόμβου.
- 3.2. Ο κεντρικός κόμβος δεν αποθηκεύει δεδομένα για περίοδο μεγαλύτερη των έξι μηνών, εξαιρουμένων των δεδομένων καταγραφής και των στατιστικών δεδομένων που αναφέρονται στο υποπροσάρτημα 4.7.
- 3.3. Ο κεντρικός κόμβος παρέχει πρόσβαση σε προσωπικά δεδομένα μόνον σε εξουσιοδοτημένο προσωπικό της Ευρωπαϊκής Επιτροπής, όταν χρειάζεται για την παρακολούθηση, τη συντήρηση και την αποκατάσταση βλαβών.
- 3.4. Κάθε συμβαλλόμενο μέρος είναι υπεύθυνο για:
 - 3.4.1. Τη σύσταση και τη διαχείριση του οικείου εθνικού συστήματος, καθώς και της διεπαφής με τον κεντρικό κόμβο.
 - 3.4.2. Την εγκατάσταση και τη συντήρηση του οικείου εθνικού συστήματος, τόσο του υλισμικού όσο και του λογισμικού, ιδιόκτητου ή εμπορικού.
 - 3.4.3. Την ορθή διαλειτουργικότητα του οικείου εθνικού συστήματος με τον κεντρικό κόμβο, καθώς και τη διαχείριση των μηνυμάτων σφάλματος που παραλαμβάνονται από τον κεντρικό κόμβο.
 - 3.4.4. Τη λήψη όλων των μέτρων για να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η διαθεσιμότητα των πληροφοριών.
 - 3.4.5. Τη λειτουργία του οικείου εθνικού συστήματος σύμφωνα με το επίπεδο εξυπηρέτησης που καθορίζεται στο υποπροσάρτημα 4.6.

Υποπροσάρτημα 4.2.

Λειτουργικότητες του TACHOnet

1. Μέσω του συστήματος ανταλλαγής μηνυμάτων TACHOnet παρέχονται οι ακόλουθες λειτουργικότητες:
 - 1.1. Έλεγχος Εκδοθεισών Καρτών (Check Issued Cards/CIC): επιτρέπει στο αιτούν συμβαλλόμενο μέρος να αποστείλει αίτηση Ελέγχου Εκδοθεισών Καρτών σε ένα ή σε όλα τα αποκρινόμενα συμβαλλόμενα μέρη, ώστε να προσδιορισθεί εάν ο αιτών κάρτα είναι ήδη κάτοχος κάρτας οδηγού εκδοθείσα από τα αποκρινόμενα συμβαλλόμενα μέρη. Τα αποκρινόμενα συμβαλλόμενα μέρη αποκρίνονται στην αίτηση αποστέλλοντας Απόκριση Ελέγχου Εκδοθεισών Καρτών.
 - 1.2. Έλεγχος Καθεστώτος Κάρτας (Check Card Status/CCS): επιτρέπει στο αιτούν συμβαλλόμενο μέρος να ζητήσει από το αποκρινόμενο συμβαλλόμενο μέρος στοιχεία σχετικά με κάρτα που έχει εκδώσει, αποστέλλοντας αίτηση Ελέγχου Καθεστώτος Κάρτας. Το αποκρινόμενο συμβαλλόμενο μέρος αποκρίνεται στην αίτηση αποστέλλοντας Απόκριση Ελέγχου Καθεστώτος Κάρτας.
 - 1.3. Τροποποίηση Καθεστώτος Κάρτας (Modify Card Status/MCS): επιτρέπει στο αιτούν συμβαλλόμενο μέρος να κοινοποιήσει στο αποκρινόμενο συμβαλλόμενο μέρος, με αίτηση τροποποίησης καθεστώτος κάρτας, ότι έχει αλλάξει το καθεστώς κάρτας που έχει εκδώσει το αποκρινόμενο συμβαλλόμενο μέρος. Το αποκρινόμενο συμβαλλόμενο μέρος αποκρίνεται με Βεβαίωση Παραλαβής Τροποποίησης Καθεστώτος Κάρτας.
 - 1.4. Έκδοση Κάρτας Άδειας Οδήγησης (Issued Card Driving License/ICDL): επιτρέπει στο αιτούν συμβαλλόμενο μέρος να κοινοποιήσει στο αποκρινόμενο συμβαλλόμενο μέρος, με Αίτηση Άδειας Εκδοθείσας Κάρτας Οδηγού, ότι το αιτούν συμβαλλόμενο μέρος έχει εκδώσει κάρτα έναντι άδειας οδήγησης που έχει εκδώσει το αποκρινόμενο συμβαλλόμενο μέρος. Το αποκρινόμενο συμβαλλόμενο μέρος αποκρίνεται με Απόκριση Άδειας Εκδοθείσας Κάρτας Οδηγού.
2. Περιλαμβάνονται άλλοι τύποι μηνυμάτων που κρίνονται κατάλληλοι για την αποτελεσματική λειτουργία του TACHOnet, παραδείγματος χάρη κοινοποιήσεις σφαλμάτων.
3. Τα εθνικά συστήματα αναγνωρίζουν τα καθεστώτα κάρτας που παρατίθενται στον πίνακα 1, όταν χρησιμοποιούν κάποια από τις λειτουργικότητες που περιγράφονται στο σημείο 1. Ωστόσο, τα συμβαλλόμενα μέρη δεν απαιτείται να εφαρμόζουν διοικητική διαδικασία στην οποία γίνεται χρήση όλων των απαριθμούμενων καθεστώτων.

4. Όταν συμβαλλόμενο μέρος παραλάβει απόκριση ή κοινοποίηση ότι καθεστώς δεν χρησιμοποιείται στις οικείες διοικητικές διαδικασίες, το εθνικό σύστημα μεταφράζει το καθεστώς που χρησιμοποιείται στο παραληφθέν μήνυμα με την κατάλληλη τιμή για τη συγκεκριμένη διαδικασία. Το μήνυμα δεν απορρίπτεται από το αποκρινόμενο συμβαλλόμενο μέρος, εφόσον το καθεστώς που χρησιμοποιείται στο μήνυμα περιλαμβάνεται στον πίνακα 1.
5. Τα καθεστώτα κάρτας που παρατίθενται στον πίνακα 1 δεν χρησιμοποιούνται για να προσδιορίζεται εάν η κάρτα οδηγού ισχύει για οδήγηση. Όταν συμβαλλόμενο μέρος υποβάλλει ερώτημα στο μητρώο της εθνικής αρχής που εξέδωσε την κάρτα μέσω της λειτουργικότητας CCS, η απόκριση περιέχει το ειδικό πεδίο «ισχύει για οδήγηση». Οι εθνικές διοικητικές διαδικασίες είναι σχεδιασμένες κατά τρόπο ώστε οι αποκρίσεις CCS να περιέχουν πάντα την ενδεδειγμένη τιμή «ισχύει για οδήγηση».

Πίνακας 1
Καθεστώτα κάρτας

Καθεστώς κάρτας	Ορισμός
Application (Αίτηση)	Η εκδίδουσα αρχή καρτών (CIA) έλαβε αίτηση έκδοσης κάρτας οδηγού. Η εν λόγω πληροφορία καταχωρίσθηκε και αποθηκεύτηκε στη βάση δεδομένων με τα κλειδιά αναζήτησης που δημιουργήθηκαν.
Approved (Εγκρίθηκε)	Η CIA ενέκρινε την αίτηση κάρτας ταχογράφου.
(Rejected) Απορρίφθηκε	Η CIA δεν ενέκρινε την αίτηση.
Personalised (Εξατομικεύτηκε)	Η κάρτα ταχογράφου εξατομικεύτηκε.
Dispatched (Απεστάλη)	Η εθνική αρχή απέστειλε την κάρτα οδηγού στον ενδιαφερόμενο οδηγό ή την παραδίδουσα υπηρεσία.
Handed Over (Παρεδόθη)	Η εθνική αρχή παρέδωσε την κάρτα οδηγού στον ενδιαφερόμενο οδηγό.
Confiscated (Κατασχέθηκε)	Η αρμόδια αρχή αφαίρεσε την κάρτα οδηγού από τον οδηγό.
Suspended (Ανεστάλη)	Η κάρτα οδηγού αφαιρέθηκε προσωρινά από τον οδηγό.
Withdrawn (Αποσύρθηκε)	Η CIA αποφάσισε να αποσύρει την κάρτα οδηγού. Η κάρτα ακυρώθηκε οριστικά.
Surrendered (Επεστράφη)	Η κάρτα ταχογράφου επεστράφη στη CIA και δηλώθηκε ως μη αναγκαία πλέον.
Lost (Απωλέσθη)	Δηλώθηκε απώλεια της κάρτας ταχογράφου στη CIA.
Stolen (Εκλάπη)	Δηλώθηκε κλοπή της κάρτας ταχογράφου στη CIA. Η κλοπή κάρτας θεωρείται ως απώλεια της κάρτας.
Malfunctioning (Ελαττωματική)	Δηλώθηκε στη CIA ότι η κάρτα ταχογράφου παρουσιάζει ελάττωμα.
Expired (Εληξε)	Η περίοδος ισχύος της κάρτας ταχογράφου έληξε.
Replaced (Αντικαταστάθηκε)	Η κάρτα ταχογράφου, για την οποία δηλώθηκε απώλεια, κλοπή ή ελάττωμα, αντικαταστάθηκε από νέα κάρτα. Τα δεδομένα στη νέα κάρτα παραμένουν τα ίδια, πλην του δείκτη αντικατάστασης του αριθμού της κάρτας, ο οποίος αυξήθηκε κατά ένα.

Renewed (Ανανεώθηκε)	Η κάρτα ταχογράφου ανανεώθηκε λόγω αλλαγής των διοικητικών δεδομένων ή λήξης της διάρκειας ισχύος. Ο αριθμός κάρτας της νέας κάρτας παραμένει ο ίδιος, πλην του δείκτη ανανέωσης του αριθμού της κάρτας, ο οποίος αυξήθηκε κατά ένα.
In Exchange (Σε ανταλλαγή)	Η CIA που εξέδωσε την κάρτα οδηγού παρέλαβε κοινοποίηση ότι κινήθηκε η διαδικασία ανταλλαγής της κάρτας με κάρτα οδηγού που εξέδωσε η CIA διαφορετικού συμβαλλομένου μέρους.
Exchanged (Ανταλλάχθηκε)	Η CIA που εξέδωσε την κάρτα οδηγού παρέλαβε κοινοποίηση ότι ολοκληρώθηκε η διαδικασία ανταλλαγής της κάρτας με κάρτα οδηγού που εξέδωσε η CIA διαφορετικού συμβαλλομένου μέρους.

Υποπροσάρτημα 4.3.

Διατάξεις για τα μηνύματα του TACHOnet

1. Γενικές τεχνικές απαιτήσεις
 - 1.1. Ο κεντρικός κόμβος παρέχει τόσο σύγχρονες όσο και ασύγχρονες διεπαφές για την ανταλλαγή μηνυμάτων. Τα συμβαλλόμενα μέρη δύνανται να επιλέξουν την πλέον κατάλληλη τεχνολογία για τη διεπαφή με τις οικείες εφαρμογές.
 - 1.2. Για όλα τα μηνύματα που ανταλλάσσονται μεταξύ του κεντρικού κόμβου και των εθνικών συστημάτων απαιτείται κωδικοποίηση UTF-8.
 - 1.3. Τα εθνικά συστήματα έχουν τη δυνατότητα να παραλαμβάνουν και να επεξεργάζονται μηνύματα που περιέχουν ελληνικούς ή κυριλλικούς χαρακτήρες.
2. Δομή μηνυμάτων XML και καθορισμός σχήματος (XSD)
 - 2.1. Η γενική δομή των μηνυμάτων XML ακολουθεί τον μορφότυπο που καθορίζεται από τα σχήματα XSD που είναι εγκατεστημένα στον κεντρικό κόμβο.
 - 2.2. Ο κεντρικός κόμβος και τα εθνικά συστήματα μεταδίδουν και παραλαμβάνουν μηνύματα τα οποία είναι σύμφωνα με το σχήμα XSD του μηνύματος.
 - 2.3. Τα εθνικά συστήματα έχουν τη δυνατότητα να αποστέλλουν, να παραλαμβάνουν και να επεξεργάζονται όλα τα μηνύματα που αντιστοιχούν σε οιαδήποτε από τις λειτουργικότητες που περιγράφονται στο υποπροσάρτημα 4.2.
 - 2.4. Τα μηνύματα XML περιλαμβάνουν τουλάχιστον τις ελάχιστες απαιτήσεις που καθορίζονται στον πίνακα 2.

