Consejo de la Unión Europea

Bruselas, 5 de noviembre de 2018
(OR. en)

13711/18
ADD 1

Expediente interinstitucional: 2018/0339 (NLE)

TRANS 488

NOTA

De:	Secretaría General del Consejo
A:	Delegaciones
N.º doc. prec.:	ST 13711/18 TRANS 448
N.° doc. Ción.:	ST 12727/18 TRANS 426 + ADD 1
Asunto:	Decisión del Consejo sobre la posición que debe adoptarse, en nombre de la Unión Europea, en el Grupo de expertos sobre el Acuerdo europeo sobre trabajo de tripulaciones de vehículos que efectúen transportes internacionales por carretera de la Comisión Económica para Europa de las Naciones Unidas

Anexo de la Decisión del Consejo de referencia.

ANEXO

Nuevo apéndice del Acuerdo europeo sobre el trabajo de las tripulaciones de los vehículos que efectúen transportes internacionales por carretera (AETR)

Apéndice 4

Especificaciones de TACHOnet

1. Ámbito de aplicación y objeto

1.1. El presente apéndice establece las condiciones que han de cumplirse para la conexión de las Partes Contratantes en el AETR a TACHOnet a través de eDelivery.

1.2. Las Partes Contratantes que se conecten a TACHOnet a través de eDelivery se atendrán a las disposiciones del presente apéndice.

2. Definiciones

a) «Parte Contratante» o «Parte»: cualquier Parte Contratante en el AETR.

b) «eDelivery»: servicio creado por la Comisión Europea que permite transmitir datos entre terceros por medios electrónicos y aporta pruebas relacionadas con la gestión de los datos transmitidos, incluida la prueba del envío y la recepción de los datos, y que protege los datos transmitidos frente al riesgo de alteración no autorizada.

c) «TACHOnet»: el sistema de intercambio electrónico de información sobre las tarjetas de conductor entre las Partes Contratantes a que se refiere el artículo 31, apartado 2, del Reglamento (UE) n.º 165/2014.

d) «Nodo central»: el sistema de información que permite el encaminamiento de los mensajes de TACHOnet entre las Partes solicitantes y las Partes que responden.

e) «Parte solicitante»: la Parte Contratante que envía una solicitud o notificación en TACHOnet, que posteriormente es encaminada por el nodo central a la correspondiente Parte que responde.

f) «Parte que responde»: la Parte Contratante a la que se dirige la solicitud o notificación de TACHOnet. g)

g) «Autoridad expedidora de la tarjeta»: la entidad facultada por una Parte Contratante para la expedición y gestión de tarjetas de tacógrafo.

3. Responsabilidades generales

3.1. Ninguna Parte Contratante podrá concluir acuerdos de acceso a TACHOnet en nombre de otra Parte ni representar de ningún otro modo a la otra Parte Contratante sobre la base del presente apéndice. Ninguna Parte Contratante podrá actuar como subcontratista de la otra Parte Contratante en las operaciones a que se hace referencia en el presente apéndice.

3.2. Las Partes Contratantes facilitarán el acceso a su registro nacional sobre tarjetas de conductor a través de TACHOnet de la manera y con el nivel de servicio que se establecen en el subapéndice 4.6.

3.3. Las Partes Contratantes se avisarán mutuamente a la mayor brevedad si observan en el ámbito de sus competencias alteraciones o errores que puedan poner en peligro el funcionamiento normal de TACHOnet.

3.4. Cada Parte designará a personas de contacto con respecto a TACHOnet a la Secretaría del AETR. Cualquier cambio en los puntos de contacto deberá indicarse por escrito a la Secretaría del AETR.

4. Ensayos de conexión a TACHOnet

4.1. La conexión de una Parte Contratante a TACHOnet se establecerá una vez hayan finalizado de forma satisfactoria los ensayos de conexión, integración y rendimiento de conformidad con las instrucciones de la Comisión Europea y bajo su supervisión.

4.2. De fracasar los ensayos preliminares, la Comisión Europea podrá suspender temporalmente la fase de ensayo. Los ensayos se reanudarán una vez que la Parte Contratante haya comunicado a la Comisión Europea la adopción de las mejoras técnicas necesarias a escala nacional para hacer posible la ejecución satisfactoria de los ensayos preliminares.

4.3. La duración máxima de los ensayos preliminares será de seis meses.

5. Arquitectura de confianza

5.1. La arquitectura de confianza de TACHOnet garantizará la confidencialidad, la integridad y el no repudio de los mensajes de TACHOnet.

5.2. La arquitectura de confianza de TACHOnet se basará en un servicio de infraestructura de clave pública (PKI por sus siglas en inglés) establecido por la Comisión Europea, cuyos requisitos se establecen en los subapéndices 4.8 y 4.9.

