Consiglio dell'Unione europea

Bruxelles, 5 novembre 2018
(OR. en)

13711/18
ADD 1

Fascicolo interistituzionale: 2018/0339(NLE)

TRANS 488

NOTA

Origine:	Segretariato generale del Consiglio
Destinatario:	delegazioni
n. doc. prec.:	ST 13711/18 TRANS 448
n. doc. Comm.:	ST 12727/18 TRANS 426 + ADD 1
Oggetto:	Decisione del Consiglio relativa alla posizione da adottare a nome dell'Unione europea in sede di gruppo di esperti sull'accordo europeo relativo alle prestazioni lavorative degli equipaggi dei veicoli addetti ai trasporti internazionali su strada della Commissione economica per l'Europa delle Nazioni Unite

Allegato della decisione del Consiglio in oggetto.

ALLEGATO

Nuova appendice dell'AETR

Appendice 4

Specifiche di TACHOnet

1. Ambito di applicazione e finalità

1.1. La presente appendice stabilisce i termini e le condizioni riguardanti la connessione delle parti contraenti dell'AETR a TACHOnet mediante eDelivery.

1.2. Le parti contraenti che si connettono a TACHOnet mediante eDelivery devono attenersi alle disposizioni stabilite nella presente appendice.

2. Definizioni

a) "Parte contraente" o "parte": qualsiasi parte contraente dell'AETR;

b) "eDelivery": il servizio messo a punto dalla Commissione europea che permette di trasmettere dati fra terzi per via elettronica, di fornire prove relative alla gestione dei dati trasmessi, tra cui la prova di spedizione e di ricevimento dei dati, e di proteggere i dati trasmessi contro il rischio di alterazione non autorizzata;

c) "TACHOnet": il sistema per lo scambio elettronico di informazioni sulle carte del conducente tra le parti contraenti, di cui all'articolo 31, paragrafo 2, del regolamento (UE) n. 165/2014;

d) "sistema centrale": il sistema di informazione che consente l'inoltro (routing) dei messaggi TACHOnet tra le parti richiedenti e destinatarie;

e) "parte richiedente": la parte contraente che emette una richiesta o una notifica TACHOnet inoltrata poi alla parte destinataria interessata dal sistema centrale;

f) "parte destinataria": la parte contraente cui è indirizzata la richiesta o la notifica TACHOnet;

g) "autorità di rilascio della carta" o "CIA": l'organismo abilitato da una parte contraente al rilascio e alla gestione delle carte tachigrafiche.

3. Responsabilità generali

3.1. Nessuna parte contraente può concludere accordi di accesso a TACHOnet a nome di un'altra parte o rappresentare in qualsiasi altro modo l'altra parte contraente sulla base della presente appendice. Nessuna parte contraente agisce in veste di subappaltatore dell'altra parte contraente nelle operazioni di cui alla presente appendice.

3.2. Le parti contraenti consentono l'accesso al proprio registro nazionale delle carte del conducente tramite TACHOnet, secondo le modalità e il livello di servizio definiti nella sottoappendice 4.6.

3.3. Qualora, nell'ambito delle proprie responsabilità, osservino disturbi o errori che possono compromettere il normale funzionamento di TACHOnet, le parti contraenti informano senza indugio le altre parti.

3.4. Ogni parte designa le persone da contattare per TACHOnet e ne informa il segretariato dell'AETR. Ogni modifica dei punti di contatto deve essere comunicata per iscritto al segretariato dell'AETR.

4. Prove di connessione a TACHOnet

4.1. La connessione di una parte contraente a TACHOnet ha luogo dopo il superamento delle prove di connessione, integrazione ed efficienza in conformità alle istruzioni della Commissione europea e sotto la sua supervisione.

4.2. Se le prove preliminari hanno esito negativo, la Commissione europea può sospendere temporaneamente la fase di prova. Le prove riprendono non appena la parte contraente abbia informato la Commissione europea che sono stati apportati i miglioramenti tecnici necessari a livello nazionale per il superamento delle prove preliminari.

4.3. Le prove preliminari hanno durata massima di sei mesi.

5. Architettura di sicurezza

5.1. La riservatezza, l'integrità e la non disconoscibilità dei messaggi TACHOnet sono garantite dall'architettura di sicurezza (trust architecture) di TACHOnet.

5.2. L'architettura di sicurezza di TACHOnet si basa su un servizio di infrastruttura a chiave pubblica (PKI) istituito dalla Commissione europea, i cui requisiti sono stabiliti nelle sottoappendici 4.8 e 4.9.

5.3. I seguenti organismi interagiscono con l'architettura di sicurezza di TACHOnet:

a) l'autorità di certificazione, cui incombe il compito di generare i certificati digitali che l'autorità di registrazione consegnerà alle autorità nazionali delle parti contraenti (tramite corrieri fiduciari da esse designati) e di predisporre l'infrastruttura tecnica riguardante il rilascio, la revoca e il rinnovo dei certificati digitali;

b) il titolare del dominio, responsabile del funzionamento del sistema centrale di cui alla sottoappendice 4.1, nonché dell'omologazione e del coordinamento dell'architettura di sicurezza di TACHOnet;

c) l'autorità di registrazione, cui incombe il compito di registrare e approvare le richieste di rilascio, revoca e rinnovo dei certificati digitali e di verificare l'identità dei corrieri fiduciari;

d) il corriere fiduciario, la persona nominata dalle autorità nazionali cui incombe il compito di consegnare la chiave pubblica all'autorità di registrazione e di ottenere il corrispondente certificato generato dall'autorità di certificazione;

e) l'autorità nazionale della parte contraente, la quale:

i) genera le chiavi private e le corrispondenti chiavi pubbliche da inserire nei certificati generati dall'autorità di certificazione;

ii) richiede i certificati digitali all'autorità di certificazione;

iii) nomina il corriere fiduciario.

5.4. L'autorità di certificazione e l'autorità di registrazione sono nominate dalla Commissione europea.

5.5. Qualsiasi parte contraente che si connette a TACHOnet deve richiedere il rilascio di un certificato digitale in conformità alla sottoappendice 4.9 al fine di firmare e criptare un messaggio TACHOnet.

5.6. Un certificato può essere revocato conformemente alla sottoappendice 4.9.

6. Protezione e riservatezza dei dati

6.1. In osservanza della normativa in materia di protezione dei dati a livello internazionale e nazionale, in particolare della convenzione sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale, le parti adottano tutte le misure tecniche e organizzative necessarie per garantire la sicurezza dei dati TACHOnet e prevenire l'alterazione, la perdita o il trattamento non autorizzato di tali dati o l'accesso non autorizzato agli stessi (in particolare l'autenticità, la riservatezza, la tracciabilità, l'integrità, la disponibilità e la non disconoscibilità dei dati e la sicurezza dei messaggi).

6.2. Ogni parte protegge il proprio sistema nazionale contro l'uso illecito, i codici maligni, i virus, le intrusioni nei computer, le violazioni e le alterazioni illecite dei dati e altri comportamenti analoghi da parte di terzi. Le parti accettano di compiere sforzi ragionevoli sul piano commerciale per evitare la trasmissione di qualsiasi virus, bomba a tempo, worm informatico o materiale analogo o di qualsiasi routine di programmazione che possa interferire con i sistemi informatici di altre parti.

7. Costi

7.1. Le parti contraenti sostengono i costi di sviluppo e di esercizio associati ai propri sistemi e procedure relativi ai dati nella misura necessaria per adempiere agli obblighi conformemente alla presente appendice.

7.2. I servizi di cui alla sottoappendice 4.1, forniti dal sistema centrale, sono gratuiti.

8. Subappalto

8.1. Le parti possono subappaltare qualsiasi servizio di cui sono responsabili a norma della presente appendice.

8.2. Il subappalto non dispensa la parte dalle responsabilità derivanti dalla presente appendice, compresa la responsabilità di garantire il livello adeguato di servizio conformemente alla sottoappendice 4.6.

Sottoappendice 4.1

Aspetti generali di TACHOnet

1. Descrizione generale

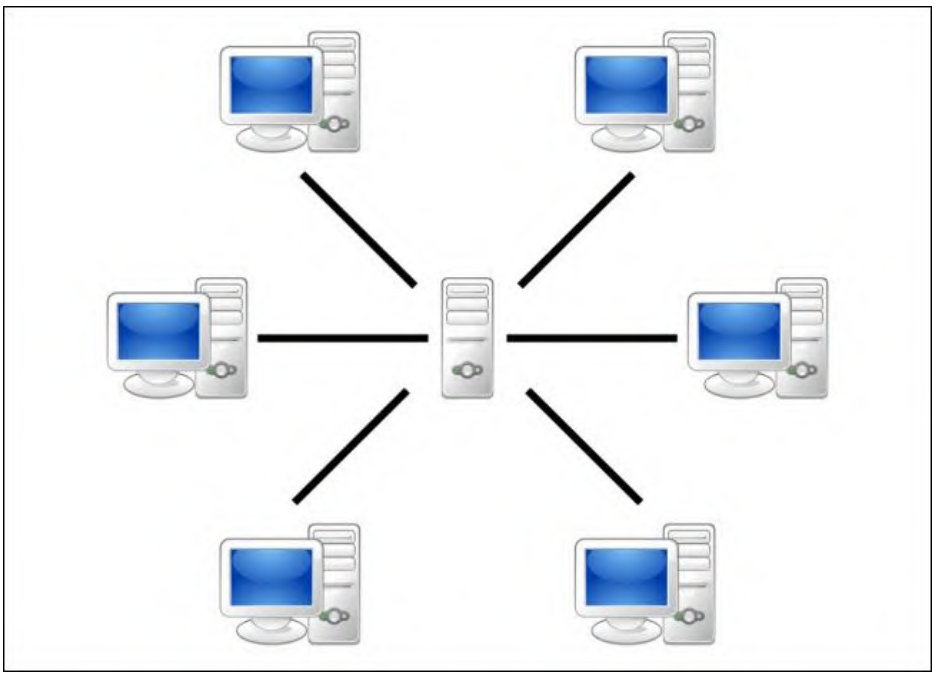
TACHOnet è un sistema elettronico per lo scambio di informazioni sulle carte del conducente tra le parti contraenti dell'AETR. TACHOnet inoltra le richieste di informazioni delle parti richiedenti alle parti destinatarie e le risposte di queste ultime alle prime. Le parti contraenti che partecipano a TACHOnet devono collegare al sistema i rispettivi registri nazionali sulle carte del conducente.