Πίνακας 2

Ελάχιστες απαιτήσεις για το περιεχόμενο των μηνυμάτων XML

Κοινή επικεφαλίδα		Υποχρεωτικό
(Version) Έκδοση	Η επίσημη έκδοση των προδιαγραφών XML θα καθορίζεται από τον χώρο ονομάτων που ορίζεται στο σχήμα XSD του μηνύματος, καθώς και στο χαρακτηριστικό <i>έκδοση</i> του στοιχείου Επικεφαλίδα κάθε μηνύματος XML. Ο αριθμός έκδοσης («n.m») θα ορίζεται ως σταθερή τιμή σε κάθε κυκλοφορία του αρχείου καθορισμού του σχήματος XML (xsd).	Ναι
Test Identifier (Δοκιμαστικός αναγνωριστικός κωδικός)	Προαιρετικό αναγνωριστικό για δοκιμές. Ο αποστολέας της δοκιμής συμπληρώνει το αναγνωριστικό και όλοι οι συμμετέχοντες στη ροή εργασίας διαβιβάζουν/επιστρέφουν το ίδιο αναγνωριστικό. Σε περιβάλλον παραγωγής, το αναγνωριστικό δεν λαμβάνεται υπόψη και, εάν παρασχεθεί, δεν χρησιμοποιείται.	Όχι
Technical Identifier (Τεχνικός αναγνωριστικός κωδικός)	Διεθνής μοναδικός αναγνωριστικός κωδικός (UUID) που ταυτοποιεί κάθε μεμονωμένο μήνυμα. Ο αποστολέας δημιουργεί διεθνή μοναδικό αναγνωριστικό κωδικό και συμπληρώνει το εν λόγω χαρακτηριστικό. Τα δεδομένα αυτά δεν χρησιμοποιούνται σε επαγγελματικό επίπεδο.	Ναι
Workflow Identifier (Αναγνωριστικός κωδικός ροής εργασίας)	Ο αναγνωριστικός κωδικός ροής εργασίας συνίσταται σε διεθνή μοναδικό αναγνωριστικό κωδικό και δημιουργείται από το αιτούν συμβαλλόμενο μέρος. Στη συνέχεια ο εν λόγω αναγνωριστικός χρησιμοποιείται σε όλα τα μηνύματα για τη συσχέτιση της ροής εργασίας.	Ναι
Sent At (Εστάλη στις)	Η ημερομηνία και η ώρα (UTC) αποστολής του μηνύματος.	Ναι
Timeout (Χρόνος λήξης)	Προαιρετικό χαρακτηριστικό της ημερομηνίας και της ώρας (σε μορφότυπο UTC). Η τιμή αυτή καθορίζεται μόνο από τον κεντρικό κόμβο για αιτήσεις που του έχουν διαβιβαστεί. Κατ' αυτόν τον τρόπο, το αποκρινόμενο συμβαλλόμενο μέρος ενημερώνεται για τον χρόνο λήξης της αίτησης. Η τιμή αυτή δεν απαιτείται για τα MS2TCN_<x>_Req και για όλα τα μηνύματα απόκρισης. Είναι προαιρετική, ώστε να είναι δυνατή η χρήση της ίδιας επικεφαλίδας σε όλους τους τύπους μηνυμάτων, ανεξαρτήτως εάν απαιτείται το χαρακτηριστικό «χρόνος λήξης».	Όχι
Από	Ο κωδικός ISO 3166-1 Alpha 2 του συμβαλλομένου μέρους που αποστέλλει το μήνυμα ή «EU».	Ναι
Προς	Ο κωδικός ISO 3166-1 Alpha 2 του συμβαλλομένου μέρους στο οποίο αποστέλλεται το μήνυμα ή «EU».	Ναι

Υποπροσάρτημα 4.4

Μεταγραμματισμός και υπηρεσίες του συστήματος NYSIIS (New York State Identification and Intelligence System)

1. Ο αλγόριθμος NYSIIS που εφαρμόζεται στον κεντρικό κόμβο χρησιμοποιείται για την κωδικοποίηση των ονοματεπωνύμων όλων των οδηγών στο εθνικό μητρώο.
2. Κατά την αναζήτηση κάρτας μέσω της λειτουργίας CIC, τα κλειδιά NYSIIS χρησιμοποιούνται ως κύριος μηχανισμός αναζήτησης.
3. Επιπλέον, τα συμβαλλόμενα μέρη δύνανται να χρησιμοποιούν προσαρμοσμένο αλγόριθμο για να λαμβάνουν περισσότερα αποτελέσματα.
4. Τα αποτελέσματα της αναζήτησης αναφέρουν τον μηχανισμό αναζήτησης που χρησιμοποιήθηκε για την εύρεση καταγραφής, NYSIIS ή συνήθη.
5. Εάν συμβαλλόμενο μέρος επιλέξει να καταγράψει τις κοινοποιήσεις ICDL, τα κλειδιά NYSIIS που περιέχει η κοινοποίηση καταγράφονται ως τμήμα των δεδομένων ICDL. Κατά την αναζήτηση δεδομένων ICDL, το συμβαλλόμενο μέρος χρησιμοποιεί τα κλειδιά NYSIIS του ονόματος του αιτούντος.

Υποπροσάρτημα 4.5

Απαιτήσεις ασφάλειας

1. Για την ανταλλαγή μηνυμάτων μεταξύ του κεντρικού κόμβου και των εθνικών συστημάτων χρησιμοποιείται το πρωτόκολλο HTTPS.
2. Τα εθνικά συστήματα χρησιμοποιούν τα ψηφιακά πιστοποιητικά που αναφέρονται στα υποπροσάρτηματα 4.8 και 4.9 με στόχο την ασφαλή μετάδοση μηνυμάτων μεταξύ του εθνικού συστήματος και του κεντρικού κόμβου.
3. Τα εθνικά συστήματα εφαρμόζουν, κατ' ελάχιστο, πιστοποιητικά που χρησιμοποιούν αλγόριθμο τεμαχισμού SHA-2 (SHA-256) για υπογραφή και μήκος δημόσιου κλειδιού 2048 bit.

Υποπροσάρτημα 4.6
Επίπεδο εξυπηρέτησης

1. Τα εθνικά συστήματα πληρούν το ακόλουθο ελάχιστο επίπεδο εξυπηρέτησης:
 - 1.1. Είναι διαθέσιμα 24 ώρες την ημέρα, 7 ημέρες την εβδομάδα.
 - 1.2. Η διαθεσιμότητά τους παρακολουθείται μέσω μηνύματος «heartbeat» που εκδίδει ο κεντρικός κόμβος.
 - 1.3. Το ποσοστό διαθεσιμότητάς τους είναι 98 %, σύμφωνα με τον ακόλουθο πίνακα (τα στοιχεία έχουν στρογγυλοποιηθεί στην πλησιέστερη κατάλληλη μονάδα):

Διαθεσιμότητα	σημαίνει μη διαθεσιμότητα		
	Ημερησίως	Μηνιαίως	Ετησίως
98%	0,5 ωρών	15 ωρών	7,5 ημερών

Τα συμβαλλόμενα μέρη καλούνται να τηρούν το ποσοστό διαθεσιμότητας ημερησίως, αναγνωρίζεται όμως ότι ορισμένες απαραίτητες εργασίες, όπως οι εργασίες συντήρησης του συστήματος, απαιτούν χρόνο μη διαθεσιμότητας άνω των 30 λεπτών. Ωστόσο, τα ποσοστά διαθεσιμότητας μηνιαίως και ετησίως παραμένουν υποχρεωτικά.

- 1.4. Απαντούν σε ποσοστό τουλάχιστον 98 % των αιτήσεων που τους διαβιβάζονται εντός ενός ημερολογιακού μήνα.
- 1.5. Αποκρίνονται στα αιτήματα εντός 10 δευτερολέπτων.
- 1.6. Ο συνολικός χρόνος λήξης της αίτησης (το χρονικό διάστημα αναμονής του αιτούντος απόκριση) δεν υπερβαίνει τα 20 δευτερόλεπτα.
- 1.7. Είναι σε θέση να εξυπηρετούν αιτήσεις με ρυθμό 6 μηνυμάτων ανά δευτερόλεπτο.
- 1.8. Τα εθνικά συστήματα δεν επιτρέπεται να αποστέλλουν αιτήσεις στον κόμβο TACHOnet με ρυθμό άνω των 2 αιτήσεων ανά δευτερόλεπτο.

1.9. Όλα τα εθνικά συστήματα είναι σε θέση να αντιμετωπίζουν τυχόν τεχνικά προβλήματα του κεντρικού κόμβου ή των εθνικών συστημάτων άλλων συμβαλλομένων μερών. Στα προβλήματα αυτά συγκαταλέγονται, ενδεικτικά, τα εξής:

- α) απώλεια σύνδεσης με τον κεντρικό κόμβο·
- β) μη απόκριση σε αίτηση·
- γ) παραλαβή απόκρισης μετά τον χρόνο λήξης του μηνύματος·
- δ) παραλαβή ανεπίκλητων μηνυμάτων·
- ε) παραλαβή μη έγκυρων μηνυμάτων.

2. Ο κεντρικός κόμβος:

2.1. διαθέτει ποσοστό διαθεσιμότητας της τάξης του 98 %·

2.2. κοινοποιεί στα εθνικά συστήματα τυχόν σφάλματα, είτε με μήνυμα απόκρισης είτε με ειδικό μήνυμα σφάλματος. Αντιστοίχως, τα εθνικά συστήματα παραλαμβάνουν αυτά τα ειδικά μηνύματα σφάλματος και διαθέτουν ροή εργασίας κλιμάκωσης, για να προβαίνουν σε κάθε κατάλληλη ενέργεια για τη διόρθωση του κοινοποιηθέντος σφάλματος.

3. Συντήρηση

Τα συμβαλλόμενα μέρη κοινοποιούν στα άλλα συμβαλλόμενα μέρη και στην Ευρωπαϊκή Επιτροπή τυχόν εργασίες συντήρησης ρουτίνας μέσω της διαδικτυακής εφαρμογής τουλάχιστον μία εβδομάδα πριν από την έναρξη των εν λόγω εργασιών, εάν αυτό είναι τεχνικώς εφικτό.