5.3. En la arquitectura de confianza de TACHOnet intervendrán las siguientes entidades:

a) Autoridad de certificación, encargada de generar los certificados digitales que debe entregar la autoridad de registro a las autoridades nacionales de las Partes Contratantes (a través de mensajeros de confianza designados por ellas), así como de crear la infraestructura técnica relativa a la expedición, revocación y renovación de los certificados digitales.

b) Titular de dominio, encargado del funcionamiento del nodo central mencionado en el subapéndice 4.1 y de la validación y coordinación de la arquitectura de confianza de TACHOnet.

c) Autoridad de registro, encargada de registrar y aprobar las solicitudes de expedición, revocación y renovación de los certificados digitales, así como de verificar la identidad de los mensajeros de confianza.

d) Mensajero de confianza: persona designada por las autoridades nacionales encargada de la entrega de la clave pública a la autoridad de registro y de la obtención del correspondiente certificado generado por la autoridad de certificación.

e) Autoridad nacional de la Parte Contratante, que deberá:

i) generar las claves privadas y las claves públicas correspondientes que deben incluirse en los certificados que generará la autoridad de certificación;

ii) solicitar los certificados digitales a la autoridad de certificación;

iii) designar al mensajero de confianza.

5.4. La Comisión Europea designará a la autoridad de certificación y a la autoridad de registro.

5.5. Toda Parte Contratante que se conecte al sistema TACHOnet deberá solicitar la expedición de un certificado digital de conformidad con el subapéndice 4.9, con el fin de firmar y encriptar un mensaje de TACHOnet.

5.6. Un certificado podrá revocarse de conformidad con el subapéndice 4.9.

6. Protección de datos y confidencialidad

6.1. Las Partes, de conformidad con las legislaciones internacionales y nacionales sobre protección de datos, y en particular con el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, adoptarán todas las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de TACHOnet y evitar su alteración, pérdida o tratamiento no autorizado, o el acceso no autorizado a los mismos (en particular en lo que respecta a la autenticidad, la confidencialidad de los datos, la trazabilidad, la integridad, la disponibilidad y el no repudio y la seguridad de los mensajes).

6.2. Cada una de las Partes protegerá sus propios sistemas nacionales contra el uso ilícito, los códigos malintencionados, los virus, las intrusiones informáticas, las infracciones y la manipulación ilegal de datos y otras acciones similares por parte de terceros. Las Partes convienen en realizar esfuerzos razonables desde el punto de vista comercial para evitar la transmisión de virus, bombas de tiempo, gusanos u otros elementos similares o cualquier práctica de programación informática que pueda interferir en los sistemas informáticos de la otra Parte.

7. Costes

7.1. Las Partes Contratantes correrán con sus propios costes de desarrollo y funcionamiento en relación con sus propios sistemas de datos y procedimientos en la medida necesaria para cumplir las obligaciones establecidas en el presente apéndice.

7.2. Los servicios que se especifican en el subapéndice 4.1, prestados por el nodo central, son gratuitos.

8. Subcontratación

8.1. Las Partes podrán subcontratar cualesquiera servicios de los que sean responsables en virtud del presente apéndice.

8.2. Tal subcontratación no eximirá a la Parte de sus responsabilidades con arreglo al presente apéndice, incluida la responsabilidad de prestar un nivel de servicios adecuado de conformidad con el subapéndice 4.6.

Subapéndice 4.1.

Aspectos generales de TACHOnet

1. Descripción general

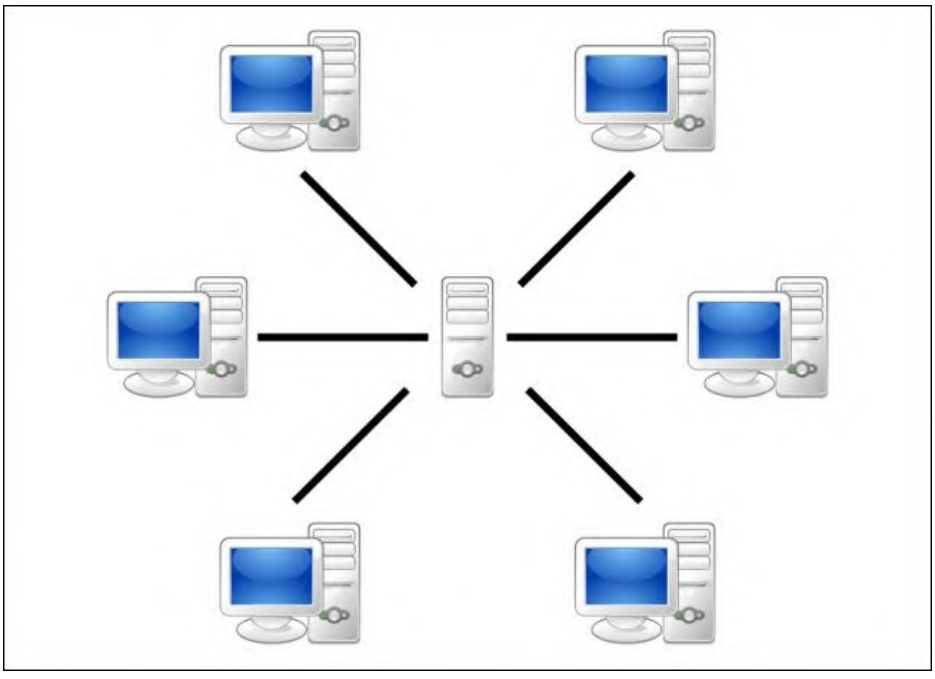
TACHOnet es un sistema electrónico de intercambio de información sobre las tarjetas de conductor entre las Partes Contratantes en el AETR. TACHOnet encamina las solicitudes de información de las Partes solicitantes a las Partes destinatarias, así como las respuestas de estas últimas a las primeras. Las Partes Contratantes que forman parte de TACHOnet deben conectar al sistema sus registros nacionales de tarjetas de conductor.