2. Architettura

Il sistema di messaggistica TACHOnet si articola nei seguenti elementi:

2.1. Un sistema centrale in grado di ricevere una richiesta dalla parte richiedente, di convalidarla, di elaborarla e di trasmetterla alle parti destinatarie. Il sistema centrale attende la risposta delle varie parti destinatarie, consolida tutte le risposte e trasmette la risposta consolidata alla parte richiedente.

2.2. I sistemi nazionali delle parti, che devono dotarsi di un'interfaccia in grado sia di inviare richieste al sistema centrale sia di ricevere le relative risposte. Per inviare e ricevere messaggi dal sistema centrale, i sistemi nazionali possono usare un proprio software o acquistarne uno.



3. Gestione

3.1. Il sistema centrale è gestito dalla Commissione europea, che ne garantisce il funzionamento tecnico e la manutenzione.

3.2. Il sistema centrale conserva per un periodo massimo di sei mesi i dati diversi da quelli di accesso e statistici di cui alla sottoappendice 4.7.

3.3. Il sistema centrale non consente l'accesso a dati personali, fatta eccezione per il personale autorizzato della Commissione europea qualora ciò sia necessario per controlli, manutenzione e risoluzione di problemi.

3.4. Spetta alle parti contraenti:

3.4.1. configurare e gestire i rispettivi sistemi nazionali, compresa l'interfaccia con il sistema centrale;

3.4.2. installare e mantenere in funzione l'hardware e il software del proprio sistema nazionale, sia che l'abbiano acquistato o che ne siano i proprietari;

3.4.3. garantire la corretta interoperabilità tra il proprio sistema nazionale e il sistema centrale nonché la gestione dei messaggi d'errore ricevuti dal sistema centrale;

3.4.4. adottare tutte le misure per garantire la riservatezza, l'integrità e la disponibilità delle informazioni;

3.4.5. garantire il funzionamento dei sistemi nazionali in conformità ai livelli di servizio di cui alla sottoappendice 4.6.

Sottoappendice 4.2

Funzioni di TACHOnet

1. Il sistema di messaggistica TACHOnet deve assolvere le seguenti funzioni:

1.1. Verifica delle carte rilasciate (Check Issued Cards — CIC): mediante una richiesta di verifica delle carte rilasciate, inviata a una o a tutte le parti destinatarie, la parte richiedente può stabilire se chi ha chiesto una carta del conducente ne possiede già una rilasciatagli da una parte destinataria. Le parti destinatarie rispondono alla richiesta inviando una risposta di verifica delle carte rilasciate.

1.2. Verifica dello stato della carta (Check Card Status — CCS): mediante una richiesta di verifica dello stato della carta, una parte richiedente chiede a una parte destinataria informazioni su una carta rilasciata da quest'ultima. La parte destinataria risponde alla richiesta inviando una risposta di verifica dello stato della carta.

1.3. Modifica dello stato della carta (Modify Card Status — MCS): mediante una richiesta di modifica dello stato della carta, una parte richiedente notifica a una parte destinataria il cambiamento dello stato di una carta rilasciata da quest'ultima. La parte destinataria risponde alla richiesta inviando un riconoscimento di modifica dello stato della carta.

1.4. Rilascio della carta del conducente sulla base della patente di guida (Issued Card Driving License — ICDL): mediante una richiesta di rilascio della carta del conducente sulla base della patente di guida, una parte richiedente notifica a una parte destinataria di aver rilasciato una carta del conducente in base alla patente di guida rilasciata da quest'ultima. La parte destinataria risponde alla richiesta inviando una risposta di rilascio della carta del conducente sulla base della patente di guida.

2. Si devono inserire altri tipi di messaggi per rendere più efficiente il funzionamento di TACHOnet: per esempio, le notifiche di errori.

3. Quando i sistemi nazionali usano una delle funzioni descritte al punto 1, devono accettare gli stati delle carte elencati nella tabella 1. Le parti non sono tuttavia tenute a mettere in atto una procedura amministrativa che utilizzi tutti gli stati elencati.

4. Se una parte riceve una risposta o una notifica in cui è citato uno stato non utilizzato nelle proprie procedure amministrative, il sistema nazionale traduce nella propria procedura lo stato usato nel messaggio ricevuto con un'adeguata espressione corrispondente. La parte destinataria non può rifiutare il messaggio, se lo stato usato nel messaggio è elencato nella tabella 1.

5. Gli stati della carta elencati nella tabella 1 non vanno usati per stabilire se una carta del conducente è valida per la guida. Se una parte vuole consultare mediante la funzione CCS il registro dell'autorità nazionale che rilascia la carta, la risposta deve contenere il campo apposito "valida per la guida". Le procedure amministrative nazionali devono far sì che le risposte CCS contengano sempre un'adeguata espressione corrispondente a "valida per la guida".

Tabella 1

Stati della carta

Stato della carta	**Definizione**
Domanda	L'autorità di rilascio della carta (Card issuing authority — CIA) ha ricevuto una domanda per il rilascio di una carta del conducente. Questa informazione è stata registrata e memorizzata nella banca dati con le chiavi di ricerca generate.
Approvata	La CIA ha approvato la domanda per la carta tachigrafica.
Respinta	La CIA ha respinto la domanda.
Personalizzata	La carta tachigrafica è stata personalizzata.
Spedita	L'autorità nazionale ha spedito la carta del conducente al rispettivo conducente o all'agenzia di servizi interessata.
Consegnata	L'autorità nazionale ha consegnato la carta del conducente al rispettivo conducente.
Confiscata	L'autorità competente ha tolto al conducente la sua carta del conducente.
Sospesa	La carta del conducente è stata provvisoriamente tolta al conducente.
Ritirata	La CIA ha deciso di ritirare la carta del conducente. La carta è stata definitivamente annullata.
Restituita	La carta tachigrafica è stata restituita alla CIA e dichiarata non più necessaria.
Persa	È stato denunciato alla CIA lo smarrimento della carta tachigrafica.
Rubata	È stato denunciato alla CIA il furto della carta tachigrafica. Una carta rubata viene considerata persa.
Funzionamento difettoso	È stato denunciato alla CIA il cattivo funzionamento della carta tachigrafica.
Scaduta	Il periodo di validità della carta tachigrafica è scaduto.
Sostituita	La carta tachigrafica dichiarata smarrita, rubata o non funzionante è stata sostituita da una nuova carta. I dati della nuova carta sono gli stessi della vecchia, eccetto il numero del codice di sostituzione della carta che viene aumentato di un'unità.

Rinnovata	La carta tachigrafica è stata rinnovata perché i dati amministrativi sono cambiati o è terminato il periodo di validità. Il numero della nuova carta è lo stesso della vecchia, eccetto il numero del codice di sostituzione della carta che viene aumentato di un'unità.
In fase di sostituzione	Alla CIA che ha rilasciato una carta del conducente è pervenuta la notifica dell'avvio della procedura per sostituire tale carta con una carta del conducente rilasciata dalla CIA di un'altra parte.
Sostituita	Alla CIA che ha rilasciato una carta del conducente è pervenuta la notifica della conclusione della procedura per sostituire tale carta con una carta del conducente rilasciata dalla CIA di un'altra parte.

Sottoappendice 4.3

Requisiti del messaggio TACHOnet

1. Requisiti tecnici generali

1.1. Per lo scambio dei messaggi, il sistema centrale deve fornire sia l'interfaccia sincrono che quello asincrono. Le parti possono scegliere la tecnologia che preferiscono per interfacciare le proprie applicazioni.

1.2. Tutti i messaggi scambiati tra sistema centrale e sistemi nazionali devono essere codificati in UTF-8.

1.3. I sistemi nazionali devono essere in grado di ricevere ed elaborare messaggi contenenti caratteri greci o cirillici.

2. Struttura dei messaggi XML e definizione dello schema (XSD)

2.1. La struttura generale dei messaggi XML deve rispettare il formato definito dagli schemi XSD installati nel sistema centrale.

2.2. Il sistema centrale e i sistemi nazionali devono trasmettere e ricevere messaggi conformi allo schema XSD di messaggio.

2.3. I sistemi nazionali devono essere in grado di inviare, ricevere ed elaborare tutti i messaggi corrispondenti a ciascuna funzione di cui alla sottoappendice 4.2.

2.4. I messaggi XML devono comprendere almeno i requisiti minimi di cui alla tabella 2.

Tabella 2

Requisiti minimi per il contenuto dei messaggi XML

Intestazione comune		**Obbligatorio**
Version (versione)	La versione ufficiale delle specifiche XML è precisata attraverso il namespace definito nel messaggio XSD e nell'attributo versione dell'elemento "intestazione" di ogni messaggio XML. Il numero di versione ("n.m") andrà stabilito come valore fisso in ogni versione del file di definizione dello schema XML (XSD).	Sì
Test Identifier (identificatore di prova)	Id facoltativo per attività di prova. L'originatore della prova alimenta l'identificatore e tutti i partecipanti al flusso di lavoro rispondono con lo stesso identificatore o lo trasmettono. Durante la produzione deve essere ignorato e, anche se fornito, non va usato.	No
Technical Identifier (identificatore tecnico)	Un UUID che identifica in modo univoco ogni singolo messaggio. Il mittente genera un UUID e alimenta questo attributo. Questo dato non può essere utilizzato in alcuna transazione.	Sì
Workflow Identifier (identificatore del flusso di lavoro)	L'identificatore del flusso di lavoro è un UUID che deve essere generato dalla parte richiedente. Tale identificatore viene poi utilizzato in tutti i messaggi per correlare il flusso di lavoro.	Sì
Sent At (inviato il)	Data e ora (UTC) in cui il messaggio è stato inviato.	Sì
Timeout (tempo scaduto)	È l'indicazione, facoltativa, di una data e di un'ora (formato UTC). Questo valore è stabilito solo dal sistema centrale per le richieste trasmesse. Esso informa la parte destinataria del momento in cui scadrà la richiesta. Tale valore non è richiesto in MS2TCN_<x>_Req e in tutti i messaggi di risposta. È facoltativo; la stessa definizione d'intestazione può perciò essere usata per tutti i tipi di messaggio indipendentemente dal fatto che sia necessario un attributo per il valore di tempo scaduto.	No
From (mittente)	Il codice ISO 3166-1 Alpha 2 della parte che invia il messaggio o "EU".	Sì
To (destinatario)	Il codice ISO 3166-1 Alpha 2 della parte alla quale viene inviato il messaggio o "EU".	Sì

Sottoappendice 4.4

Traslitterazione e servizi NYSIIS (New York State Identification and Intelligence System)

1. Per codificare nel registro nazionale i nomi di tutti i conducenti si deve usare l'algoritmo NYSIIS implementato nel sistema centrale.