Υποπροσάρτημα 4.7

Καταγραφή και στατιστικά στοιχεία των δεδομένων που συλλέγονται στον κεντρικό κόμβο

1. Για να διασφαλιστεί η προστασία των προσωπικών δεδομένων, τα δεδομένα για στατιστικούς σκοπούς είναι ανώνυμα. Τα αναγνωριστικά στοιχεία δεδομένων συγκεκριμένης κάρτας, άδειας οδήγησης ή συγκεκριμένου οδηγού δεν είναι διαθέσιμα για στατιστικούς σκοπούς.
2. Μέσω των στοιχείων καταγραφής ιχνηλατούνται όλες οι συναλλαγές παρακολούθησης και εντοπισμού σφαλμάτων, και καθίσταται δυνατή η παραγωγή στατιστικών για τις συναλλαγές αυτές.
3. Τα προσωπικά δεδομένα δεν διατηρούνται στα αρχεία καταγραφής επί περισσότερο από 6 μήνες. Οι στατιστικές πληροφορίες διατηρούνται για απεριόριστο χρονικό διάστημα.
4. Τα στατιστικά στοιχεία που χρησιμοποιούνται για την υποβολή αναφορών περιλαμβάνουν:
 - α) το αιτούν συμβαλλόμενο μέρος·
 - β) το αποκρινόμενο συμβαλλόμενο μέρος·
 - γ) τον τύπο του μηνύματος·
 - δ) τον κωδικό καθεστώτος της απόκρισης·
 - ε) την ημερομηνία και την ώρα των μηνυμάτων·
 - στ) τον χρόνο απόκρισης.

Υποπροσάρτημα 4.8

Γενικές διατάξεις για τα ψηφιακά κλειδιά και τα πιστοποιητικά για το TACHOnet

1. Η Γενική Διεύθυνση Πληροφορικής της Ευρωπαϊκής Επιτροπής (ΓΔ DIGIT) διαθέτει υπηρεσία υποδομής δημόσιου κλειδιού (PKI)¹ (αναφερόμενη ως «υπηρεσία CEF PKI») στα συμβαλλόμενα μέρη της AETR που συνδέονται με το TACHOnet (εφεξής «εθνικές αρχές») μέσω της υπηρεσίας eDelivery.
2. Η διαδικασία αίτησης και ανάκλησης ψηφιακών πιστοποιητικών, καθώς και οι λεπτομερείς όροι και προϋποθέσεις χρήσης τους, καθορίζονται στο προσάρτημα.
3. Χρήση των πιστοποιητικών
 - 3.1. Μόλις εκδοθεί το πιστοποιητικό, η εθνική αρχή² το χρησιμοποιεί μόνον στο TACHOnet. Το πιστοποιητικό είναι δυνατό να χρησιμοποιείται για:
 - α) τον έλεγχο αυθεντικότητας της προέλευσης του μηνύματος·
 - β) την κρυπτογράφηση δεδομένων·
 - γ) τον εντοπισμό παραβίασης της ακεραιότητας δεδομένων.
 - 3.2. Απαγορεύεται οποιαδήποτε μη ρητά εξουσιοδοτημένη χρήση από τις επιτρεπόμενες χρήσεις του πιστοποιητικού.
4. Τα συμβαλλόμενα μέρη:
 - α) προστατεύουν τα οικεία ιδιωτικά κλειδιά από μη εξουσιοδοτημένη χρήση τους·
 - β) δεν μεταβιβάζουν, ούτε αποκαλύπτουν τα οικεία ιδιωτικά κλειδιά σε τρίτα μέρη, ακόμη και εάν πρόκειται για εκπροσώπους·

¹ PKI (Public Key Infrastructure/υποδομή δημόσιου κλειδιού) είναι ένα σύνολο ρόλων, πολιτικών, διαδικασιών και συστημάτων αναγκαίων για τη δημιουργία, τη διαχείριση, τη διανομή και την ανάκληση ψηφιακών πιστοποιητικών.

² την ταυτοποιημένη με την τιμή χαρακτηριστικού «O=» στο αποκλειστικό όνομα υποκειμένου του εκδοθέντος πιστοποιητικού

- γ) διασφαλίζουν την εμπιστευτικότητα, την ακεραιότητα και τη διαθεσιμότητα των ιδιωτικών κλειδιών που δημιουργούνται, αποθηκεύονται και χρησιμοποιούνται για το TACHOnet·
- δ) δεν συνεχίζουν τη χρήση των ιδιωτικών κλειδιών μετά τη λήξη ισχύος τους ή την ανάκληση του πιστοποιητικού, εξαιρουμένης της προβολής κρυπτογραφημένων δεδομένων (π.χ. για την αποκρυπτογράφηση ηλεκτρονικών μηνυμάτων). Τα ληγμένα κλειδιά είτε καταστρέφονται είτε διατηρούνται κατά τρόπο απαγορευτικό για τη χρήση τους·
- ε) παρέχουν στην αρχή καταχώρισης το αναγνωριστικό των εξουσιοδοτημένων εκπροσώπων οι οποίοι είναι εξουσιοδοτημένοι να ζητούν την ανάκληση πιστοποιητικών που έχουν εκδοθεί στον φορέα (οι αιτήσεις ανάκλησης περιέχουν τον κλειδάριθμο της αίτησης ανάκλησης και στοιχεία σχετικά με τα συμβάντα που οδήγησαν στην ανάκληση)·
- στ) αποτρέπουν την κατάχρηση των ιδιωτικών κλειδιών με αίτηση ανάκλησης του σχετικού πιστοποιητικού δημόσιου κλειδιού σε περίπτωση παραβίασης του ιδιωτικού κλειδιού ή των δεδομένων ενεργοποίησης του ιδιωτικού κλειδιού·
- ζ) ευθύνονται για την ανάκληση πιστοποιητικού και υποχρεούνται να την ζητήσουν στις περιστάσεις που προσδιορίζονται στις πολιτικές πιστοποίησης (CPS) και στη δήλωση πρακτικών πιστοποίησης (CPS) της αρχής πιστοποίησης·
- η) κοινοποιούν αμέσως στην αρχή καταχώρισης την απώλεια, την κλοπή ή τυχόν παραβίαση κλειδιού της AETR χρησιμοποιούμενου στο TACHOnet.

5. Υποχρεώσεις

Με την επιφύλαξη της ευθύνης της Ευρωπαϊκής Επιτροπής κατά παράβαση οποιασδήποτε απαίτησης καθορισμένης στο εφαρμοστέο εθνικό δίκαιο ή ευθύνης της σε θέματα μη εξαιρούμενων βάσει του εν λόγω δικαίου, η Ευρωπαϊκή Επιτροπή δεν ευθύνεται όσον αφορά:

- α) το περιεχόμενο του πιστοποιητικού, για το οποίο ευθύνεται αποκλειστικά ο κάτοχος. Ο κάτοχος του πιστοποιητικού έχει την ευθύνη να ελέγχει την ακρίβεια του περιεχομένου του πιστοποιητικού·
- β) τη χρήση του πιστοποιητικού από τον κάτοχό του.

Υποπροσάρτημα 4.9

Περιγραφή της υπηρεσίας PKI για το TACHOnet

1. Εισαγωγή

Η PKI (Public Key Infrastructure/υποδομή δημόσιου κλειδιού) είναι ένα σύνολο ρόλων, πολιτικών, διαδικασιών και συστημάτων αναγκαίων για τη δημιουργία, τη διαχείριση, τη διανομή και την ανάκληση ψηφιακών πιστοποιητικών³. Η υπηρεσία CEF PKI του eDelivery επιτρέπει την έκδοση και τη διαχείριση των ψηφιακών πιστοποιητικών που χρησιμοποιούνται για να διασφαλίζεται η εμπιστευτικότητα, η ακεραιότητα και η μη αποκήρυξη των πληροφοριών που ανταλλάσσονται μεταξύ των σημείων πρόσβασης (AP).

Η υπηρεσία PKI του eDelivery έχει τη βάση της στην Trust Center Services TeleSec Shared Business CA (αρχή πιστοποίησης) στην οποία εφαρμόζονται⁴ η πολιτική πιστοποίησης (CP) / η δήλωση πρακτικών πιστοποίησης (CPS) της TeleSec Shared-Business-CA της T-Systems International GmbH.

Η υπηρεσία PKI εκδίδει πιστοποιητικά κατάλληλα για την ασφάλεια διαφόρων επιχειρηματικών διεργασιών εντός και εκτός εταιρειών, φορέων, δημοσίων αρχών και οργάνων, για τα οποία απαιτείται μέσο επίπεδο ασφάλειας για την απόδειξη της αυθεντικότητας, της ακεραιότητας και της αξιοπιστίας της τελικής αποδέκτριας οντότητας.

2. Διαδικασία αίτησης πιστοποιητικού

2.1. Ρόλοι και αρμοδιότητες

2.1.1. «Φορέας» ή «εθνική αρχή» που αιτείται το πιστοποιητικό

2.1.1.1. Η εθνική αρχή αιτείται τα πιστοποιητικά για το έργο TACHOnet.

2.1.1.2 Η εθνική αρχή:

α) αιτείται τα πιστοποιητικά από την υπηρεσία CEF PKI.

³ https://en.wikipedia.org/wiki/Public_key_infrastructure

⁴ Η τελευταία έκδοση των CP και CPS μπορεί να τηλεφορτωθεί από τη διεύθυνση <https://www.telesec.de/en/sbca-en/support/download-area/>

- β) παράγει τα ιδιωτικά κλειδιά και τα αντίστοιχα δημόσια κλειδιά που πρέπει να περιέχουν τα πιστοποιητικά που εκδίδει η αρχή πιστοποίησης·
- γ) τηλεφορτώνει το πιστοποιητικό μόλις εκδοθεί·
- δ) υπογράφει και επιστρέφει στην αρχή καταχώρισης:
 - i) το έντυπο ταυτοποίησης των προσώπων επικοινωνίας και των εμπιστευμένων ταχυδρόμων,
 - ii) το υπογεγραμμένο ατομικό πληρεξούσιο⁵.

2.1.2. Εμπιστευμένος ταχυδρόμος

2.1.2.1. Η εθνική αρχή ορίζει εμπιστευμένο ταχυδρόμο.

2.1.2.2. Ο εμπιστευμένος ταχυδρόμος:

- α) παραδίδει το δημόσιο κλειδί στην αρχή καταχώρισης με διαδικασία ταυτοποίησης και καταχώρισης αυτοπροσώπως·
- β) παραλαμβάνει το σχετικό πιστοποιητικό από την αρχή καταχώρισης.

2.1.3. Κάτοχος τομέα

2.1.3.1. Κάτοχος τομέα είναι η ΓΔ MOVE.

2.1.3.2. Ο κάτοχος τομέα:

- α) επικυρώνει και συντονίζει το δίκτυο TACHOnet και την αρχιτεκτονική εμπιστευσης του TACHOnet, όπως επίσης επικυρώνει τις διαδικασίες έκδοσης των πιστοποιητικών·
- β) χειρίζεται τον κεντρικό κόμβο του TACHOnet και συντονίζει τη δραστηριότητα των συμβαλλομένων μερών όσον αφορά τη λειτουργία του TACHOnet·
- γ) εκτελεί, μαζί με τις εθνικές αρχές, τις δοκιμές σύνδεσης με το TACHOnet.

⁵Πληρεξούσιο είναι ένα νομικό έγγραφο με το οποίο ο φορέας εξουσιοδοτεί την Ευρωπαϊκή Επιτροπή, εκπροσωπούμενη από τον ταυτοποιημένο υπάλληλό της αρμόδιο για την υπηρεσία CEF PKI, και της επιτρέπει να ζητεί την παραγωγή πιστοποιητικού εξ ονόματός της από την T-Systems International GmbH TeleSec Shared Business CA. Βλ. επίσης σημείο 6.

2.1.4. Αρχή καταχώρισης

2.1.4.1. Αρχή καταχώρισης είναι το Κοινό Κέντρο Ερευνών (ΚΚΕρ).

2.1.4.2. Η αρχή καταχώρισης είναι αρμόδια για την εξακρίβωση της ταυτότητας του εμπιστευμένου ταχυδρόμου, την καταχώριση και την έγκριση των αιτήσεων έκδοσης, ανάκλησης και ανανέωσης των ψηφιακών πιστοποιητικών.