2. Arquitectura

El sistema de mensajería TACHOnet se compondrá de las siguientes partes:

2.1. Un nodo central, capaz de recibir una solicitud de la Parte solicitante, validarla y tramitarla enviándola a las Partes que responden. El nodo central esperará la respuesta de cada Parte que responda, consolidará todas las respuestas y enviará la respuesta consolidada a la Parte solicitante.

2.2. Los sistemas nacionales de las Partes, que estarán equipados con una interfaz que permita enviar solicitudes al nodo central y recibir las correspondientes respuestas. Los sistemas nacionales pueden utilizar programas informáticos sujetos a derechos de propiedad o comerciales para transmitir y recibir mensajes desde el nodo central.



3. Gestión

3.1. La gestión del nodo central correrá a cargo de la Comisión Europea, que será responsable de su funcionamiento técnico y de su mantenimiento.

3.2. El nodo central no almacenará datos por un período superior a seis meses, excepto los datos de registro y los datos estadísticos que figuran en el subapéndice 4.7.

3.3. El nodo central no permitirá el acceso a los datos personales, excepto en el caso de personal autorizado de la Comisión Europea, cuando sea necesario a efectos de supervisión, mantenimiento y diagnóstico de averías.

3.4. Cada una de las Partes Contratantes será responsable de lo siguiente:

3.4.1. La creación y gestión de sus sistemas nacionales, incluida la interfaz con el nodo central.

3.4.2. La instalación y mantenimiento de los soportes físicos y programas informáticos de su sistema nacional, tanto si están sujetos a derechos de propiedad como si son comerciales.

3.4.3. La correcta interoperabilidad de sus sistemas nacionales con el nodo central, incluida la gestión de los mensajes de error recibidos del nodo central.

3.4.4. La adopción de todas las medidas necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de la información.

3.4.5. El funcionamiento de los sistemas nacionales de conformidad con los niveles de servicio establecidos en el subapéndice 4.6.

Subapéndice 4.2

Funcionalidades de TACHOnet

1. Deberán facilitarse las siguientes funcionalidades a través del sistema de mensajería TACHOnet:

1.1. Control de Tarjetas Expedidas (CIC): permite a la Parte solicitante enviar una Solicitud de Control de Tarjetas Expedidas a una o a todas las Partes que responden para determinar si un solicitante de tarjeta ya posee una tarjeta de conductor expedida por las Partes que responden. Las Partes que responden contestarán a la solicitud mediante el envío de una Respuesta al Control de Tarjetas Expedidas.

1.2. Control del Estado de la Tarjeta(CCS): permite a la Parte solicitante preguntar a la Parte que responde acerca de los detalles de una tarjeta expedida por esta última mediante el envío de una Solicitud de Control del Estado de la Tarjeta. La Parte que responde contestará a la solicitud mediante el envío de una Respuesta al Control del Estado de la Tarjeta.

1.3. Modificación del Estado de la Tarjeta(MCS): permite a la Parte solicitante notificar a la Parte que responde, mediante una Solicitud de Modificación del Estado de la Tarjeta, que el estado de una tarjeta expedida por esta última ha sido modificado. La Parte que responde contestará con un Acuse de Recibo de la Modificación del Estado de la Tarjeta.

1.4. Tarjeta de Permiso de Conducción Expedida(ICDL): permite a la Parte solicitante notificar a la Parte que responde, mediante una Solicitud de Tarjeta de Permiso de Conducción Expedida, que la primera Parte ha expedido una tarjeta correspondiente a un permiso de conducción expedido por la segunda. La Parte que responde deberá contestar con una Respuesta de Tarjeta de Permiso de Conducción Expedida.

2. Se incluirán otros tipos de mensajes que se consideren adecuados para el eficaz funcionamiento de TACHOnet como, por ejemplo, notificaciones de error.

3. Los sistemas nacionales deberán reconocer los estados de tarjeta enumerados en el cuadro 1 cuando utilicen cualquiera de las funcionalidades descritas en el punto 1. No obstante, las Partes no estarán obligadas a aplicar un procedimiento administrativo que haga uso de todos los estados enumerados.

4. Cuando una Parte reciba una respuesta o una notificación en la que figure un estado que no se utiliza en sus procedimientos administrativos, el sistema nacional deberá traducir el estado que figura en el mensaje recibido al correspondiente valor en dicho procedimiento. El mensaje no podrá ser rechazado por la Parte que responde, siempre que el estado que figure en el mensaje esté enumerado en el cuadro 1.

5. El estado de la tarjeta enumerado en el cuadro 1 no se utilizará para determinar si una tarjeta de conductor es válida para la conducción. Cuando una Parte formule preguntas al registro de la autoridad nacional que ha expedido la tarjeta a través de la funcionalidad CCS, la respuesta contendrá el campo específico «válida para la conducción». Los procedimientos administrativos nacionales serán tales que las respuestas CCS contengan siempre el correspondiente valor «válida para la conducción».