2. Quando si effettua la ricerca di una carta mediante la funzione CIC si usano le chiavi NYSIIS come principale meccanismo di ricerca.

3. Per ottenere ulteriori risultati le parti possono impiegare un algoritmo proprio.

4. I risultati della ricerca dovranno indicare il meccanismo di ricerca usato per trovare l'elemento registrato:

5. NYSIIS o proprio. Se una parte decide di registrare le notifiche ICDL, le chiavi NYSIIS contenute nella notifica vanno registrate come parte dei dati ICDL. Quando cerca i dati ICDL, la parte deve utilizzare le chiavi NYSIIS per il nome di chi ha presentato la domanda.

Sottoappendice 4.5

Requisiti di sicurezza

1. Per lo scambio di messaggi tra sistema centrale e sistemi nazionali si deve utilizzare il protocollo HTTPS.

2. Per garantire la sicurezza nella trasmissione dei messaggi tra il sistema nazionale e il sistema centrale, i sistemi nazionali devono utilizzare i certificati digitali di cui alle sottoappendici 4.8 e 4.9.

3. I sistemi nazionali devono implementare certificati che utilizzino almeno l'algoritmo hash della firma SHA-2 (SHA-256) e abbiano una chiave pubblica con una lunghezza di 2048 bit.

Sottoappendice 4.6

Livelli del servizio

1. I sistemi nazionali devono raggiungere i livelli minimi di servizio riportati di seguito.

1.1. Essi sono disponibili 24 ore al giorno, 7 giorni alla settimana.

1.2. La loro disponibilità è monitorata mediante messaggi heartbeat rilasciati dal sistema centrale.

1.3. Il loro tasso di disponibilità deve corrispondere al 98%, in conformità alla tabella che segue (cifre arrotondate all'unità conveniente più prossima):

Una disponibilità del	comporta una indisponibilità pari a		
	giornalmente	mensilmente	annualmente
98%	0,5 ore	15 ore	7,5 giorni

Si invitano le parti a rispettare il tasso di disponibilità giornaliera sebbene sia noto che talune attività necessarie, come la manutenzione del sistema, richiedano tempi superiori a 30 minuti. I tassi di disponibilità mensili e annuali rimangono comunque obbligatori.

1.4. I sistemi nazionali devono rispondere ad almeno il 98% delle richieste trasmesse loro in un mese di calendario.

1.5. Essi devono rispondere alle richieste entro 10 secondi.

1.6. Il timeout globale della richiesta (termine entro cui il richiedente può attendere la risposta) non deve superare 20 secondi.

1.7. I sistemi nazionali devono essere in grado di assorbire una frequenza di 6 messaggi al secondo.

1.8. Essi non possono inviare richieste al sistema centrale di TACHOnet con una frequenza superiore a 2 richieste al secondo.

1.9. Ogni sistema nazionale deve essere in grado di far fronte a potenziali problemi tecnici del sistema centrale o dei sistemi nazionali di altre parti. Tali problemi tecnici includono (l'elenco non è esaustivo):

a) l'interruzione del collegamento con il sistema centrale;

b) la mancata risposta a una richiesta;

c) il ricevimento di risposte dopo il message timeout;

d) il ricevimento di messaggi non richiesti;

e) il ricevimento di messaggi non validi.

2. Il sistema centrale deve:

2.1. garantire un tasso di disponibilità del 98%;

2.2. notificare ai sistemi nazionali eventuali errori mediante il messaggio di risposta o un apposito messaggio di errore. I sistemi nazionali devono a loro volta ricevere tali messaggi di errore dedicati e disporre di un flusso di lavoro di riassegnazione (escalation) capace di adottare i provvedimenti opportuni per rettificare l'errore notificato.

3. Manutenzione

Le parti devono informare le altre parti e la Commissione europea di ogni attività di manutenzione di routine tramite l'applicazione web almeno una settimana prima dell'inizio di tali attività, se tecnicamente possibile.

Sottoappendice 4.7

Registrazione di informazioni e statistiche dei dati raccolti presso il sistema centrale

1. Per garantire la riservatezza, i dati utilizzati a fini statistici devono essere anonimi. I dati che identifichino una carta, un conducente o una patente di guida non possono essere utilizzati a fini statistici.

2. Le informazioni registrate servono a documentare le operazioni eseguite, a scopo di monitoraggio e di risoluzione dei problemi, e consentono la generazione di statistiche su tali operazioni.

3. I dati personali non possono essere conservati nei registri per un periodo superiore a sei mesi. Le informazioni statistiche possono essere conservate a tempo indeterminato.

4. I dati statistici da utilizzare a fini di comunicazione comprendono:

   a) la parte richiedente;

   b) la parte destinataria;

   c) il tipo di messaggio;

   d) il codice dello stato della risposta;

   e) la data e l'ora dei messaggi;

   f) il tempo di risposta.

Sottoappendice 4.8

Disposizioni generali riguardanti le chiavi e i certificati digitali per TACHOnet

1. La direzione generale dell'Informatica della Commissione europea (DIGIT) mette a disposizione delle parti contraenti dell'AETR che si collegano a TACHOnet (in seguito denominate "le autorità nazionali") un servizio PKI[1] ("il servizio PKI dell'MCE") mediante eDelivery.

2. La procedura per la richiesta e la revoca dei certificati digitali, nonché i termini e le condizioni dettagliati per il suo impiego sono definiti nell'appendice.

3. Uso dei certificati:

3.1. Dopo il suo rilascio, il certificato è utilizzato dall'autorità nazionale[2] soltanto nel contesto di TACHOnet. Il certificato può essere utilizzato per:

a) autenticare l'origine dei dati;

b) criptare i dati;

c) assicurare il rilevamento di violazioni dell'integrità dei dati.

3.2. È vietato qualsiasi uso non espressamente autorizzato nell'ambito degli utilizzi permessi del certificato.

4. Le parti contraenti:

a) proteggono la propria chiave privata contro l'uso non autorizzato;

b) si astengono dal trasferire o rivelare a terzi, anche in qualità di rappresentanti, la propria chiave privata;

---

1 Per PKI (Public Key Infrastructure, infrastruttura a chiave pubblica) si intende l'insieme di ruoli, politiche, procedure e sistemi necessari per creare, gestire, distribuire e revocare i certificati digitali.

2 Identificata dal valore dell'attributo "O=" nel nome caratteristico del soggetto (Subject Distinguished Name) del certificato rilasciato.

c) garantiscono la riservatezza, l'integrità e la disponibilità delle chiavi private generate, memorizzate e utilizzate per TACHOnet;

d) si astengono dal continuare a utilizzare la chiave privata dopo la scadenza del periodo di validità o la revoca del certificato, salvo per visualizzare dati criptati (per es., decrittare messaggi di posta elettronica); le chiavi scadute vengono distrutte o conservate in modo da impedirne l'impiego;

e) forniscono all'autorità di registrazione l'identificazione dei mandatari autorizzati a richiedere la revoca dei certificati rilasciati all'organizzazione (le richieste di revoca comprendono una password della richiesta di revoca e informazioni sulle anomalie che determinano la revoca);

f) prevengono l'uso improprio della chiave privata, richiedendo la revoca del certificato della chiave pubblica associato in caso di compromissione della chiave privata o dei dati di attivazione della stessa;

g) sono responsabili e hanno l'obbligo di richiedere la revoca del certificato nelle circostanze indicate nelle politiche di certificazione (CP) e nella dichiarazione sulle prassi di certificazione (CPS) dell'autorità di certificazione;

h) in caso di perdita, furto o potenziale compromissione di qualsiasi chiave AETR utilizzata nel contesto di TACHOnet, informano immediatamente l'autorità di registrazione.

5. Responsabilità

Fatta salva la responsabilità della Commissione europea in violazione di disposizioni della legge nazionale applicabile o in relazione a questioni rientranti nell'ambito di applicazione di detta legge, la Commissione europea declina ogni responsabilità per quanto riguarda:

a) il contenuto del certificato, del quale è responsabile esclusivamente il titolare del certificato stesso; spetta al titolare del certificato verificare l'accuratezza del contenuto dello stesso;

b) l'utilizzo del certificato da parte del titolare.

Sottoappendice 4.9

Descrizione del servizio PKI per TACHOnet

1. Introduzione

Per PKI (Public Key Infrastructure, infrastruttura a chiave pubblica) si intende l'insieme di ruoli, politiche, procedure e sistemi necessari per creare, gestire, distribuire e revocare i certificati digitali[3]. Il servizio PKI dell'MCE tramite eDelivery consente il rilascio e la gestione di certificati digitali utilizzati per garantire la riservatezza, l'integrità e la non disconoscibilità delle informazioni scambiate tra punti di accesso (AP).

Il servizio PKI di eDelivery si basa sulla soluzione TeleSec Shared-Business-CA (Certification Authority, autorità di certificazione) del Trust Center, cui si applicano la politica di certificazione (Certificate Policy, CP) / la dichiarazione sulle prassi di certificazione (Certification Practices Statement, CPS) di TeleSec Shared-Business-CA di T-Systems International GmbH[4].

Il servizio PKI rilascia certificati idonei a garantire la sicurezza di vari processi all'interno e all'esterno di imprese, organizzazioni, autorità e istituzioni pubbliche che richiedono un livello medio di sicurezza per verificare l'autenticità, l'integrità e l'affidabilità dell'entità finale.