2.1.4.3. Η αρχή καταχώρισης:

- α) αποδίδει μοναδικό αναγνωριστικό στην εθνική αρχή·
- β) ελέγχει την ταυτότητα της εθνικής αρχής, των σημείων επαφής της και των εμπιστευμένων ταχυδρόμων της·
- γ) επικοινωνεί με την υποστήριξη CEF για την αυθεντικότητα της εθνικής αρχής, των σημείων επαφής της και των εμπιστευμένων ταχυδρόμων της·
- δ) ενημερώνει την εθνική αρχή για την έγκριση ή την απόρριψη πιστοποιητικού.

2.1.5. Αρχή πιστοποίησης

2.1.5.1. Η αρχή πιστοποίησης είναι αρμόδια για την παροχή της τεχνικής υποδομής αίτησης, έκδοσης και ανάκλησης των ψηφιακών πιστοποιητικών.

2.1.5.2. Η αρχή πιστοποίησης:

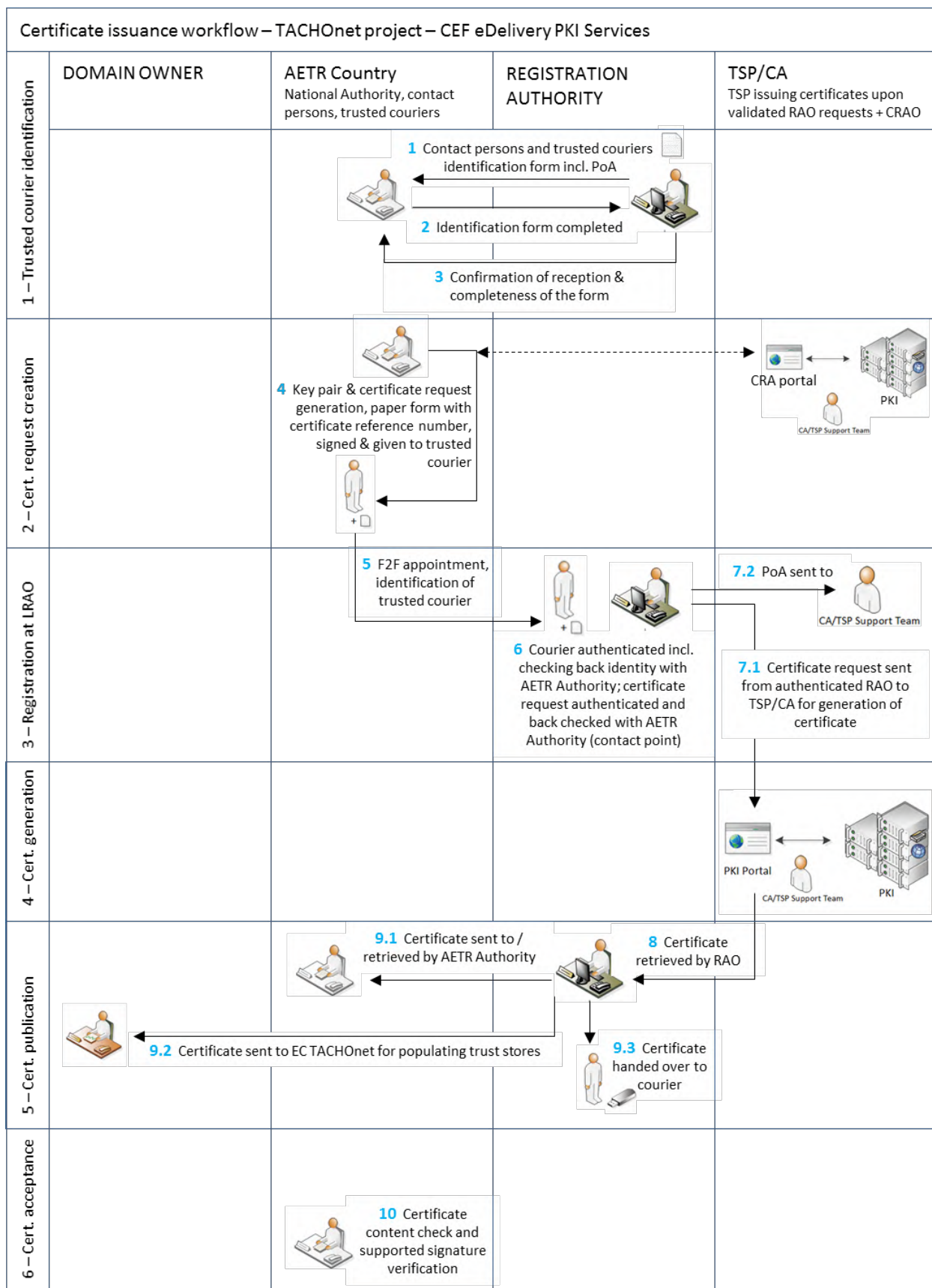
- α) παρέχει την τεχνική υποδομή για αιτήσεις πιστοποιητικών από εθνικές αρχές·
- β) επικυρώνει ή απορρίπτει αίτηση για πιστοποιητικό·
- γ) επικοινωνεί με την αρχή καταχώρισης για την εξακρίβωση της ταυτότητας του αιτούντος φορέα, όταν απαιτείται.

2.2. Έκδοση πιστοποιητικού

2.2.1. Η έκδοση πιστοποιητικού πραγματοποιείται σύμφωνα με τις ακόλουθες διαδοχικές ενέργειες που αναπαριστώνται στο σχήμα 1:

- α) **1η ενέργεια:** Ταυτοποίηση του εμπιστευμένου ταχυδρόμου·

- β) **2η ενέργεια:** Δημιουργία αίτησης για πιστοποιητικό.
- γ) **3η ενέργεια:** Καταχώριση στην αρχή καταχώρισης.
- δ) **4η ενέργεια:** Δημιουργία του πιστοποιητικού.
- ε) **5η ενέργεια:** Δημοσίευση του πιστοποιητικού.
- στ) **6η ενέργεια:** Αποδοχή του πιστοποιητικού.



Σχήμα 1 - Ροή εργασίας έκδοσης πιστοποιητικού

2.2.2. 1η ενέργεια: Ταυτοποίηση του εμπιστευμένου ταχυδρόμου·

Για την ταυτοποίηση του εμπιστευμένου ταχυδρόμου ακολουθείται η κάτωθι διαδικασία:

- α) Η αρχή καταχώρισης αποστέλλει στην εθνική αρχή το έντυπο ταυτοποίησης των προσώπων επικοινωνίας και των εμπιστευμένων ταχυδρόμων⁶. Το εν λόγω έντυπο περιλαμβάνει επίσης το πληρεξούσιο το οποίο υπογράφει ο φορέας (αρχή της AETR).
- β) Η εθνική αρχή επιστρέφει στην αρχή καταχώρισης συμπληρωμένο το έντυπο και υπογεγραμμένο το πληρεξούσιο.
- γ) Η αρχή καταχώρισης βεβαιώνει την παραλαβή και την πληρότητα του εντύπου.
- δ) Η αρχή καταχώρισης παρέχει στον κάτοχο τομέα επικαιροποιημένο αντίτυπο του καταλόγου με τα πρόσωπα επικοινωνίας και τους εμπιστευμένους ταχυδρόμους.

2.2.3. 2η ενέργεια: Δημιουργία αίτησης για πιστοποιητικό·

2.2.3.1. Η αίτηση και η ανάκτηση πιστοποιητικού πραγματοποιούνται στον ίδιο υπολογιστή και με το ίδιο λογισμικό περιήγησης.

2.2.3.2. Για τη δημιουργία αίτησης για πιστοποιητικό ακολουθείται η κάτωθι διαδικασία:

- α) Ο φορέας περιηγείται στη διεπαφή του χρήστη για να αιτηθεί το πιστοποιητικό μέσω του ομοιόμορφου εντοπιστή πόρου (URL)
<https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en>: και εισάγει την ταυτότητα χρήστη «**sbca/CEF_eDelivery.europa.eu**» και τον κλειδάριθμο «**digit.333**»

⁶ Βλ. σημείο 5

Version: 1.5.5 Home German RSS Newsletter Locations Contact

■ end entity certificate
request
fetch
revoke
renew
search
■ login
■ CRL
■ CA certificates
■ Informations

Login

All actions in the "User certificate" menu option are security critical and require login. The "informations | documents" section can also only be entered after login.

You will receive the relevant login data from your responsible sub-registrar.

login:

password:

Login cancel

© 2007-2013 T-Systems International GmbH. All rights reserved. Deutsche Telekom About this Website Privacy Policy Sitemap Glossary

Σχήμα 2

- β) Ο φορέας κάνει κλικ στο «request» (αίτηση) στην αριστερή πλευρά του πίνακα και επιλέγει «CEF_TACHOnet» στον αναπτυσσόμενο κατάλογο.

■ End entity certificate
■ request
fetch
revoke
renew
search
logout
■ CRL
■ CA certificates
■ Information

User certificate

To issue a certificate for a user, please fill in the following certificate application.

Please fill in at least the input fields marked with an asterisk (*) (mandatory fields). Here, you can enter additional data that is not included in the certificate but which is used by the registration authority to identify the applicant.

Subdomain: CEF_ELRC-SHARE ▼

Σχήμα 3

- γ) Ο φορέας συμπληρώνει το έντυπο αίτησης για πιστοποιητικό που παρατίθεται στο σχήμα 4 με τις πληροφορίες του πίνακα 3, κάνοντας κλικ στο «Next (soft-PSE)» για να περατώσει τη διαδικασία.

Must start with: 'GRP-' concatenated with CEF_TACHOnet_<TYPE>_<COUNTRY CODE>_<Unique_Identifier_of_the_Access_Point>

TYPE=AP_PROD
COUNTRY CODE = as defined above.
E.g.:
'GRP: CEF_TACHOnet_AP_PROD_BE_001'

Organisation's Country Code (Case Sensitive, ISO 3166-1)

Official Organisation Name (case sensitive)

Must be:
TYPE=AP_PROD
concatenated with '/' separator and
'GTC_OID-1.3.130.0.2018.xxxxxx' where Ares(2018)xxxxxx is the allocated number

Must be:
'CEF-EDELIVERY-SUPPORT@ec.europa.eu'

Must be the official address of the Organisation. (Used for the Power of Attorney.)
Attention: if the ZIP code is NOT a 5-digit ZIP code, leave the ZIP code field empty and put the ZIP code in the City field.

Email: the email address must be the same as the one used for registering the Unique Identifier.
+ Name of the person representing the organisation. (Used for the Power of Attorney)

The organisation can choose its own password or click on the button 'Adopt revocation password proposal'

Click here to end

Country: BE

Organisation/company (O): My Company

Internet domain (OU1): CEF_eDelivery.europa.eu

Responsibility (OU2): CEF_TACHOnet

Identifier (OU3): AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx

First name (CN): Leave Empty

Last name (CN): GRP:CEF_TACHOnet_AP_PROD_BE_001

E-mail: CEF-EDELIVERY-SUPPORT@ec.europa.eu

E-mail 1 (SAN): Leave Empty

E-mail 2 (SAN): Leave Empty

E-mail 3 (SAN): Leave Empty

Address: Leave Empty

Street: Street no.