Cuadro 1

Estados de las tarjetas

Estado de la tarjeta	**Definición**
Solicitud	La autoridad expedidora de la tarjeta ha recibido una solicitud de expedición de una tarjeta de conductor. Esta información ha sido registrada y almacenada en la base de datos con las claves de búsqueda generadas.
Aprobada	La autoridad expedidora de la tarjeta ha aprobado la solicitud de la tarjeta de tacógrafo.
Rechazada	La autoridad expedidora de la tarjeta no ha aprobado la solicitud.
Personalizada	La tarjeta de tacógrafo ha sido personalizada.
Remitida	La autoridad nacional ha remitido la tarjeta de conductor al conductor pertinente o a la agencia responsable de la entrega.
Entregada	La autoridad nacional ha entregado la tarjeta de conductor al conductor pertinente.
Confiscada	La tarjeta de conductor ha sido retirada al conductor por la autoridad competente.
Suspendida	La tarjeta de conductor ha sido retirada al conductor con carácter temporal.
Retirada	La autoridad expedidora de la tarjeta ha decidido retirar la tarjeta al conductor. La tarjeta ha sido definitivamente invalidada.
Devuelta	La tarjeta de tacógrafo ha sido devuelta a la autoridad expedidora de la tarjeta y se ha declarado que ya no es necesaria.
Perdida	La tarjeta de tacógrafo ha sido declarada perdida a la autoridad expedidora de la tarjeta.
Robada	La tarjeta de tacógrafo ha sido robada, según una denuncia presentada a la autoridad expedidora de la tarjeta. Una tarjeta robada se considera una tarjeta perdida.
Defectuosa	La tarjeta de tacógrafo ha sido declarada defectuosa por anomalías de funcionamiento a la autoridad expedidora de la tarjeta.
Caducada	El período de validez de la tarjeta de tacógrafo ha expirado.
Sustituida	La tarjeta de tacógrafo, que había sido declarada perdida, robada o defectuosa, ha sido sustituida por una nueva tarjeta. Los datos que figuran en la nueva tarjeta son los mismos, con excepción del índice de sustitución del número de la tarjeta, que se incrementa en una unidad.

Renovada	La tarjeta de tacógrafo ha sido renovada debido a un cambio de los datos administrativos o a la expiración del período de validez. El número de tarjeta de la tarjeta nueva es el mismo, con la excepción del índice de renovación del número de tarjeta, que se incrementa en una unidad.
En trámite de intercambio	La autoridad expedidora de la tarjeta que ha expedido una tarjeta de conductor ha recibido la notificación de que se ha iniciado el procedimiento de intercambio de esa tarjeta por otra tarjeta de conductor expedida por la autoridad expedidora de las tarjetas de otra Parte.
Intercambiada	La autoridad expedidora de la tarjeta que ha expedido una tarjeta de conductor ha recibido la notificación de que ha concluido el procedimiento de intercambio de esa tarjeta por otra tarjeta de conductor expedida por la autoridad expedidora de las tarjetas de otra Parte.

Subapéndice 4.3

Disposiciones relativas a los mensajes de TACHOnet

1. Requisitos técnicos generales

1.1. El nodo central dispondrá de interfaces síncronas y asíncronas para el intercambio de mensajes. Las Partes podrán elegir la tecnología más adecuada para interactuar con sus propias aplicaciones.

1.2. Todos los mensajes intercambiados entre el nodo central y los sistemas nacionales deben estar codificados en UTF-8.

1.3. Los sistemas nacionales deberán poder recibir y procesar mensajes que contengan caracteres cirílicos o griegos.

2. Estructura de los mensajes XML y definición del esquema (XSD)

2.1. La estructura general de los mensajes XML se ajustará al formato definido por los esquemas XSD instalados en el nodo central.

2.2. El nodo central y los sistemas nacionales transmitirán y recibirán mensajes que se ajusten al esquema de mensajes XSD.

2.3. Los sistemas nacionales deberán poder enviar, recibir y tratar todos los mensajes correspondientes a cualquiera de las funcionalidades establecidas en el subapéndice 4.2.

2.4. Los mensajes XML incluirán al menos los requisitos mínimos establecidos en el cuadro 2.

Cuadro 2

Requisitos mínimos en relación con contenido de los mensajes XML

Encabezamiento común		**Obligatorio**
Versión	La versión oficial de las especificaciones XML se indicará a través del espacio de nombres («namespace») definido en el mensaje XSD y en el atributo versión del elemento «encabezamiento» de cualquier mensaje XML. El número de versión («n.m») se definirá como valor fijo en cada versión del fichero XLM Schema Definition (fichero de definiciones del esquema XML) (xsd).	Sí
Identificador de ensayo	ID opcional para ensayo. El originador del ensayo introducirá los datos en el ID y todos los participantes en el flujo de trabajo enviarán/devolverán el mismo ID. Debe omitirse en la producción y no se utilizará si se suministra.	No
Identificador técnico	Un UUID de identificación única de cada mensaje. El remitente genera un UUID e introduce los datos en este atributo. Estos datos no se utilizan para fines de capacidad empresarial.	Sí
Identificador de flujo de trabajo	EL ID del flujo de trabajo («workflowId») es un UUID y debe ser generado por la Parte solicitante. Este ID se utilizará en todos los mensajes para correlacionar el flujo de trabajo.	Sí
Enviado el	La fecha y hora (UTC) en que el mensaje ha sido enviado.	Sí
Tiempo de espera agotado	Atributo opcional de fecha y hora (en formato UTC). Este valor será fijado solamente por el nodo central para las solicitudes enviadas. Informará a la Parte que responde del momento en que el tiempo de espera de la solicitud se haya rebasado. Este valor no es obligatorio en MS2TCN_<x>_Req ni en ningún mensaje de respuesta. Es opcional para que la misma definición de encabezamiento pueda utilizarse en todos los tipos de mensaje independientemente de si se requiere o no el atributo Valor de tiempo de espera agotado.	No
De	El código ISO 3166-1 alfa 2 de la Parte que envía el mensaje o «EU».	Sí
To	El código ISO 3166-1 alfa 2 de la Parte a la que se envía el mensaje o «EU».	Sí