2. Procedura di richiesta del certificato

2.1. Ruoli e responsabilità

2.1.1. "Organizzazione" o "autorità nazionale" che richiede il certificato

2.1.1.1. L'autorità nazionale richiede i certificati nel contesto del progetto TACHOnet.

2.1.1.2 L'autorità nazionale:

a) richiede i certificati al servizio PKI dell'MCE;

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

[4] Le versioni aggiornate della CP e della CPS possono essere consultate all'indirizzo: https://www.telesec.de/en/sbca-en/support/download-area/.

b) genera le chiavi private e le corrispondenti chiavi pubbliche da inserire nei certificati rilasciati dall'autorità di certificazione;

c) scarica il certificato approvato;

d) firma e spedisce all'autorità di registrazione:

i) il modulo identificativo delle persone da contattare e dei corrieri fiduciari,

ii) la procura individuale firmata[5].

2.1.2. Corriere fiduciario

2.1.2.1. L'autorità nazionale nomina un corriere fiduciario.

2.1.2.2. Il corriere fiduciario:

a) consegna la chiave pubblica all'autorità di registrazione nell'ambito di una procedura di identificazione e registrazione faccia a faccia;

b) ottiene il certificato corrispondente dall'autorità di registrazione.

2.1.3. Titolare del dominio

2.1.3.1. La DG MOVE è titolare del dominio.

2.1.3.2. Il titolare del dominio:

a) convalida e coordina la rete TACHOnet e l'architettura di sicurezza di TACHOnet, compresa la convalida delle procedure di rilascio dei certificati;

b) gestisce il sistema centrale di TACHOnet e coordina l'attività delle parti per quanto riguarda il funzionamento di TACHOnet;

c) esegue, insieme con le autorità nazionali, le prove di connessione a TACHOnet.

---

[5] Per procura si intende un atto giuridico mediante il quale l'organizzazione autorizza e conferisce alla Commissione europea, rappresentata dal funzionario identificato responsabile del servizio PKI dell'MCE, il potere di richiedere a TeleSec Shared-Business-CA di T-Systems International GmbH la generazione di un certificato a proprio nome. Cfr. anche punto 6.

2.1.4. Autorità di registrazione

2.1.4.1. Il centro comune di ricerca (JRC) è l'autorità di registrazione.

2.1.4.2. All'autorità di registrazione incombe il compito di verificare l'identità del corriere fiduciario e di registrare e approvare le richieste di rilascio, revoca e rinnovo dei certificati digitali.

2.1.4.3. L'autorità di registrazione:

a) assegna l'identificatore univoco all'autorità nazionale;

b) autentica l'identità dell'autorità nazionale, i suoi punti di contatto e corrieri fiduciari;

c) comunica con il servizio di assistenza dell'MCE per quanto riguarda l'autenticità dell'autorità nazionale, i suoi punti di contatto e corrieri fiduciari;

d) informa l'autorità nazionale in merito all'approvazione o al rigetto del certificato.

2.1.5. Autorità di certificazione

2.1.5.1. All'autorità di certificazione incombe il compito di predisporre l'infrastruttura tecnica per la richiesta, il rilascio e la revoca dei certificati digitali.

2.1.5.2. L'autorità di certificazione:

a) mette a disposizione l'infrastruttura tecnica per le richieste di certificati da parte delle autorità nazionali;

b) convalida o respinge la richiesta di certificato;

c) comunica con l'autorità di registrazione per la verifica dell'identità dell'organizzazione richiedente, ove necessario.

2.2. Rilascio del certificato

2.2.1. Il rilascio del certificato è effettuato conformemente alle seguenti fasi sequenziali, illustrate nella figura 1:

a) **fase 1:** identificazione del corriere fiduciario;

b) **fase 2:** creazione della richiesta di certificato;

c) **fase 3:** registrazione presso l'autorità di registrazione;

d) **fase 4:** generazione del certificato;

e) **fase 5:** pubblicazione del certificato;

f) **fase 6:** accettazione del certificato.

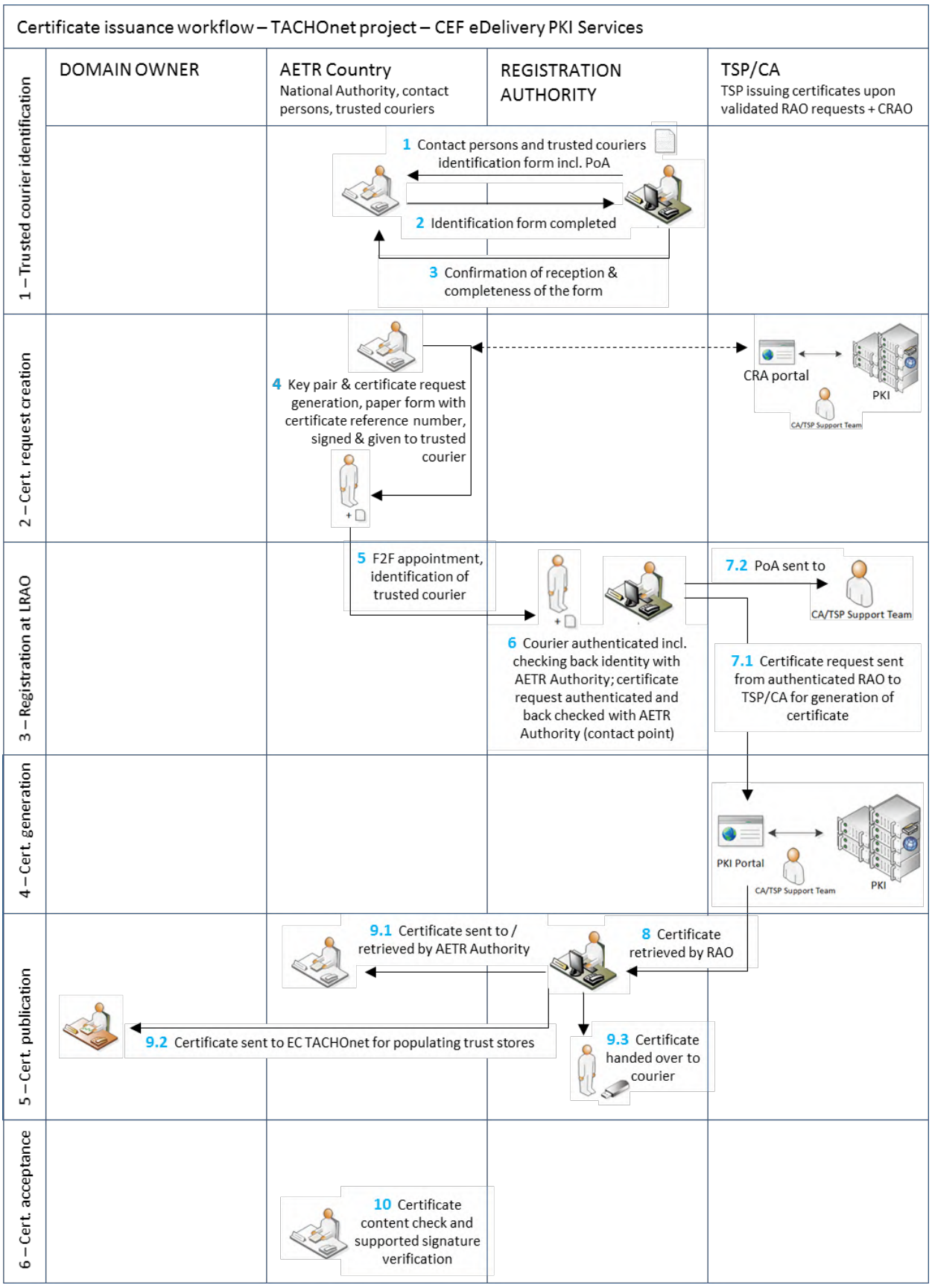


Figura 1 - Flusso di lavoro relativo al rilascio del certificato

2.2.2. Fase 1 - Identificazione del corriere fiduciario

L'identificazione del corriere fiduciario avviene conformemente alla procedura seguente:

a) L'autorità di registrazione invia all'autorità nazionale il modulo identificativo delle persone da contattare e dei corrieri fiduciari[6]. Tale modulo comprende anche una procura che deve essere firmata dall'organizzazione (autorità AETR).

b) L'autorità nazionale rispedisce all'autorità di registrazione il modulo compilato e la procura firmata.

c) L'autorità di registrazione conferma l'avvenuto ricevimento e la completezza del modulo.

d) L'autorità di registrazione fornisce al titolare del dominio una copia aggiornata dell'elenco di persone da contattare e corrieri fiduciari.

2.2.3. Fase 2 - Creazione della richiesta di certificato

2.2.3.1. La richiesta e il reperimento del certificato sono effettuati sullo stesso computer e utilizzando lo stesso browser.

2.2.3.2. La creazione della richiesta di certificato avviene conformemente alla procedura descritta di seguito.

a) L'organizzazione si collega all'interfaccia web dell'utente per richiedere il certificato tramite l'URL https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en: e inserisce il nome utente "**sbca/CEF_eDelivery.europa.eu**" e la password "**digit.333**".

[6] Cfr. punto 5.

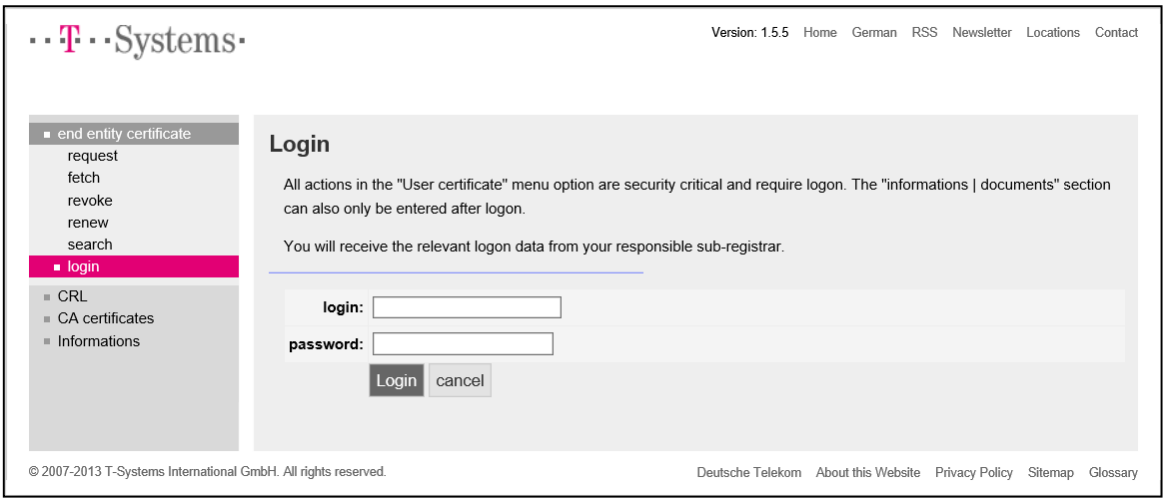


Figura 2

b) L'organizzazione clicca su "request" (richiesta) sul lato sinistro del quadro e seleziona "CEF_TACHOnet" nel menù a tendina.