ZIP code: City

Phone no.: Leave Empty

business.register.xx@mail.com

Mr Johan Smith

Identification data:

* Revocation password: (max. 50 characters)

* Revocation password repetition: (max. 50 characters)

Revocation password proposal: juHEVeV136

Adopt revocation password proposal

Next (soft-PSE)

Next (SmartCard/applet) Cancel

Σχήμα 4

Ζητούμενα πεδία	Περιγραφή
Χώρα	C=Κωδικός χώρας, τόπος του κατόχου του πιστοποιητικού, κατόπιν εξακρίβωσης σε δημόσιο κατάλογο· Περιορισμοί: 2 χαρακτήρες σύμφωνα με το ISO 3166-1, alpha-2, με διάκριση μεταξύ κεφαλαίων και μικρών· Παραδείγματα: DE, BE, NL, Ειδικές περιπτώσεις: UK (για τη μεγάλη Βρετανία), EL (για την Ελλάδα)
Φορέας/Εταιρεία (O)	O=Όνομα του φορέα κατόχου του πιστοποιητικού
Κύριος τομέας (OU1)	OU=CEF_eDelivery.europa.eu
Πεδίο αρμοδιότητας (OU2)	OU=CEF_TACHOnet
Τμήμα (OU3)	Υποχρεωτική τιμή ανά «AREA OF RESPONSIBILITY» (ΠΕΔΙΟ ΑΡΜΟΔΙΟΤΗΤΑΣ) Το περιεχόμενο πρέπει να ελέγχεται με τη χρήση θετικού καταλόγου (λευκός κατάλογος) όταν ζητείται το πιστοποιητικό. Εάν οι πληροφορίες δεν αντιστοιχούν στον κατάλογο, η αίτηση απορρίπτεται. Μορφότυπος: OU=<TYPE>-<GTC_NUMBER> Όπου το «<TYPE>» αντικαθίσταται από το AP_PROD: Σημείο πρόσβασης σε περιβάλλον παραγωγής. Και όπου <GTC_NUMBER> είναι GTC_OID-1.3.130.0.2018.xxxxxx, όπου Ares(2018)xxxxxx είναι ο αριθμός GTC για το έργο TACHOnet. Π.χ.: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First name (Όνομα) (CN):	Πρέπει να αφήεται κενό
Last name (CN) (Επώνυμο)	Πρέπει να αρχίζει με «GRP:», ακολουθούμενο από κοινό όνομα. Μορφότυπος: CN=GRP:<AREA OF RESPONSIBILITY (ΠΕΔΙΟ ΑΡΜΟΔΙΟΤΗΤΑΣ)>_<TYPE (ΤΥΠΟΣ)>_<COUNTRY CODE (ΚΩΔΙΚΟΣ ΧΩΡΑΣ)>_<UNIQUE IDENTIFIER (ΜΟΝΑΔΙΚΟ ΑΝΑΓΝΩΡΙΣΤΙΚΟ)> Π.χ.: GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail (Ηλεκτρονική διεύθυνση)	E=CEF-EDELIVERY-SUPPORT@ec.europa.eu
E-mail 1 (Ηλεκτρονική διεύθυνση 1) (SAN)	Πρέπει να αφήεται κενό
E-mail 2 (Ηλεκτρονική διεύθυνση 1) (SAN)	Πρέπει να αφήεται κενό
E-mail 3 (Ηλεκτρονική διεύθυνση 1) (SAN)	Πρέπει να αφήεται κενό

Address (Διεύθυνση)	Πρέπει να αφήται κενό
Street (Οδός)	Πρέπει να είναι η επίσημη διεύθυνση του φορέα κατόχου του πιστοποιητικού. (Χρησιμοποιείται για το πληρεξούσιο.)
Street no. (Οδός αριθ.)	Πρέπει να είναι η επίσημη διεύθυνση του φορέα κατόχου του πιστοποιητικού. (Χρησιμοποιείται για το πληρεξούσιο.)
Zip Code (Ταχυδρομικός κώδικας)	Πρέπει να είναι η επίσημη διεύθυνση του φορέα κατόχου του πιστοποιητικού. (Χρησιμοποιείται για το πληρεξούσιο.) <u>Προσοχή:</u> εάν ο ταχυδρομικός κώδικας ΔΕΝ είναι 5ψήφιος, το πεδίο του ταχυδρομικού κώδικα αφήται κενό και ο ταχυδρομικός κώδικας συμπληρώνεται στο πεδίο της πόλης.
City (Πόλη)	Πρέπει να είναι η επίσημη διεύθυνση του φορέα κατόχου του πιστοποιητικού. (Χρησιμοποιείται για το πληρεξούσιο.) <u>Προσοχή:</u> εάν ο ταχυδρομικός κώδικας ΔΕΝ είναι 5ψήφιος, το πεδίο του ταχυδρομικού κώδικα αφήται κενό και ο ταχυδρομικός κώδικας συμπληρώνεται στο πεδίο της πόλης.
Phone no (Αριθ. τηλεφ.)	Πρέπει να αφήται κενό
Identification data (Στοιχεία ταυτοποίησης)	Η ηλεκτρονική διεύθυνση πρέπει να είναι η ίδια με εκείνη που χρησιμοποιείται για την καταχώριση του μοναδικού αναγνωριστικού. + Πρέπει να είναι το όνομα του προσώπου που εκπροσωπεί τον φορέα. (Χρησιμοποιείται για το πληρεξούσιο) + Αριθ. εμπορικού μητρώου (υποχρεωτικό μόνον για τους ιδιωτικούς φορείς) Εισήχθη στο τοπικό δικαστήριο (απαιτείται μόνον για τους ιδιωτικούς φορείς της Γερμανίας και της Αυστρίας)
Revocation password (Κλειδάριθμος ανάκλησης)	Υποχρεωτικό πεδίο που έχει επιλέξει ο αιτών
Revocation password repetition (Επανάληψη κλειδάριθμου ανάκλησης)	Επανάληψη του υποχρεωτικού πεδίου που έχει επιλέξει ο αιτών

Πίνακας 3. Πλήρη στοιχεία κάθε ζητούμενου πεδίου

δ) Το μήκος του επιλεγέντος κλειδιού είναι 2048 (υψηλός βαθμός)

The screenshot shows the 'User certificate' page of the T-Systems portal. On the left is a sidebar with a menu: 'End entity certificate' (expanded), 'request' (selected), 'fetch', 'revoke', 'renew', 'search', 'logout', 'CRL', 'CA certificates', and 'Information'. The main content area is titled 'User certificate' and contains instructions about key length and a note about approval. Below this is a 'Certificate data' section with a form. The form fields are: Country (C) [BE], Organization/company (O) [European Commission], Master domain (OU1) [CEF_eDelivery.europa.eu], Area of responsibility (OU2) [CEF_TACHOnet], Department (OU3) [AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx], First name (CN) [], Last name (CN) [GRP:CEF_TACHOnet_AP_PROD_BE_001], E-mail [CEF-EDELIVERY-SUPPORT@ec.europa.eu], and Selection of key length [2048 (High Grade)]. At the bottom of the form are 'Request' and 'Cancel' buttons. The footer includes copyright information for 2007-2019 T-Systems International GmbH and links to 'Deutsche Telekom', 'About this Website', 'Privacy Policy', 'Sitemap', and 'Glossary'.

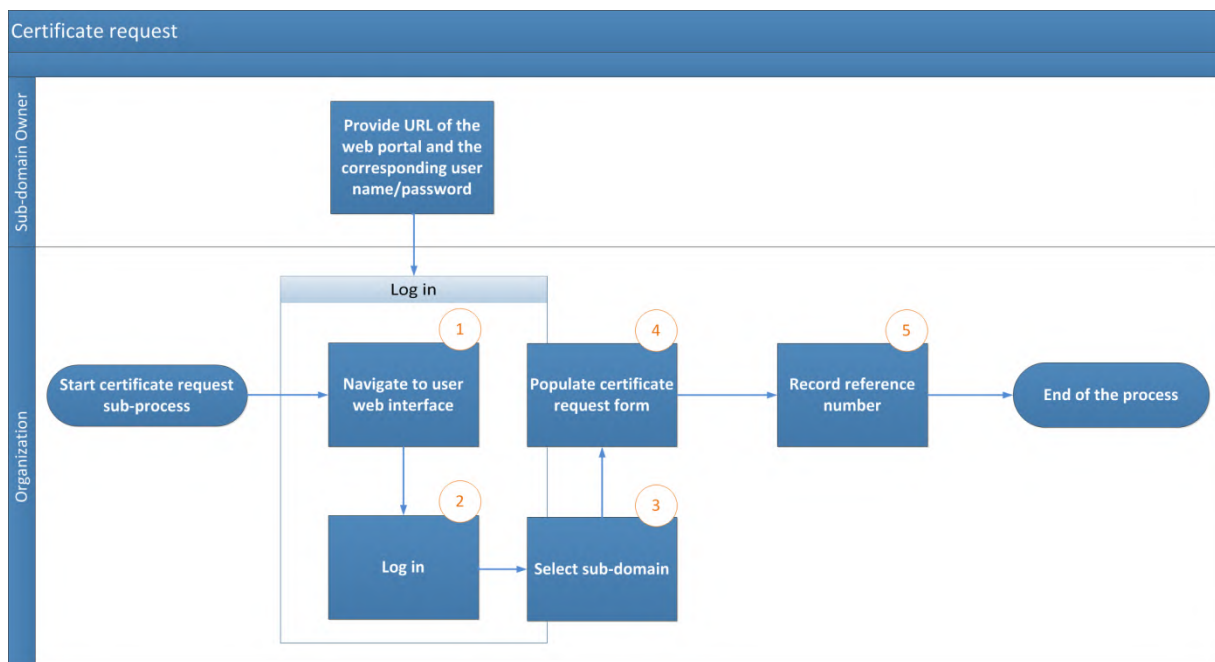
Σχήμα 5

ε) Ο φορέας καταγράφει τον αριθμό αναφοράς για να ανακτήσει το πιστοποιητικό.

This screenshot shows the confirmation page after a certificate request. The sidebar is identical to the previous screenshot. The main content area, titled 'User certificate', displays the message: 'The certificate was requested. Your request was stored with reference number 776002.' Below this is the same approval note. A blue callout bubble with the text 'Certificate Reference Number' points to the reference number '776002'. The footer is the same as in the previous screenshot.

Σχήμα 6

- στ) Η ομάδα υποστήριξης CEF ελέγχει εάν υπάρχουν νέες αιτήσεις για πιστοποιητικό και εξακριβώνει εάν είναι έγκυρες οι πληροφορίες στην αίτηση για το πιστοποιητικό, δηλ. εάν είναι σύμφωνες με τη σύμβαση ονοματοδοσίας που προσδιορίζεται στο προσάρτημα 5.1 Σύμβαση ονοματοδοσίας πιστοποιητικού.
- ζ) Η ομάδα υποστήριξης CEF ελέγχει εάν οι πληροφορίες που εισάχθηκαν στην αίτηση είναι σε έγκυρο μορφότυπο.
- η) Σε περίπτωση αρνητικού αποτελέσματος στον έλεγχο του σημείου 5 ή 6 ανωτέρω, η ομάδα υποστήριξης CEF αποστέλλει ηλεκτρονικό μήνυμα στην ηλεκτρονική διεύθυνση που έχει συμπληρωθεί στο «Στοιχεία ταυτοποίησης» του εντύπου της αίτησης, με κοινοποίηση στον κάτοχο του τομέα, με το οποίο ζητείται από τον φορέα να αρχίσει εκ νέου τη διαδικασία. Η αποτυχημένη αίτηση για πιστοποιητικό ακυρώνεται.
- θ) Η ομάδα υποστήριξης CEF αποστέλλει ηλεκτρονικό μήνυμα στην αρχή καταχώρισης σχετικά με την εγκυρότητα της αίτησης. Το ηλεκτρονικό μήνυμα περιέχει:
- (1) το όνομα του φορέα, όπως έχει συμπληρωθεί στο πεδίο «Organisation (O)» (Φορέας) της αίτησης πιστοποιητικού·
 - (2) τα δεδομένα του πιστοποιητικού με το όνομα του σημείου πρόσβασης για το οποίο πρόκειται να εκδοθεί το πιστοποιητικό, όπως έχει συμπληρωθεί στο πεδίο «Last Name (CN)» (Επώνυμο) της αίτησης πιστοποιητικού·
 - (3) τον αριθμό αναφοράς του πιστοποιητικού·
 - (4) τη διεύθυνση του φορέα, την ηλεκτρονική του διεύθυνση και το ονοματεπώνυμο του προσώπου που τον εκπροσωπεί.