Subapéndice 4.4

Transliteración y Servicios NYSIIS (New York State Identification and Intelligence System)

1. El algoritmo NYSIIS aplicado en el nodo central se utilizará para codificar los nombres de todos los conductores en el registro nacional.

2. Cuando se realice la búsqueda de una tarjeta a través de la funcionalidad CIC, se utilizarán las claves NYSIIS como mecanismo de búsqueda primaria.

3. Además, las Partes podrán emplear un algoritmo personalizado para obtener resultados adicionales.

4. Los resultados de las búsquedas indicarán el mecanismo de búsqueda que se ha utilizado para comprobar un registro, ya sea NYSIIS o personalizado.

5. Si una Parte decide registrar notificaciones ICDL, las claves NYSIIS incluidas en la notificación se registrarán como parte de los datos ICDL. Cuando se realice una búsqueda de datos ICDL, la Parte utilizará las claves NYSIIS del nombre del solicitante.

Subapéndice 4.5

Requisitos de seguridad

1. Para el intercambio de mensajes entre el nodo central y los sistemas nacionales se utilizará HTTPS.

2. Los sistemas nacionales utilizarán los certificados digitales mencionados en los subapéndices 4.8 y 4.9 a los efectos de proteger la transmisión de mensajes entre el sistema nacional y el nodo central.

3. Los sistemas nacionales aplicarán, como mínimo, certificados que utilicen el algoritmo de firma hash SHA-2 (SHA-256) y una clave pública de 2048 bits de longitud.

Subapéndice 4.6

Niveles de servicio

1. Los sistemas nacionales deberán prestar los siguientes niveles de servicio mínimos:

1.1. Estarán disponibles 24 horas al día, 7 días a la semana.

1.2. Su disponibilidad será supervisada por un mensaje automático «heartbeat» enviado desde el nodo central.

1.3. Su tasa de disponibilidad será del 98 % de acuerdo con la tabla siguiente (las cifras se han redondeado a la unidad conveniente más próxima):

Una disponibilidad del	significa que el sistema no está disponible		
	diariamente	mensualmente	anualmente
98 %	0,5 horas	15 horas	7,5 días

Se insta a las Partes a respetar la tasa de disponibilidad diaria, si bien se reconoce que determinadas actividades necesarias, como el mantenimiento del sistema, exigen un tiempo de indisponibilidad superior a 30 minutos. No obstante, las tasas de disponibilidad mensual y anual siguen siendo obligatorias.

1.4. Deberán responder como mínimo al 98 % de las solicitudes que se les envíen en un mes natural.

1.5. Deberán responder a las solicitudes en un plazo máximo de 10 segundos.

1.6. El tiempo global antes de la desconexión de la solicitud (el tiempo que el solicitante puede esperar una respuesta) no deberá superar los 20 segundos.

1.7. Tendrán capacidad para tramitar solicitudes a un ritmo de 6 mensajes por segundo.

1.8. Los sistemas nacionales no podrán enviar solicitudes al nodo central de TACHOnet a un ritmo superior a 2 solicitudes por segundo.

1.9. Cada sistema nacional deberá poder hacer frente a posibles problemas técnicos del nodo central o de los sistemas nacionales de otras Partes. Se incluyen aquí, entre otros:

a) pérdida de conexión con el nodo central;

b) falta de respuesta a una solicitud;

c) recepción de respuestas después del tiempo fijado de espera del mensaje;

d) recepción de mensajes no solicitados;

e) recepción de mensajes no válidos.

2. El nodo central:

2.1. presentará una tasa de disponibilidad del 98 %;

2.2. facilitará a los sistemas nacionales la notificación de cualquier error, bien a través del mensaje de respuesta, bien mediante un mensaje de error específico. Los sistemas nacionales, a su vez, recibirán dichos mensajes de error específicos y estarán dotados de un flujo de trabajo progresivo a fin de adoptar las medidas adecuadas para rectificar el error notificado.

3. Mantenimiento

Las Partes notificarán a las demás Partes y a la Comisión Europea cualquier actividad de mantenimiento rutinaria a través de la aplicación web, como mínimo una semana antes del comienzo de dicha actividad, si es técnicamente posible.

Subapéndice 4.7

Registro y estadísticas de los datos recopilados en el nodo central

1. A fin de garantizar la protección de la vida privada, los datos recopilados a efectos estadísticos serán anónimos. Los datos que identifiquen una tarjeta, un conductor o un permiso de conducción específicos no podrán utilizarse para fines estadísticos.

2. La información de registro conservará constancia de todas las transacciones con fines de seguimiento o depuración y permitirá generar estadísticas sobre dichas transacciones.