Figura 3

c) L'organizzazione compila il modulo di richiesta del certificato illustrato nella figura 4 con le informazioni di cui alla tabella 3, cliccando su "Next (soft-PSE)" per concludere la procedura.

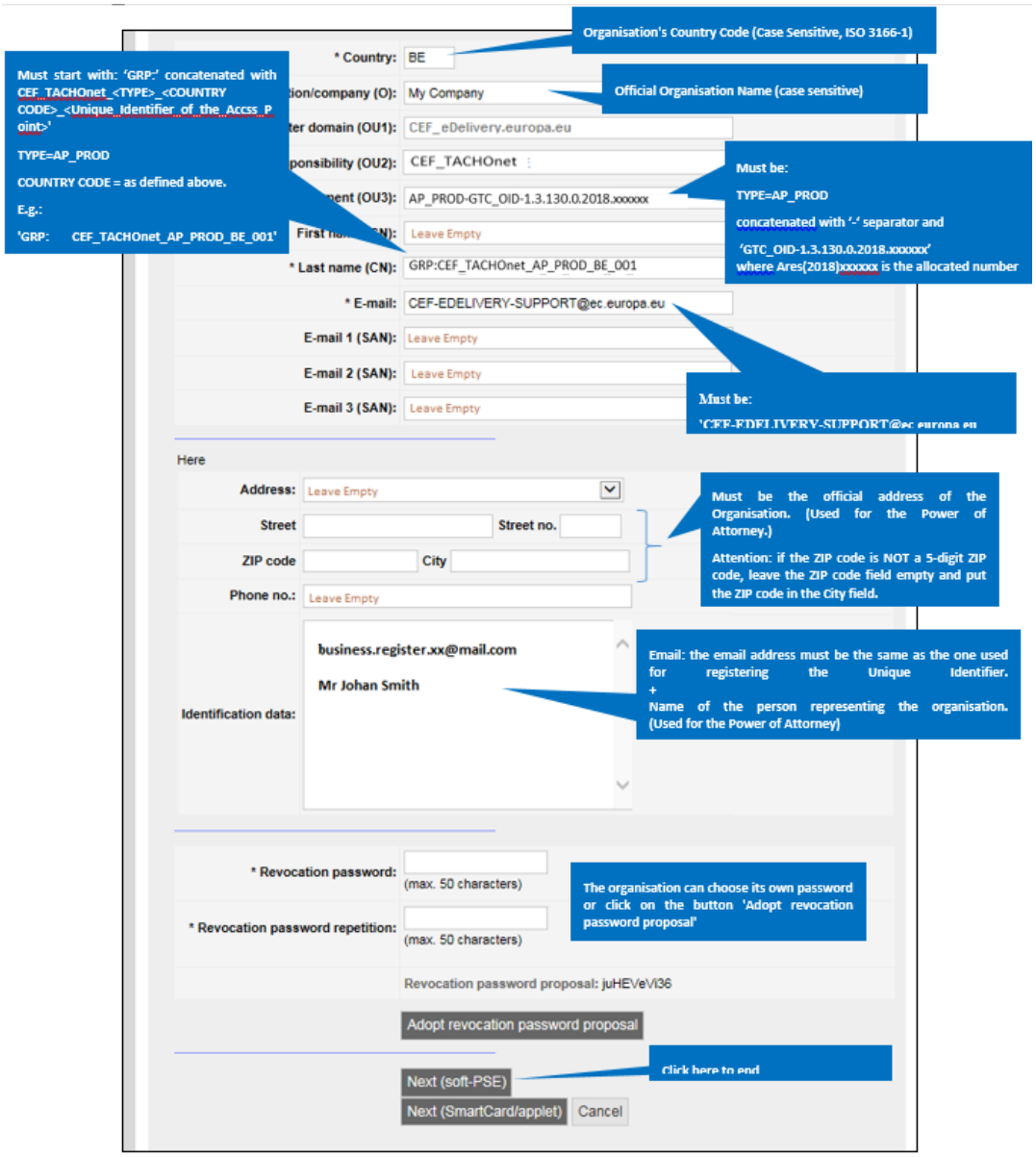

Organisation's Country Code (Case Sensitive, ISO 3166-1)
Official Organisation Name (case sensitive)
Must start with: 'GRP:' concatenated with CEF_TACHOnet_<TYPE>_<COUNTRY CODE>_<Unique_Identifier_of_the_Accss_Point>'
TYPE=AP_PROD
COUNTRY CODE = as defined above.
E.g.:
'GRP: CEF_TACHOnet_AP_PROD_BE_001'
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
My Company
CEF_eDelivery.europa.eu
CEF_TACHOnet
AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
Leave Empty
GRP:CEF_TACHOnet_AP_PROD_BE_001
CEF-EDELIVERY-SUPPORT@ec.europa.eu
E-mail 1 (SAN):
E-mail 2 (SAN):
E-mail 3 (SAN):
Here
Address:
Street
Street no.
ZIP code
City
Phone no.:
Identification data:
business.register.xx@mail.com
Mr Johan Smith
* Revocation password:
(max. 50 characters)
* Revocation password repetition:
(max. 50 characters)
Revocation password proposal: juHEVeVi36
Adopt revocation password proposal
Next (soft-PSE)
Next (SmartCard/applet)
Cancel

Figura 4

Campi richiesti	Descrizione
Paese [Country]	**C=Country Code** (codice paese), ubicazione del titolare del certificato, verificata consultando un elenco pubblico; Vincoli: 2 caratteri, conformemente alla norma ISO 3166-1, alpha-2, distinzione tra maiuscole e minuscole; Esempi: DE, BE, NL Casi specifici: UK (per il Regno Unito), EL (per la Grecia)
Organizzazione/Impresa [Organisation/Company (O)]	**O=Nome dell'organizzazione del titolare del certificato**
Dominio principale [Master domain (OU1)]	**OU=CEF_eDelivery.europa.eu**
Settore di responsabilità [Area of responsibility (OU2)]	**OU=CEF_TACHOnet**
Dipartimento [Department (OU3)]	Valore obbligatorio per "AREA OF RESPONSIBILITY" (settore di responsabilità) Il contenuto deve essere verificato consultando un elenco positivo al momento della richiesta del certificato. Se il dato non corrisponde all'elenco, la richiesta è bloccata. Formato: **OU=<TYPE>-<GTC_NUMBER>** dove "<TYPE>" è sostituito da AP_PROD: punto di accesso in ambiente di produzione (Access Point in Production environment) e dove <GTC_NUMBER> è **GTC_OID-1.3.130.0.2018.xxxxxx**, dove Ares(2018)xxxxxx è il numero GTC del progetto TACHOnet. per es.: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
Nome [First Name (CN)]	Deve essere vuoto
Cognome [Last name (CN)]	Deve cominciare con "GRP:", seguito da un nome comune. Formato: **CN=GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** per es.: GRP:CEF_TACHOnet_AP_PROD_BE_001
Indirizzo di posta elettronica [E-mail]	**E=CEF-EDELIVERY-SUPPORT@ec.europa.eu**
Indirizzo di posta elettronica [E-mail 1 (SAN)]	Deve essere vuoto
Indirizzo di posta elettronica [E-mail 2 (SAN)]	Deve essere vuoto
Indirizzo di posta elettronica [E-mail 3 (SAN)]	Deve essere vuoto

Indirizzo [Address]	Deve essere vuoto
Via [Street]	Deve essere l'indirizzo ufficiale dell'organizzazione del titolare del certificato. (Utilizzato per la procura.)
Numero civico [Street no.]	Deve essere l'indirizzo ufficiale dell'organizzazione del titolare del certificato. (Utilizzato per la procura.)
CAP [Zip Code]	Deve essere l'indirizzo ufficiale dell'organizzazione del titolare del certificato. (Utilizzato per la procura.) **Attenzione**: se il CAP NON è un codice di avviamento postale a 5 cifre, lasciare il campo vuoto e inserire il CAP nel campo Città [City].
Città [City]	Deve essere l'indirizzo ufficiale dell'organizzazione del titolare del certificato. (Utilizzato per la procura.) **Attenzione**: se il CAP NON è un codice di avviamento postale a 5 cifre, lasciare il campo vuoto e inserire il CAP nel campo Città [City].
Numero di telefono [Phone no]	Deve essere vuoto
Dati identificativi [Identification data]	L'indirizzo di posta elettronica deve essere identico a quello usato per la registrazione dell'identificatore unico (Unique Identifier). + Deve essere il nome della persona che rappresenta l'organizzazione. (Utilizzato per la procura.) + Numero di registro delle imprese (**Commercial Register No**, obbligatorio solo per le organizzazioni private) Registrata presso il tribunale di (**Entered at the Local Court of**, richiesto solo per le organizzazioni private tedesche e austriache)
Password di revoca [Revocation password]	Campo obbligatorio scelto dal richiedente
Ripetizione password di revoca [Revocation password repetition]	Ripetizione campo obbligatorio scelto dal richiedente

Tabella 3 - Dati completi di ciascun campo richiesto

d) La lunghezza della chiave selezionata è 2048(High Grade).