Σχήμα 7 – Διαδικασία αίτησης πιστοποιητικού

2.2.4.3η ενέργεια: Καταχώριση στην αρχή καταχώρισης (έγκριση του πιστοποιητικού)

2.2.4.1. Ο εμπιστευμένος ταχυδρόμος ή το σημείο επαφής συμφωνούν με την αρχή καταχώρισης να συναντηθούν με ανταλλαγή μηνυμάτων, στα οποία ταυτοποιείται ο εμπιστευμένος ταχυδρόμος που θα προβεί στη συνάντηση αυτοπροσώπως.

2.2.4.2. Ο φορέας ετοιμάζει το πακέτο τεκμηρίωσης, το οποίο συνίσταται:

- α) στο συμπληρωμένο και υπογεγραμμένο πληρεξούσιο,
- β) σε αντίγραφο του έγκυρου διαβατηρίου του εμπιστευμένου ταχυδρόμου που θα προβεί στην συνάντηση αυτοπροσώπως. Το αντίγραφο πρέπει να έχει υπογραφεί από ένα από τα σημεία επαφής του ταυτοποιημένου στην 1η ενέργεια φορέα·
- γ) στο έντυπο αίτησης πιστοποιητικού υπογεγραμμένο από ένα από τα σημεία επαφής του ταυτοποιημένου στην 1η ενέργεια φορέα.

2.2.4.3. Η αρχή καταχώρισης δέχεται στην είσοδο του κτηρίου τον εμπιστευμένο ταχυδρόμο μετά από έλεγχο της ταυτότητάς του. Η αρχή καταχώρισης διενεργεί αυτοπροσώπως καταχώριση της αίτησης πιστοποιητικού με:

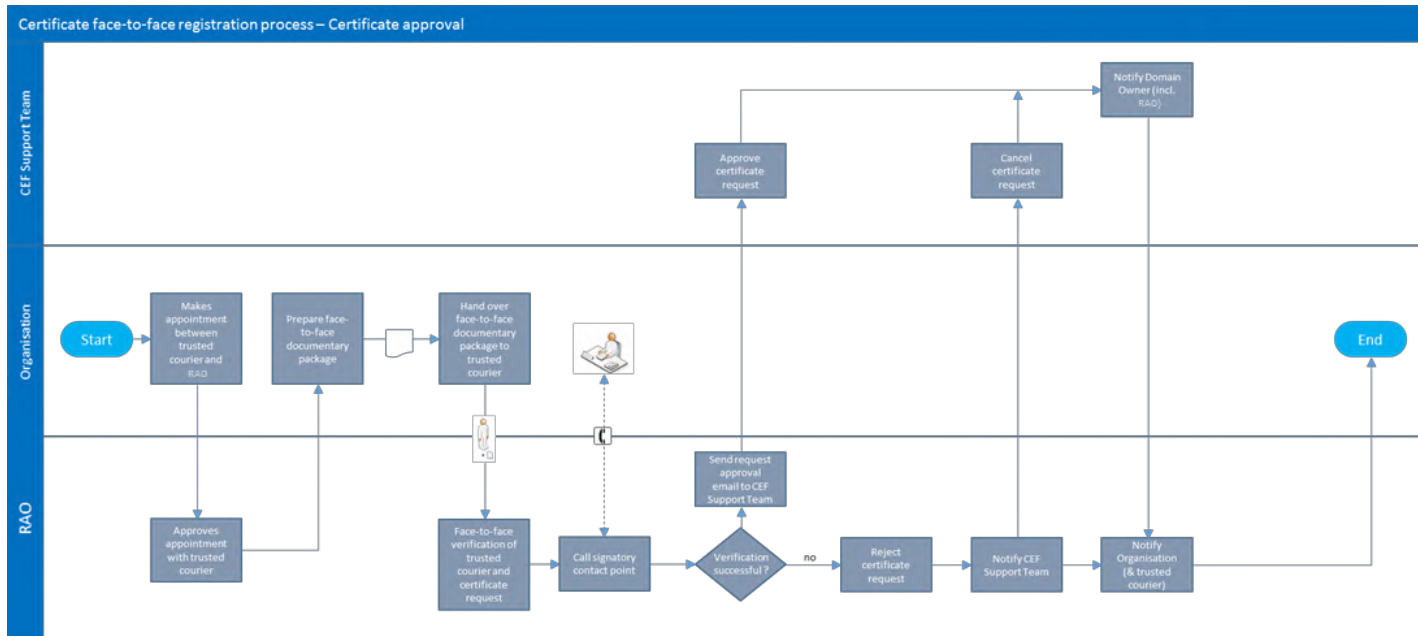
- α) ταυτοποίηση και έλεγχο της ταυτότητας του εμπιστευμένου ταχυδρόμου·
- β) επαλήθευση της σωματικής εμφάνισης του εμπιστευμένου ταχυδρόμου ως προς το διαβατήριό που προσκομίζει ο εμπιστευμένος ταχυδρόμος·
- γ) εξακρίβωση της ισχύος του διαβατηρίου που προσκομίζει ο εμπιστευμένος ταχυδρόμος·
- δ) εξακρίβωση του επικυρωμένου διαβατηρίου που προσκομίζει ο εμπιστευμένος ταχυδρόμος ως προς το αντίγραφο του ισχύοντος διαβατηρίου του εμπιστευμένου ταχυδρόμου υπογεγραμμένο από ένα από τα ταυτοποιημένα σημεία επαφής του φορέα. Το γνήσιο της υπογραφής ελέγχεται ως προς το πρωτότυπο «έντυπο ταυτοποίησης του εμπιστευμένου ταχυδρόμου και των σημείων επαφής»·
- ε) έλεγχο του συμπληρωμένου και υπογεγραμμένου πληρεξούσιου·
- στ) έλεγχο του εντύπου αίτησης πιστοποιητικού και της υπογραφής του ως προς το πρωτότυπο «έντυπο ταυτοποίησης του εμπιστευμένου ταχυδρόμου και των σημείων επαφής»·
- ζ) με κλήση του υπογράφοντος σημείου επαφής για να ελέγξει εκ νέου την ταυτότητα του εμπιστευμένου ταχυδρόμου και το περιεχόμενο της αίτησης πιστοποιητικού.

2.2.4.4. Η αρχή καταχώρισης επιβεβαιώνει στην ομάδα υποστήριξης CEF ότι η εθνική αρχή εξουσιοδοτείται όντως να λειτουργεί τα στοιχεία για τα οποία αιτείται τα πιστοποιητικά και ότι η σχετική καταχώριση αυτοπροσώπως ήταν επιτυχής. Η επιβεβαίωση αποστέλλεται με ασφαλές ηλεκτρονικό ταχυδρομείο του πιστοποιητικού «CommiSign», στο οποίο επισυνάπτεται σαρωμένο αντίγραφο του πακέτου τεκμηρίωσης που ελέγχθηκε αυτοπροσώπως ως προς τη γνησιότητά του και του υπογεγραμμένου καταλόγου ελέγχου της διαδικασίας που ακολούθησε η αρχή καταχώρισης.

2.2.4.5. Εάν η αρχή καταχώρισης επιβεβαιώσει την εγκυρότητα της αίτησης, η διαδικασία συνεχίζεται κατά τα 2.2.4.6 και 2.2.4.7. Ειδάλλως, απορρίπτεται η έκδοση του πιστοποιητικού και ενημερώνεται ο φορέας.

2.2.4.6. Η ομάδα υποστήριξης CEF εγκρίνει την αίτηση πιστοποιητικού και κοινοποιεί στην αρχή καταχώρισης την έγκριση του πιστοποιητικού.

2.2.4.7. Η αρχή καταχώρισης κοινοποιεί στον φορέα ότι το πιστοποιητικό μπορεί να ανακτηθεί μέσω της διαδικτυακής πύλης χρήστη.



Σχήμα 8 - Έγκριση του πιστοποιητικού

2.2.5. 4η ενέργεια: Δημιουργία του πιστοποιητικού

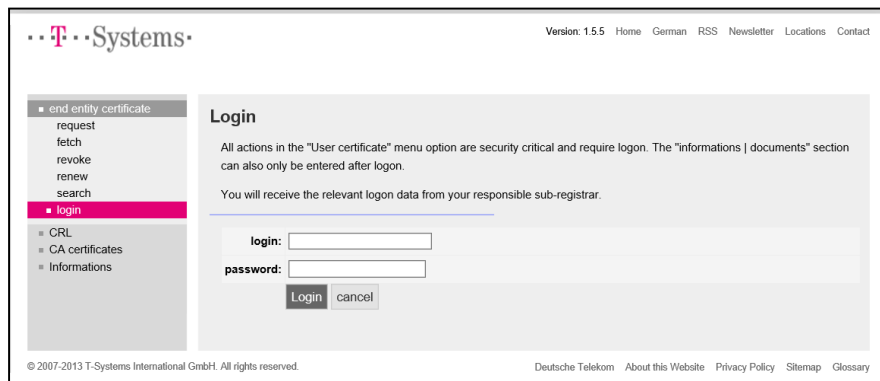
Μετά την έγκριση της αίτησης πιστοποιητικού, το πιστοποιητικό δημιουργείται.

2.2.6. 5η ενέργεια: Δημοσίευση και ανάκτηση του πιστοποιητικού

2.2.6.1. Μετά την έγκριση της αίτησης πιστοποιητικού, η αρχή καταχώρισης ανακτά το πιστοποιητικό και παραδίδει αντίγραφο του στον εμπιστευμένο ταχυδρόμο.

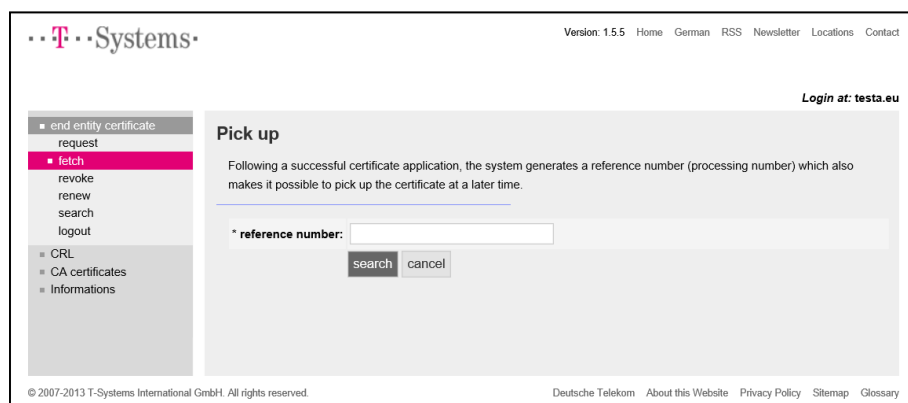
2.2.6.2. Ο φορέας λαμβάνει κοινοποίηση από την αρχή καταχώρισης ότι το πιστοποιητικό μπορεί να ανακτηθεί.

2.2.6.3. Ο φορέας περιηγείται στη διαδικτυακή πύλη χρήστη <https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en> και εισέρχεται με την ταυτότητα χρήστη «sbca/CEF_eDelivery.europa.eu» και τον κλειδάριθμο «digit.333».