3. Los datos personales no se conservarán en los registros durante más de 6 meses. La información estadística se conservará indefinidamente.

4. Los datos estadísticos utilizados para los informes incluirán:

   a) la Parte solicitante;

   b) la Parte que responde;

   c) el tipo de mensaje;

   d) el código de estado de la respuesta;

   e) la fecha y hora de los mensajes;

   f) el tiempo de respuesta.

Subapéndice 4.8

Disposiciones generales relativas a las claves y certificados digitales destinados a TACHOnet

1. La Dirección General de Informática de la Comisión Europea (DIGIT) pondrá un servicio PKI [1](denominado en lo sucesivo «servicio CEF PKI» por sus siglas en inglés) a disposición de las Partes Contratantes en el AETR que se conecten a TACHOnet (en lo sucesivo, las autoridades nacionales) a través de eDelivery.

2. En el apéndice se definen el procedimiento de solicitud y revocación de certificados digitales, así como las condiciones detalladas para su uso.

3. Utilización de certificados:

3.1. Una vez expedido el certificado,[2], la autoridad nacional lo utilizará únicamente en el contexto de TACHOnet. El certificado puede utilizarse para:

a) autenticar la procedencia de los datos;

b) encriptar los datos;

c) garantizar la detección de las violaciones de integridad de los datos.

3.2. Queda prohibido todo uso no autorizado expresamente dentro de los usos permitidos del certificado.

4. Las Partes Contratantes deberán:

a) proteger su clave privada contra usos no autorizados;

b) abstenerse de transferir o revelar su clave privada a terceros, ni siquiera en calidad de representantes;

---

1 Una PKI (infraestructura de clave pública) es el conjunto de funciones, políticas, procedimientos y sistemas necesarios para crear, gestionar, distribuir y revocar certificados digitales.

2 Identificado por el valor de atributo «O=» en el Nombre Distintivo de Firmante (Subject Distinguished Name) del certificado expedido

c) garantizar la confidencialidad, integridad y disponibilidad de las claves privadas generadas, almacenadas y utilizadas en TACHOnet;

d) abstenerse de hacer uso continuado de la clave privada tras la expiración del período de validez o la revocación del certificado, salvo para visualizar datos encriptados (por ejemplo, descifrar correos electrónicos); las claves expiradas se destruirán o se conservarán de forma que no puedan utilizarse;

e) comunicar a la autoridad de registro la identidad de los representantes autorizados a solicitar la revocación de los certificados expedidos a la organización (las solicitudes de revocación deberán incluir una contraseña de solicitud de revocación y pormenores sobre los hechos que han dado lugar a la misma);

f) prevenir el uso indebido de la clave privada solicitando la revocación del certificado de clave pública correspondiente en caso de que se vean comprometidos la clave privada o los datos de activación de la clave privada;

g) ser responsables y tener la obligación de solicitar la revocación del certificado en las circunstancias indicadas en las políticas de certificación (CP) y la declaración de prácticas de certificación (CPS) de la autoridad de certificación;

h) notificar sin demora a la autoridad de registro la pérdida, el robo o la posible situación de riesgo de las claves AETR utilizadas en el contexto de TACHOnet.

5. Responsabilidad

Sin perjuicio de la responsabilidad de la Comisión Europea en contravención de cualesquiera requisitos establecidos en la legislación nacional aplicable o con respecto a la responsabilidad por cuestiones que no puedan ser excluidas en virtud de dicha legislación, la Comisión Europea no será responsable con respecto:

a) al contenido del certificado, del que es únicamente responsable su titular; corresponderá a dicho titular comprobar la exactitud del contenido del certificado;

b) al uso del certificado por parte de su titular.

Subapéndice 4.9

Descripción del servicio PKI para TACHOnet

1. Introducción

Una PKI (infraestructura de clave pública) es el conjunto de funciones, políticas, procedimientos y sistemas necesarios para crear, gestionar, distribuir y[3]. El servicio CEF PKI de eDelivery permite la expedición y gestión de certificados digitales utilizados para garantizar la confidencialidad, la integridad y el no repudio de la información intercambiada entre los puntos de acceso.

El servicio PKI de eDelivery se basa en Trust Center Services TeleSec Shared Business CA (autoridad de certificación), a la que son aplicables la política de certificación y la declaración de prácticas de certificación de TeleSec Shared-Business-CA de T-Systems International GmbHT-Systems International GmbH[4].

El servicio PKI expide certificados apropiados para garantizar la seguridad de diversos procesos empresariales dentro y fuera de las empresas, organizaciones, autoridades públicas e instituciones que requieren un nivel de seguridad medio para demostrar la autenticidad, integridad y fiabilidad de la entidad final.

2. Proceso de solicitud de certificados

2.1. Funciones y responsabilidades

2.1.1. «Organización» o «autoridad nacional» que solicita el certificado

2.1.1.1. La autoridad nacional solicitará los certificados en el contexto del proyecto TACHOnet.

2.1.1.2 La autoridad nacional:

a) solicitará los certificados al servicio CEF PKI;

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

La última versión de la política de certificación y la declaración de prácticas de certificación puede descargarse en https://www.telesec.de/en/sbca-en/support/download-area/

b) generará las claves privadas y las claves públicas correspondientes que deben incluirse en los certificados expedidos por la autoridad de certificación;

c) descargará el certificado en cuanto este sea aprobado;

d) firmará y remitirá de nuevo a la autoridad de registro:

i) el formulario de identificación de personas de contacto y mensajeros de confianza,

ii) el poder individual firmado[5].