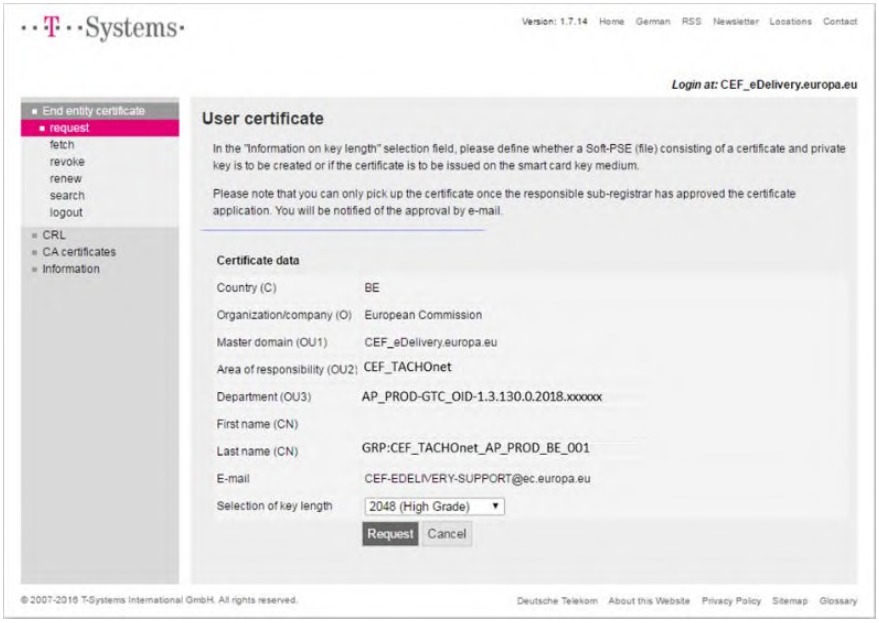


Figura 5

e) L'organizzazione registra il numero di riferimento per reperire il certificato.

Figura 6

f) Il servizio di assistenza dell'MCE controlla le nuove richieste di certificati e verifica se le informazioni contenute nella richiesta di certificato siano valide, cioè conformi alla convenzione di denominazione di cui all'appendice 5.1, Convenzione di denominazione per i certificati.

g) Il servizio di assistenza dell'MCE verifica che il formato delle informazioni inserite nella richiesta sia valido.

h) Se un controllo di cui ai precedenti punti 5 o 6 dà esito negativo, il servizio di assistenza dell'MCE invia un messaggio di posta elettronica all'indirizzo fornito nei dati identificativi ("Identification data") del modulo di richiesta, con copia al titolare del dominio, in cui invita l'organizzazione a riavviare la procedura. La richiesta di certificato non andata a buon fine è annullata.

i) Il servizio di assistenza dell'MCE invia all'autorità di registrazione un messaggio di posta elettronica relativo alla validità della richiesta. Il messaggio comprende:

    1) il nome dell'organizzazione, indicato nel campo "Organisation (O)" della richiesta di certificato;

    2) i dati del certificato, compreso il nome del punto di accesso (AP) per cui deve essere rilasciato il certificato, indicato nel campo "Last Name (CN)" della richiesta di certificato;

    3) il numero di riferimento del certificato;

    4) l'indirizzo dell'organizzazione, l'indirizzo di posta elettronica e il nome della persona che la rappresenta.

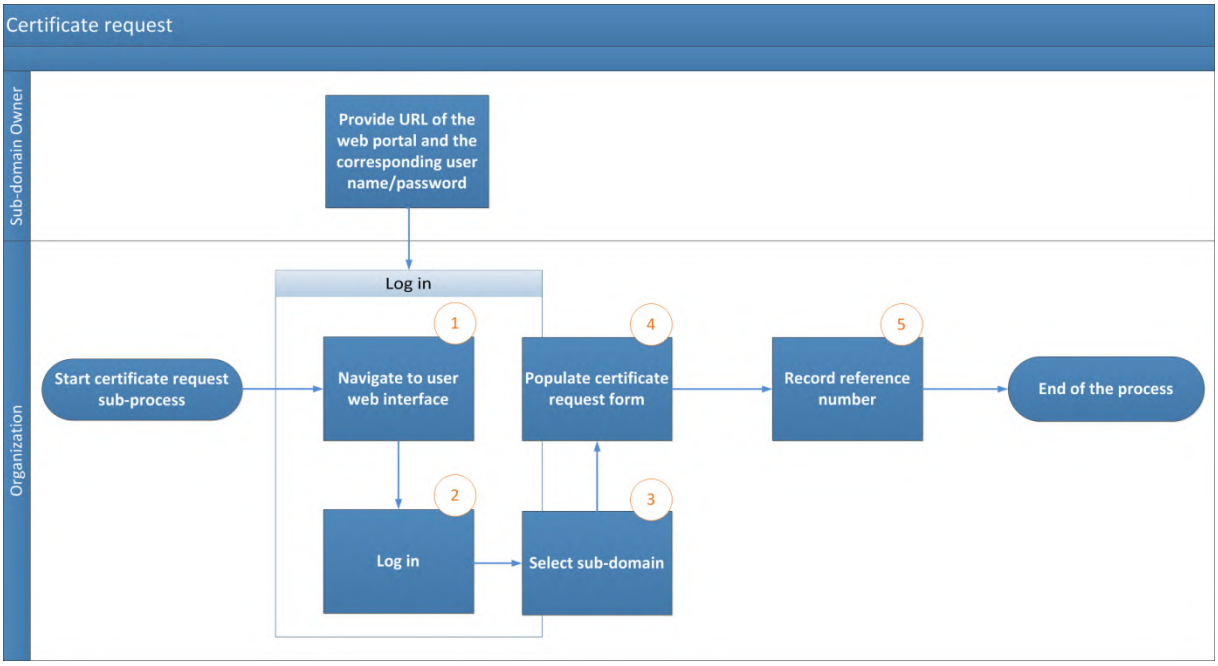


Figura 7 – Procedura di richiesta del certificato

2.2.4. Fase 3 - Registrazione presso l'autorità di registrazione (approvazione del certificato)

2.2.4.1. Il corriere fiduciario o il punto di contatto prende appuntamento con l'autorità di registrazione mediante scambio di messaggi di posta elettronica, identificando il corriere fiduciario che si presenterà fisicamente all'incontro.

2.2.4.2. L'organizzazione prepara la documentazione, costituita da:

a) procura compilata e firmata;

b) copia del passaporto in corso di validità del corriere fiduciario che si presenterà fisicamente; tale copia deve essere firmata da un punto di contatto dell'organizzazione identificato nella fase 1;

c) modulo cartaceo di richiesta del certificato firmato da un punto di contatto dell'organizzazione.

2.2.4.3. L'autorità di registrazione riceve il corriere fiduciario previa verifica dell'identità presso la portineria dell'edificio. L'autorità di registrazione esegue la registrazione faccia a faccia della richiesta di certificato come segue:

a) verifica e convalida l'identità del corriere fiduciario;

b) verifica l'aspetto fisico del corriere fiduciario rispetto al passaporto presentato dal medesimo;

c) verifica la validità del passaporto presentato dal corriere fiduciario;

d) verifica il passaporto convalidato presentato dal corriere fiduciario rispetto alla copia del passaporto valido del corriere fiduciario firmata da un punto di contatto identificato dell'organizzazione; la firma è autenticata mediante confronto con l'originale di cui al "modulo identificativo del corriere fiduciario e dei punti di contatto";

e) verifica la procura compilata e firmata;

f) verifica il modulo cartaceo di richiesta del certificato e la relativa firma rispetto all'originale di cui al "modulo identificativo del corriere fiduciario e dei punti di contatto";

g) telefona al punto di contatto firmatario per ricontrollare l'identità del corriere fiduciario e il contenuto della richiesta di certificato.

2.2.4.4. L'autorità di registrazione conferma al servizio di assistenza dell'MCE che l'autorità nazionale è autorizzata a gestire gli elementi per i quali richiede i certificati e che la corrispondente procedura di registrazione faccia a faccia ha dato esito positivo. La conferma è trasmessa mediante messaggio di posta elettronica sicura certificata "CommiSign", allegando copia scansionata della documentazione autenticata faccia a faccia e della lista di controllo firmata della procedura eseguita dall'autorità di registrazione.

2.2.4.5. Se l'autorità di registrazione conferma la validità della richiesta, la procedura prosegue come indicato ai punti 2.2.4.6 e 2.2.4.7. In caso contrario, il rilascio del certificato è rifiutato e l'organizzazione ne viene informata.

2.2.4.6. Il servizio di assistenza dell'MCE approva la richiesta di certificato e comunica all'autorità di registrazione l'approvazione del certificato.

2.2.4.7. L'autorità di registrazione comunica all'organizzazione che il certificato può essere reperito attraverso il portale dell'utente.