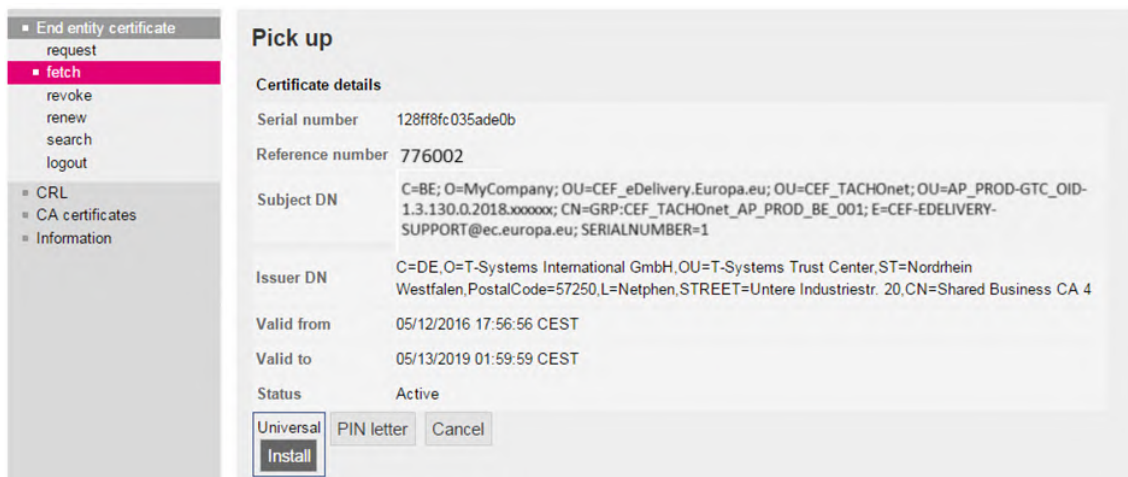
Σχήμα 9

2.2.6.4. Ο φορέας κάνει κλικ στο κουμπί «fetch» (λήψη) στην αριστερή πλευρά και δίνει τον αριθμό αναφοράς που καταγράφηκε κατά τη διαδικασία αίτησης του πιστοποιητικού.



Σχήμα 10

2.2.6.5. Ο φορέας εγκαθιστά τα πιστοποιητικά πατώντας το κουμπί εγκατάστασης.

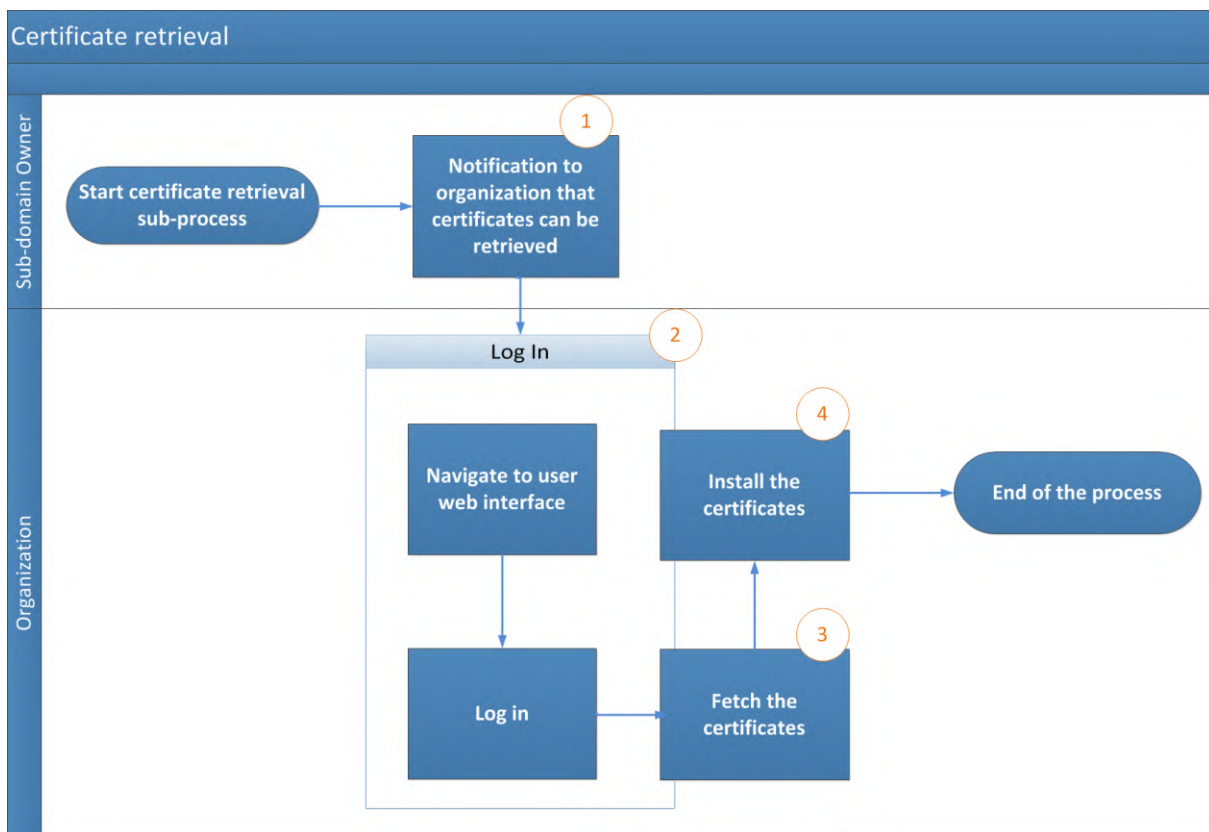


Σχήμα 11

2.2.6.6. Το πιστοποιητικό εγκαθίσταται στο σημείο πρόσβασης. Επειδή αυτό σχετίζεται ειδικά με την υλοποίηση, ο φορέας αποτελείται στον πάροχο του οικείου σημείου πρόσβασης για να λάβει την περιγραφή της διαδικασίας αυτής.

2.2.6.7. Για την εγκατάσταση του πιστοποιητικού στο σημείο πρόσβασης απαιτούνται οι εξής ενέργειες:

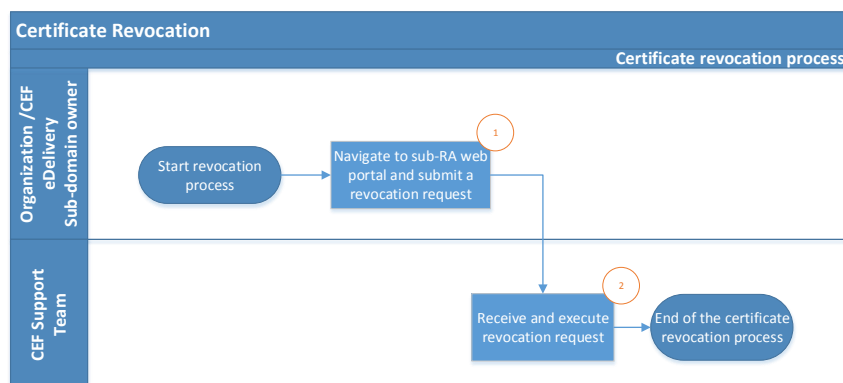
- α) εξαγωγή του ιδιωτικού κλειδιού και του πιστοποιητικού,
- β) δημιουργία χώρου αποθήκευσης κλειδιών και χώρου εμπιστευμένης αποθήκευσης,
- γ) εγκατάσταση του χώρου αποθήκευσης κλειδιών και του χώρου εμπιστευμένης αποθήκευσης στο σημείο πρόσβασης.



Σχήμα 12 - Ανάκτηση του πιστοποιητικού

3. Διαδικασία ανάκλησης πιστοποιητικού

- 3.1. Ο φορέας υποβάλλει αίτηση ανάκλησης πιστοποιητικού μέσω της διαδικτυακής πύλης χρήστη.
- 3.2. Η ομάδα υποστήριξης CEF εκτελεί την ανάκληση του πιστοποιητικού.



Σχήμα 13 - Ανάκληση του πιστοποιητικού

4. Γενικοί όροι και προϋποθέσεις της υπηρεσίας CEF PKI

4.1. Πλαίσιο

Η ΓΔ DIGIT, υπό την ιδιότητα παρόχου λύσεων του δομικού τμήματος της υπηρεσίας eDelivery του μηχανισμού «Συνδέοντας την Ευρώπη» (CEF), διαθέτει υπηρεσία PKI⁷ («υπηρεσία CEF PKI») στα συμβαλλόμενα μέρη της AETR. Η υπηρεσία CEF PKI χρησιμοποιείται από τις εθνικές αρχές («τελικοί χρήστες») που συμμετέχουν στο TACHOnet.

Η ΓΔ DIGIT είναι μισθωτής υποδομής δημόσιου κλειδιού (PKI) της λύσης TeleSec Shared-Business-CA («SBCA») που λειτουργεί στο Trust Center της μονάδας ομάδας T-Systems International GmbH («T-Systems»⁸). Η ΓΔ DIGIT έχει την ιδιότητα του Ανώτατου Γραμματέα του τομέα της SBCA «CEF_eDelivery.europa.eu». Υπό αυτή την ιδιότητα, η ΓΔ DIGIT δημιουργεί υποτομείς εντός του τομέα «CEF_eDelivery.europa.eu» για κάθε έργο στο οποίο χρησιμοποιείται η υπηρεσία CEF PKI.

Το έγγραφο αυτό περιέχει λεπτομέρειες για τους όρους και τις προϋποθέσεις του υποτομέα TACHOnet. Η ΓΔ DIGIT έχει την ιδιότητα του αναπληρωτή Γραμματέα του υποτομέα αυτού. Υπό την ιδιότητα αυτή, εκδίδει, ανακαλεί και ανανεώνει τα πιστοποιητικά του έργου αυτού.

4.2. Αποποίηση ευθύνης

Η Ευρωπαϊκή Επιτροπή δεν αναλαμβάνει καμία ευθύνη για το περιεχόμενο του πιστοποιητικού, την πλήρη ευθύνη του οποίου έχει ο κάτοχός του. Ο κάτοχος του πιστοποιητικού έχει την ευθύνη να ελέγχει την ακρίβεια του περιεχομένου του πιστοποιητικού.

Η Ευρωπαϊκή Επιτροπή δεν αναλαμβάνει καμία ευθύνη για τη χρήση του πιστοποιητικού από τον κάτοχό του, διότι ο κάτοχος είναι τρίτη νομική οντότητα εκτός της Ευρωπαϊκής Επιτροπής.

⁷ PKI (Public Key Infrastructure/υποδομή δημόσιου κλειδιού) είναι ένα σύνολο ρόλων, πολιτικών, διαδικασιών και συστημάτων αναγκαίων για τη δημιουργία, τη διαχείριση, τη διανομή και την ανάκληση ψηφιακών πιστοποιητικών.

⁸ Ο χειριστής του κέντρου εμπιστευσης, υπό την εμπιστευμένη ιδιότητά του, ο οποίος βρίσκεται στο κέντρο εμπιστευσης των T-Systems, ενεργεί επίσης ως εσωτερική αρχή καταχώρισης.

Η παρούσα αποποίηση ευθύνης δεν αποβλέπει σε περιορισμό της ευθύνης της Επιτροπής κατά παραβίαση τυχόν απαιτήσεων που έχουν καθορισθεί σε εφαρμοστέο εθνικό δίκαιο, ή σε απαλλαγή της ευθύνης της σε θέματα τα οποία δεν είναι δυνατόν να εξαιρεθούν δυνάμει του εν λόγω δικαίου.

4.3. Εξουσιοδοτημένες / απαγορευμένες χρήσεις των πιστοποιητικών

4.3.1. Επιτρεπόμενη χρήση των πιστοποιητικών

Μόλις εκδοθεί το πιστοποιητικό, ο κάτοχος του πιστοποιητικού⁹ το χρησιμοποιεί μόνον στο TACHOnet. Στο πλαίσιο αυτό, το πιστοποιητικό είναι δυνατό να χρησιμοποιείται για:

- τον έλεγχο αυθεντικότητας της προέλευσης του μηνύματος·
- την κρυπτογράφηση δεδομένων·
- τον εντοπισμό παραβίασης της ακεραιότητας δεδομένων.

4.3.2. Απαγορευμένη χρήση των πιστοποιητικών

Απαγορεύεται οποιαδήποτε μη ρητά εξουσιοδοτημένη χρήση από τις επιτρεπόμενες χρήσεις του πιστοποιητικού.

4.4. Πρόσθετες υποχρεώσεις του κατόχου του πιστοποιητικού

Οι λεπτομερείς όροι και προϋποθέσεις της SBCA καθορίζονται από την T-Systems στην πολιτική πιστοποίησης (CP)/δήλωση πρακτικών πιστοποίησης (CPS) της υπηρεσίας SBCA¹⁰. Το εν λόγω έγγραφο περιέχει τις προδιαγραφές ασφάλειας και κατευθύνσεις για τις τεχνικές και οργανωτικές πτυχές και περιγράφει τις δραστηριότητες του χειριστή του κέντρου εμπιστευσης στους ρόλους της αρχής πιστοποίησης και της αρχής καταχώρισης, καθώς και εκπροσώπου τρίτου μέρους.

Μπορούν να αιτηθούν πιστοποιητικό μόνον οι οντότητες που εξουσιοδοτούνται να συμμετέχουν στο TACHOnet.

⁹ την ταυτοποιημένη με την τιμή χαρακτηριστικού «O=» στο αποκλειστικό όνομα υποκειμένου του εκδοθέντος πιστοποιητικού

¹⁰ Η τελευταία έκδοση των CP/CPS της SBCA της T-Systems διατίθεται στη διεύθυνση <https://www.telesec.de/en/sbca-en/support/download-area/>.

Όσον αφορά την αποδοχή του πιστοποιητικού, ισχύει η ρήτρα 4.4.1 της πολιτικής πιστοποίησης και της δήλωσης πρακτικών πιστοποίησης («CP/CPS») της SBCA, επιπλέον δε οι όροι χρήσης και οι διατάξεις που περιγράφονται στο παρόν έγγραφο θεωρούνται αποδεκτοί από τον φορέα στον οποίο εκδίδεται («Ο=») το πιστοποιητικό όταν χρησιμοποιείται για πρώτη φορά.

Όσον αφορά τη δημοσίευση του πιστοποιητικού, ισχύει η ρήτρα 2.2 της CP/CPS της SBCA.

Όλοι οι κάτοχοι πιστοποιητικών συμμορφώνονται με τις κάτωθι απαιτήσεις:

- (1) προστατεύουν τα οικεία ιδιωτικά κλειδιά από μη εξουσιοδοτημένη χρήση τους·
- (2) δεν μεταβιβάζουν, ούτε αποκαλύπτουν τα οικεία ιδιωτικά κλειδιά σε τρίτα μέρη, ακόμη και εάν πρόκειται για εκπροσώπους·
- (3) δεν συνεχίζουν τη χρήση των ιδιωτικών κλειδιών μετά τη λήξη ισχύος τους ή την ανάκληση του πιστοποιητικού, εξαιρουμένης της προβολής κρυπτογραφημένων δεδομένων (π.χ. για την αποκρυπτογράφηση ηλεκτρονικών μηνυμάτων).
- (4) ο κάτοχος πιστοποιητικού είναι υπεύθυνος για την αντιγραφή ή τη διαβίβαση του κλειδιού στην τελική αποδέκτρια οντότητα ή οντότητες·
- (5) ο κάτοχος πιστοποιητικού οφείλει να υποχρεώσει την τελική αποδέκτρια οντότητα/όλες τις τελικές αποδέκτριες οντότητες να συμμορφώνεται/συμμορφώνονται με τους παρόντες όρους και προϋποθέσεις, μεταξύ των οποίων είναι η CP/CPS της SBCA, όταν χειρίζονται το ιδιωτικό κλειδί·
- (6) ο κάτοχος πιστοποιητικού οφείλει να παρέχει την ταυτοποίηση των εξουσιοδοτημένων εκπροσώπων στους οποίους επιτρέπεται να ζητήσουν ανάκληση των πιστοποιητικών που έχουν εκδοθεί για τον φορέα με τα στοιχεία που οδήγησαν στην ανάκληση, και τον κλειδάριθμο ανάκλησης·
- (7) για τα πιστοποιητικά που σχετίζονται με ομάδες προσώπων και λειτουργιών και/ή νομικά πρόσωπα, μετά την αποχώρηση προσώπου από την ομάδα των τελικών αποδεκτριών οντοτήτων (π.χ. λήξη σχέσης απασχόλησης), ο κάτοχος του πιστοποιητικού οφείλει να προλαμβάνει την κατάχρηση του ιδιωτικού κλειδιού με ανάκληση του πιστοποιητικού·
- (8) ο κάτοχος πιστοποιητικού είναι υπεύθυνος και αιτείται ανάκληση του πιστοποιητικού υπό τις συνθήκες που αναφέρονται στη ρήτρα 4.9.1 της CP/CPS της SBCA.

Όσον αφορά την ανανέωση ή την αλλαγή κλειδιού πιστοποιητικού, ισχύει η ρήτρα 4.6 ή 4.7 της CP/CPS της SBCA.

Όσον αφορά την τροποποίηση πιστοποιητικού, ισχύει η ρήτρα 4.8 της CP/CPS της SBCA.

Όσον αφορά την ανάκληση πιστοποιητικού, ισχύει η ρήτρα 4.9 της CP/CPS της SBCA.

5. Έντυπο ταυτοποίησης των προσώπων επικοινωνίας και των εμπιστευμένων ταχυδρόμων (δείγμα)

Ο κάτωθι υπογεγραμμένος, [ονοματεπώνυμο και διεύθυνση του εκπροσώπου του οργανισμού], βεβαιώνω ότι οι κάτωθι πληροφορίες πρόκειται να χρησιμοποιηθούν για την αίτηση, τη δημιουργία και την ανάκτηση ψηφιακών πιστοποιητικών δημόσιου κλειδιού για τα σημεία πρόσβασης στο TACHOnet που υποστηρίζουν την εμπιστευτικότητα, την ακεραιότητα και τη μη αποκήρυξη των μηνυμάτων TACHOnet:

Στοιχεία προσώπου επικοινωνίας:

– Πρόσωπο επικοινωνίας #1	– Πρόσωπο επικοινωνίας #2
– Επώνυμο:	– Επώνυμο:
– Ονόματα:	– Ονόματα:
– Κινητό τηλέφωνο:	– Κινητό τηλέφωνο:
– Σταθερό τηλέφωνο:	– Σταθερό τηλέφωνο:
– Ηλεκτρονικό ταχυδρομείο:	– Ηλεκτρονικό ταχυδρομείο:
– Δείγμα ιδιόχειρης υπογραφής:	– Δείγμα ιδιόχειρης υπογραφής:
–	–
	–
	–

Στοιχεία του εμπιστευμένου ταχυδρόμου:

– Εμπιστευμένος ταχυδρόμος #1	– Εμπιστευμένος ταχυδρόμος #2
– Επώνυμο:	– Επώνυμο:
– Ονόματα:	– Ονόματα:
– Κινητό τηλέφωνο:	– Κινητό τηλέφωνο:
– Ηλεκτρονικό ταχυδρομείο:	– Ηλεκτρονικό ταχυδρομείο:
– Χώρα έκδοσης του διαβατηρίου:	– Χώρα έκδοσης του διαβατηρίου:
– Αριθμός του διαβατηρίου:	– Αριθμός του διαβατηρίου:
– Ημερομηνία λήξης της ισχύος του διαβατηρίου:	– Ημερομηνία λήξης της ισχύος του διαβατηρίου:

Τόπος, ημερομηνία και σφραγίδα της επιχείρησης:

Υπογραφή του εξουσιοδοτημένου εκπροσώπου:

6. Έγγραφο

6.1. Ατομικό πληρεξούσιο (δείγμα)

Δείγμα του ατομικού πληρεξούσιου που πρέπει να υπογραφεί και να προσκομισθεί από τον εμπιστευμένο ταχυδρόμο κατά την αυτοπροσώπως καταχώριση στην αρχή καταχώρισης διατίθεται στη διεύθυνση:

Please print the text of this document on your letterhead, add your company stamp and have it signed by the administrative contact or admin-c of the domain.

The power of attorney must be signed by an authorized representative of the organization (principal).

The Shared-Business-CA customer will then submit this document together with the order document to the T-Systems International GmbH Trust Center.

Individual power of attorney / Power of attorney granted to one person

I, *[name and address of the end-user]*, empower as an authorized person of this organization *

[name of the company receiving the certificate]

(e. g. sample company, sample authority, to be registered in the O-field of the certificate *)

following company and/or person:

Company: **European Commission**

Address: **DG DIGIT, 28 rue Belliard, 1000 Brussels**

Represented by Mr/Mrs/Ms: **Adrien FERIAI**

On my behalf, by complying with all and any regulations and formalities (particularly Certificate Policy (CP) / Certification Practice Statement (CPS)), for authorisation to manage (i.e. issue, revoke, renew) X.509v3-certificates, including the complete key-material, issued by the certification authority „TeleSec Shared-Business-CA“, in respect of the domain as above mentioned.

This power of attorney relates to issuing and management of the following certificate types (the applicable type has to be marked):

☒ user¹: e.g. mail security (signature, encryption), virtual private network (VPN), TLS/SSL client

☐ server²: e.g. identity of web server, TLS/SSL client server authentication

Please enter additionally the country, organization, locality, state or province name of the server:

☐ eMail-Gateway³: e.g. identity of eMail gateways / eMail-Appliance, virtual mail-administrating centre.

Validity

☒ The power of attorney is valid until further notice, but up to a **maximum of 27 months²** or **maximum of 36 months^{1,3}** from date of issuance.

☐ The power of attorney is valid until _____ (mm.dd.yyyy), but up to a **maximum of 27 month²** months or **maximum of 36 months^{1,3}** from date of issuance.

Please note that a time limit on the power of attorney can cause that a request for certificate order, renewal or revocation may not be possible because the validity period of the authorization has been exceeded!

Place, date, company stamp or seal of the organisation (principal)

Signature of the authorized representative

6.2. Έντυπο αίτησης πιστοποιητικού (δείγμα)

Δείγμα του εντύπου αίτησης πιστοποιητικού που πρέπει να υπογραφεί και να προσκομισθεί από τον εμπιστευμένο ταχυδρόμο κατά την αυτοπροσώπως καταχώριση στην αρχή καταχώρισης διατίθεται στη διεύθυνση:

7. Γλωσσάριο

Οι βασικοί όροι που χρησιμοποιούνται στο παρόν υποπροσάρτημα περιλαμβάνονται στο τμήμα των ορισμών του CEF στην ενιαία διαδικτυακή πύλη CEF Digital:

<https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Definitions>

Τα βασικά ακρωνύμια που χρησιμοποιούνται στην παρούσα περιγραφή στοιχείων περιλαμβάνονται στο τμήμα των ορισμών του CEF στην ενιαία διαδικτυακή πύλη CEF Digital:

<https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?spaceKey=CEFDIGITAL&title=CEF+Glossary>