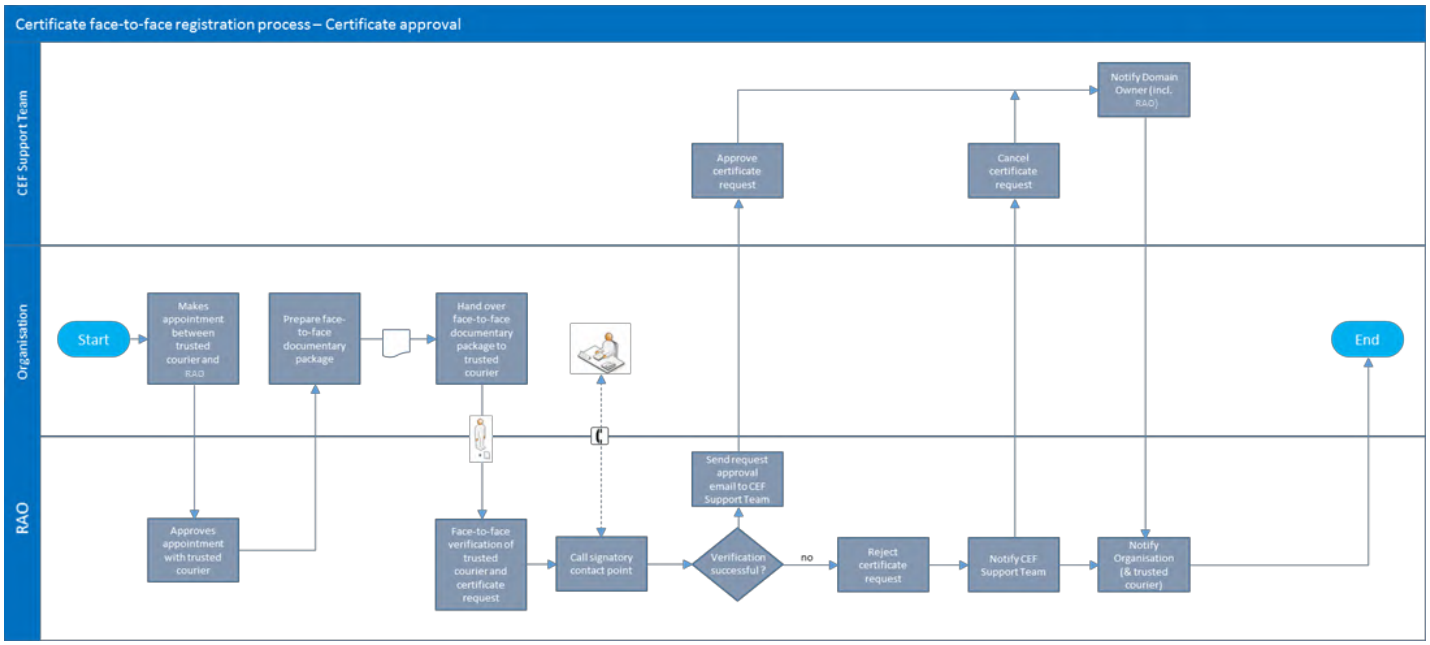


Figura 8 - Approvazione del certificato

2.2.5. Fase 4 - Generazione del certificato

Il certificato viene generato al momento dell'approvazione della richiesta.

2.2.6. Fase 5 - Pubblicazione e reperimento del certificato

2.2.6.1. Successivamente all'approvazione della richiesta di certificato, l'autorità di registrazione recupera il certificato e ne consegna una copia al corriere fiduciario.

2.2.6.2. L'autorità di registrazione comunica all'organizzazione che il certificato può essere reperito.

2.2.6.3. L'organizzazione si collega al portale dell'utente all'indirizzo https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en e vi accede con il nome utente "**sbca/CEF_eDelivery.europa.eu**" e la password "**digit.333**".

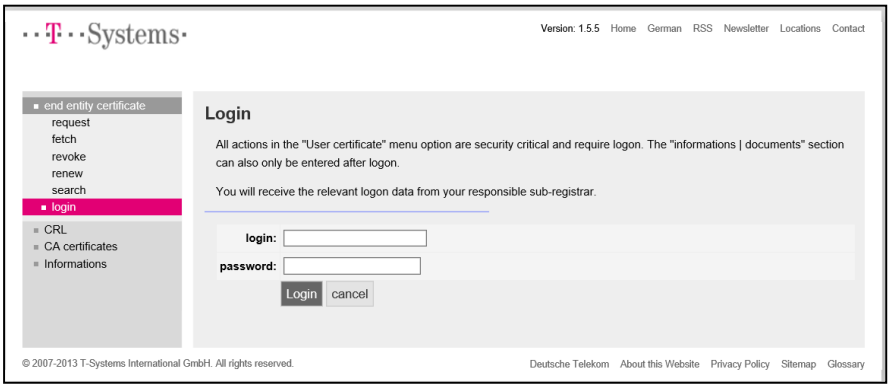


Figura 9

2.2.6.4. L'organizzazione clicca sul pulsante "fetch" (recupera) nell'elenco a sinistra e inserisce il numero di riferimento registrato durante la procedura di richiesta del certificato.

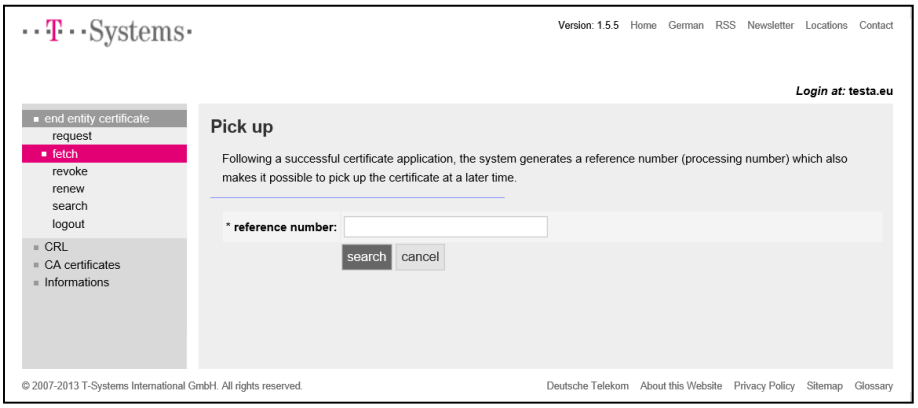


Figura 10

2.2.6.5. L'organizzazione installa i certificati cliccando sul pulsante "Install".

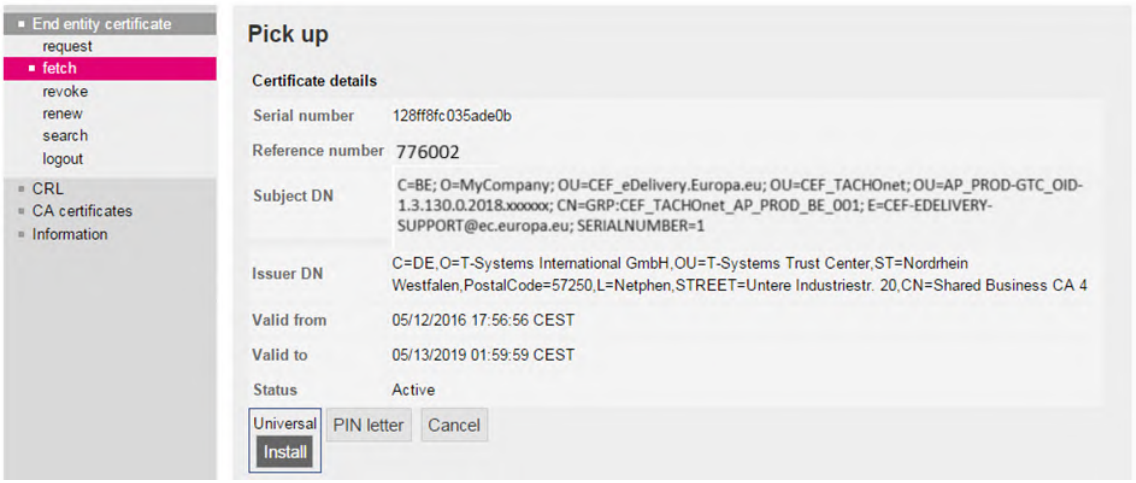


Figura 11

2.2.6.6. Il certificato viene installato sul punto di accesso. Poiché l'operazione dipende dall'applicazione specifica, l'organizzazione si rivolge al proprio fornitore di punto di accesso per ottenere la descrizione di questa procedura.

2.2.6.7. Per installare il certificato sul punto di accesso è necessario eseguire le operazioni seguenti:

a) esportare la chiave privata e il certificato,

b) creare il keystore e il truststore,

c) installare il keystore e il truststore sul punto di accesso.

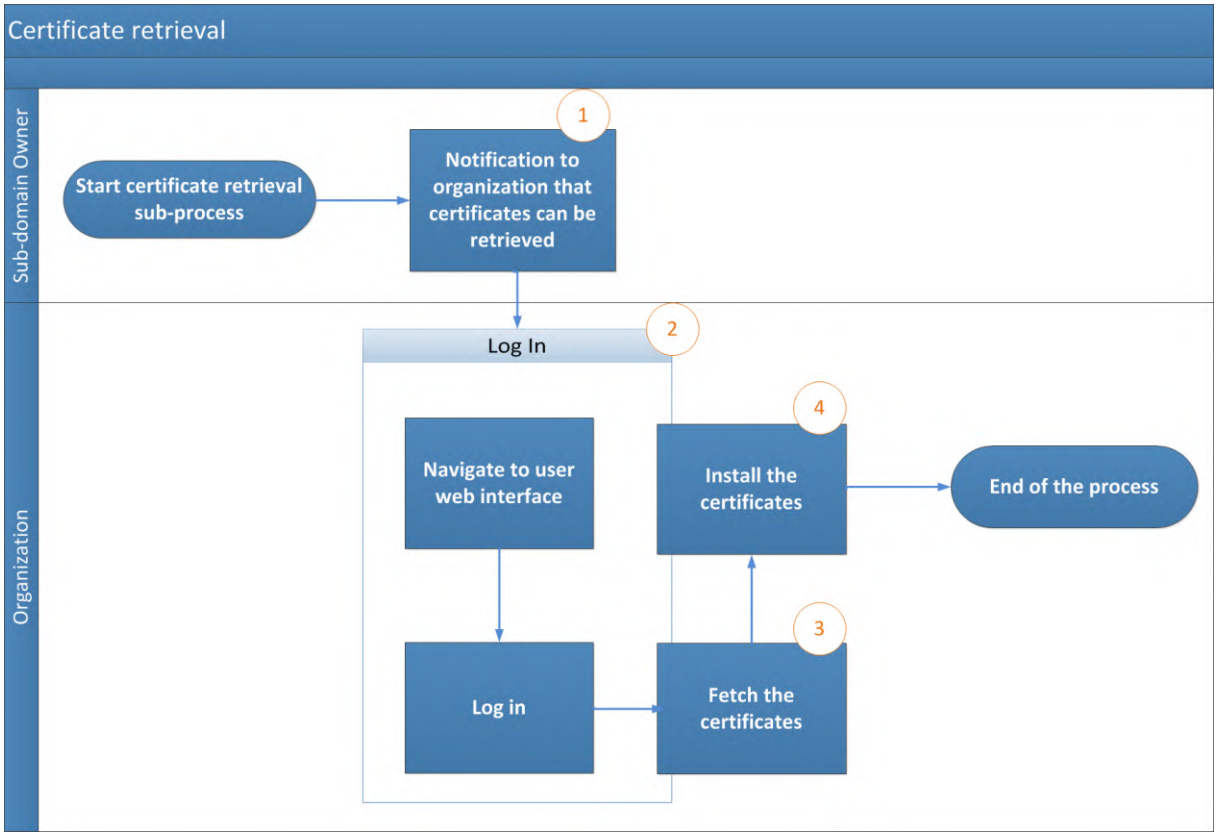


Figura 12 - Reperimento del certificato

3. Procedura di revoca del certificato

3.1. L'organizzazione presenta una richiesta di revoca tramite il portale web dell'utente.

3.2. Il servizio di assistenza dell'MCE esegue la revoca del certificato.

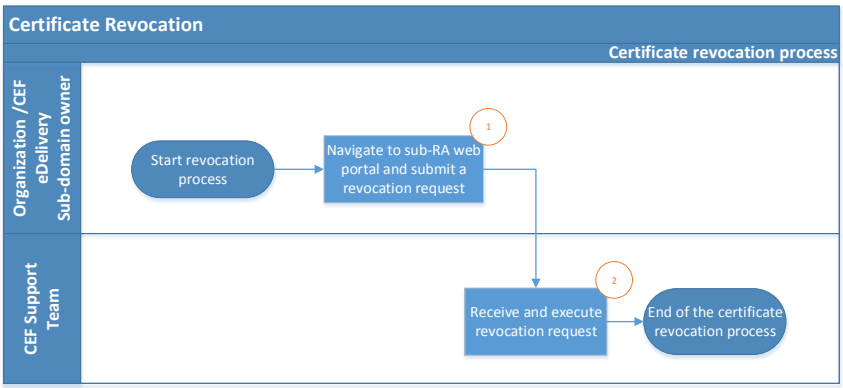


Figura 13 - Revoca del certificato

4. Termini e condizioni generali del servizio PKI dell'MCE

4.1. Contesto

In qualità di fornitore di soluzioni per l'elemento eDelivery del meccanismo per collegare l'Europa, la DIGIT mette a disposizione delle parti contraenti dell'AETR un servizio PKI[7] ("servizio PKI dell'MCE"). Il servizio PKI dell'MCE è utilizzato dalle autorità nazionali ("utenti finali") che partecipano a TACHOnet.

La DIGIT è titolare della PKI all'interno della soluzione TeleSec Shared-Business-CA ("SBCA") gestita dal Trust Center di T-Systems International GmbH ("T-Systems"[8]). La DIGIT svolge il ruolo di conservatore principale del dominio "CEF_eDelivery.europa.eu" della SBCA. In tale ruolo, la DIGIT crea sottodomini nell'ambito del dominio "CEF_eDelivery.europa.eu" per ciascun progetto che utilizza il servizio PKI dell'MCE.

Il presente documento fornisce informazioni sui termini e le condizioni del sottodominio TACHOnet. La DIGIT svolge il ruolo di sottoconservatore di questo sottodominio. In tale veste, essa rilascia, revoca e rinnova i certificati di questo progetto.

4.2. Clausola di esclusione della responsabilità

La Commissione europea declina ogni responsabilità per quanto riguarda il contenuto del certificato, del quale è responsabile esclusivamente il titolare del certificato stesso. Spetta al titolare del certificato verificare l'accuratezza del contenuto dello stesso.

La Commissione europea declina ogni responsabilità per quanto riguarda l'uso del certificato da parte del titolare, il quale è un soggetto giuridico esterno alla Commissione europea.

---

7 Per PKI (Public Key Infrastructure, infrastruttura a chiave pubblica) si intende l'insieme di ruoli, politiche, procedure e sistemi necessari per creare, gestire, distribuire e revocare i certificati digitali.

8 Il ruolo fiduciario dell'operatore del Trust Center, ubicato presso il Trust Center di T-Systems, comprende anche la mansione di autorità di registrazione interna.

La presente clausola di esclusione della responsabilità non ha lo scopo di limitare la responsabilità della Commissione europea in violazione di disposizioni della legge nazionale applicabile, né di escluderla nei casi in cui non può essere esclusa in forza di detta legge.

4.3. Utilizzi autorizzati/vietati dei certificati

4.3.1. Uso permesso dei certificati

Una volta rilasciato, il certificato è utilizzato dal titolare[9] soltanto nel contesto di TACHOnet. In questo contesto, il certificato può essere utilizzato per:

- autenticare l'origine dei dati;
- criptare i dati;
- assicurare il rilevamento di violazioni dell'integrità dei dati.

4.3.2. Uso vietato dei certificati

È vietato qualsiasi uso non espressamente autorizzato nell'ambito degli utilizzi permessi del certificato.

4.4. Altri obblighi del titolare del certificato

I termini e le condizioni dettagliati della SBCA sono definiti da T-Systems nella politica di certificazione (Certificate Policy, CP) / dichiarazione sulle prassi di certificazione (Certification Practice Statement, CPS) del servizio SBCA[10]. Tale documento comprende le specifiche di sicurezza e le linee guida riguardanti gli aspetti tecnici e organizzativi e descrive le attività dell'operatore del Trust Center nel ruolo di autorità di certificazione (CA) e di autorità di registrazione (RA), nonché del terzo delegato dall'autorità di registrazione (RA).

Possono richiedere un certificato soltanto gli organismi autorizzati a partecipare a TACHOnet.

---

[9] Identificata dal valore dell'attributo "O=" nel nome caratteristico del soggetto (Subject Distinguished Name) del certificato rilasciato.

[10] Le versioni aggiornate della CP/CPS del servizio SBCA di T-Systems sono disponibili all'indirizzo: https://www.telesec.de/en/sbca-en/support/download-area/.

Per quanto riguarda l'accettazione del certificato, si applica la clausola 4.4.1 della politica di certificazione e dichiarazione sulle prassi di certificazione ("CP/CPS") del servizio SBCA; inoltre, le condizioni d'uso e le disposizioni di cui al presente documento sono considerate accettate dall'organizzazione alla quale viene rilasciato il certificato ("O=") al momento del primo utilizzo.

Per quanto riguarda la pubblicazione del certificato, si applica la clausola 2.2 della CP/CPS del servizio SBCA.

Tutti i titolari di certificati rispettano le seguenti disposizioni:

1) proteggono la propria chiave privata contro l'uso non autorizzato;

2) si astengono dal trasferire o rivelare a terzi, anche in qualità di rappresentanti, la propria chiave privata;

3) si astengono dal continuare a utilizzare la chiave privata dopo la scadenza del periodo di validità o la revoca del certificato, salvo per visualizzare dati criptati (per es., decrittare messaggi di posta elettronica);

4) al titolare del certificato incombe il compito di copiare o inoltrare la chiave all'entità o alle entità finali;

5) il titolare del certificato deve imporre all'entità finale/a tutte le entità finali l'obbligo di rispettare i presenti termini e condizioni, compresa la CP/CPS del servizio SBCA, quando utilizzano la chiave privata;

6) il titolare del certificato deve fornire l'identificazione dei mandatari autorizzati a richiedere la revoca dei certificati rilasciati all'organizzazione con le informazioni sulle anomalie che determinano la revoca e la password di revoca;

7) per i certificati associati a gruppi di persone e funzioni e/o persone giuridiche, quando una persona esce dal gruppo di entità finali (per es. cessazione del rapporto di lavoro), il titolare del certificato deve prevenire l'uso improprio della chiave privata revocando il certificato;

8) il compito di richiedere la revoca del certificato incombe al titolare del certificato, il quale è tenuto a farlo nelle circostanze di cui alla clausola 4.9.1 della CP/CPS del servizio SBCA.

Per quanto riguarda il rinnovo o la creazione di nuove chiavi per i certificati, si applica la clausola 4.6 o 4.7 della CP/CPS del servizio SBCA.

Per quanto riguarda la modifica del certificato, si applica la clausola 4.8 della CP/CPS del servizio SBCA.

Per quanto riguarda la revoca del certificato, si applica la clausola 4.9 della CP/CPS del servizio SBCA.

5. Modulo identificativo delle persone da contattare e dei corrieri fiduciari (modello)

Il sottoscritto, *[nominativo e indirizzo del rappresentante dell'organizzazione]***, certifica che le seguenti informazioni devono essere usate nel contesto della richiesta, della generazione e del reperimento dei certificati digitali delle chiavi pubbliche dei punti di accesso a TACHOnet per assicurare la riservatezza, l'integrità e la non disconoscibilità dei messaggi TACHOnet.**

Informazioni sulle persone da contattare**:**

– **Persona da contattare n. 1**	– **Persona da contattare n. 2**
– Cognome:	– Cognome:
– Nome:	– Nome:
– Cellulare:	– Cellulare:
– Telefono fisso:	– Telefono fisso:
– Indirizzo di posta elettronica:	– Indirizzo di posta elettronica:
– Specimen di firma: –	– Specimen di firma: – – –

Informazioni sul corriere fiduciario:

– **Corriere fiduciario n. 1**	– **Corriere fiduciario n. 2**
– Cognome:	– Cognome:
– Nome:	– Nome:
– Cellulare:	– Cellulare:
– Indirizzo di posta elettronica:	– Indirizzo di posta elettronica:
– Paese di rilascio del passaporto:	– Paese di rilascio del passaporto:
– Numero di passaporto:	– Numero di passaporto:
– Data di scadenza del passaporto:	– Data di scadenza del passaporto:

Luogo, data, timbro dell'impresa o dell'organizzazione:

Firma del mandatario:

6. Documenti

6.1. Procura individuale (modello)

Un modello della procura individuale che deve essere firmata e presentata dal corriere fiduciario durante la registrazione faccia a faccia presso la RAO è disponibile qui di seguito:

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 FERIAL**

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):

☒ user [1]: e.g. mail security (signature, encryption), virtual private network (VPN), TLS/SSL client

☐ server [2]: 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-Gateway [3]: 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 months** [2] 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 month** [2] 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. Modulo cartaceo di richiesta del certificato (modello)

Un modello del modulo cartaceo di richiesta del certificato che deve essere firmato e presentato dal corriere fiduciario durante la registrazione faccia a faccia presso la RAO è disponibile qui di seguito:

7. Glossario

I principali termini utilizzati nella presente sottoappendice sono definiti nella sezione "CEF Definitions" del portale web digitale unico dell'MCE:

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

I principali acronimi utilizzati nella presente descrizione dell'offerta di componenti sono definiti nella sezione "CEF Glossary" del portale web digitale unico dell'MCE:

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