2.1.2. Mensajero de confianza

2.1.2.1. La autoridad nacional designará a un mensajero de confianza.

2.1.2.2. El mensajero de confianza:

a) entregará la clave pública a la autoridad de registro durante un proceso de identificación y registro presencial;

b) obtendrá el certificado correspondiente de la autoridad de registro.

2.1.3. Titular del dominio

2.1.3.1. El titular del dominio será la DG MOVE.

2.1.3.2. El titular del dominio:

a) validará y coordinará la red TACHOnet y la arquitectura de confianza de TACHOnet, incluida la validación de los procedimientos para la expedición de certificados;

b) gestionará el nodo central de TACHOnet y coordinará la actividad de las Partes en lo que respecta al funcionamiento de TACHOnet;

c) llevará a cabo, junto con las autoridades nacionales, los ensayos de conexión a TACHOnet.

---

5 Un poder es un documento jurídico por el que la organización faculta y autoriza a la Comisión Europea, representada por el funcionario designado responsable del servicio CEF PKI, a solicitar en su nombre la generación de un certificado a T-Systems International GmbH TeleSec Shared Business CA. Véase también el punto 6 Véase el punto 6.

2.1.4. Autoridad de registro

2.1.4.1. La autoridad de registro será el Centro Común de Investigación (JRC).

2.1.4.2. La autoridad de registro se encargará de verificar la identidad del mensajero de confianza y de registrar y aprobar las solicitudes de expedición, revocación y renovación de los certificados digitales.

2.1.4.3. La autoridad de registro:

a) asignará el identificador único a la autoridad nacional;

b) autenticará la identidad de la autoridad nacional, sus puntos de contacto y sus mensajeros de confianza;

c) se comunicará con el servicio de apoyo del CEF en relación con la autenticidad de la autoridad nacional, sus puntos de contacto y sus mensajeros de confianza;

d) informará a la autoridad nacional de la aprobación o desestimación del certificado.

2.1.5. Autoridad de certificación

2.1.5.1. La autoridad de certificación se encargará del suministro de la infraestructura técnica para la solicitud, expedición y revocación de los certificados digitales.

2.1.5.2. La autoridad de certificación:

a) facilitará la infraestructura técnica necesaria para que las autoridades nacionales puedan solicitar certificados;

b) validará o desestimará las solicitudes de certificado;

c) se comunicará con la autoridad de registro para verificar la identidad de la organización solicitante, cuando sea necesario.

2.2. Expedición de certificados

2.2.1. La expedición de certificados se llevará a cabo con arreglo a las siguientes etapas secuenciales, representadas en la figura 1:

a) **Etapa 1:** Identificación del mensajero de confianza

b) **Etapa 2:** Creación de la solicitud de certificado

c) **Etapa 3:** Registro ante la autoridad de registro

d) **Etapa 4:** Generación del certificado

e) **Etapa 5:** Publicación del certificado

f) **Etapa 6:** Aceptación del certificado

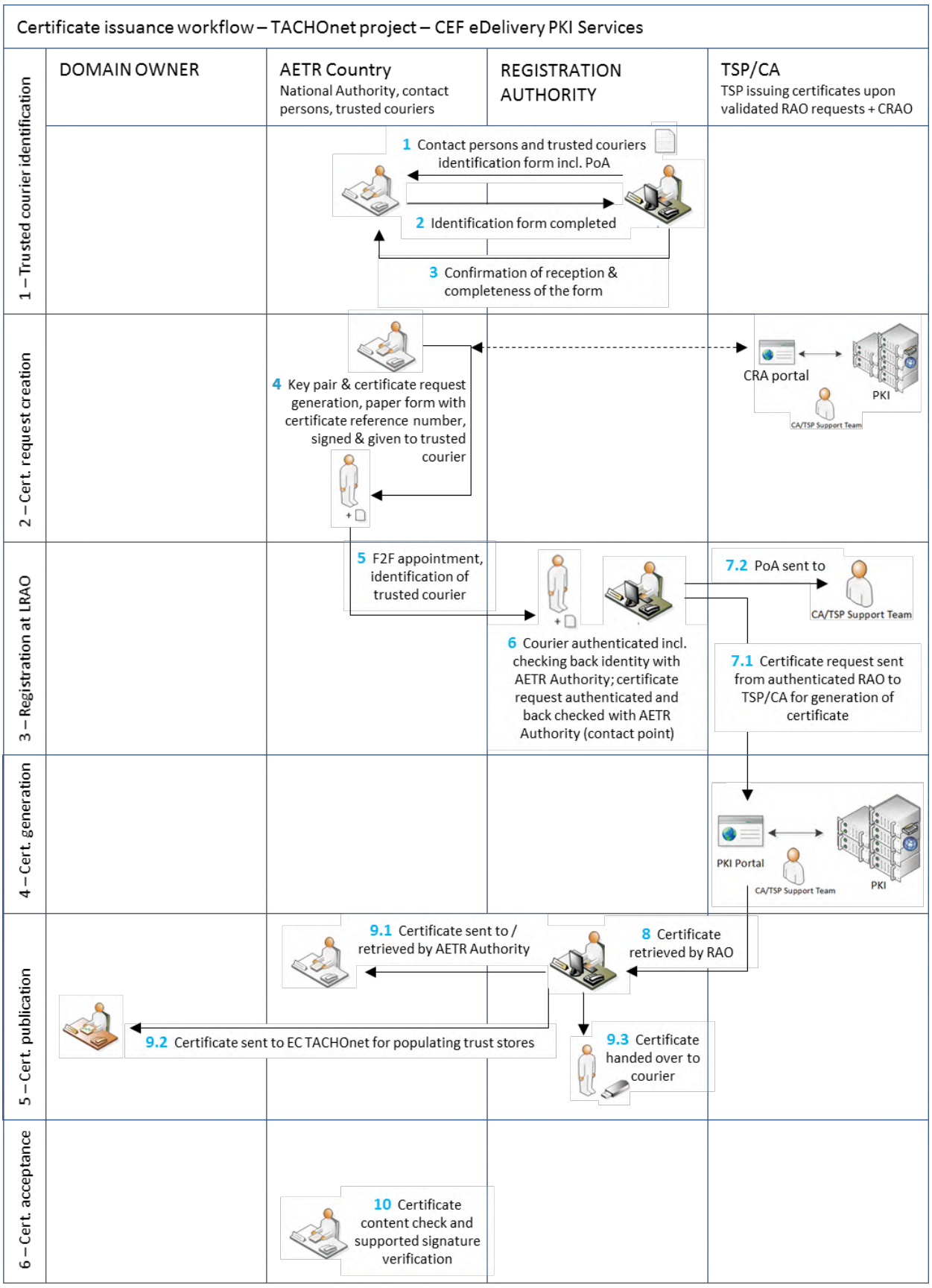


Figura 1 - Flujo de expedición de certificados

2.2.2. Etapa 1: Identificación del mensajero de confianza

Se seguirá el siguiente proceso para identificar al mensajero de confianza:

a) La autoridad de registro enviará a la autoridad nacional el formulario de identificación de las personas de contacto y los mensajeros de confianza[6]. Dicho formulario también incluirá un poder que deberá firmar la organización (autoridad AETR).

b) La autoridad nacional devolverá el formulario cumplimentado y el poder firmado a la autoridad de registro.

c) La autoridad de registro acusará recibo de la correcta recepción y la integridad del formulario.

d) La autoridad de registro facilitará al titular del dominio una copia actualizada de la lista de personas de contacto y de mensajeros de confianza.

2.2.3. Etapa 2: Creación de la solicitud de certificado

2.2.3.1. La solicitud y la recuperación del certificado se efectuarán en el mismo ordenador y con el mismo navegador.

2.2.3.2. Se seguirá el siguiente proceso para crear la solicitud de certificado:

a) Desde la interfaz web del usuario, la organización solicitará el certificado a través de la URL https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en, introduciendo el nombre de usuario «sbca/CEF_eDelivery.europa.eu» y la contraseña «digit.333». introduciendo el nombre de usuario‘ **«sbca/CEF_eDelivery.europa.eu»** y la contraseña **«digit.333»**’.

[6]Véase el punto 5.

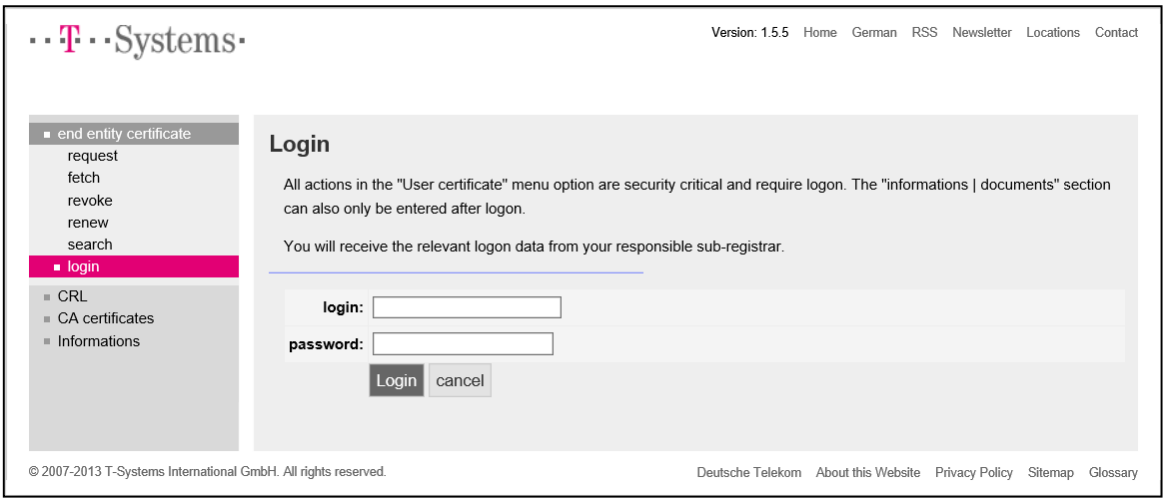


Figura 2

b) La organización hará clic en «request» (solicitar) en el lado izquierdo de la pantalla y seleccionará «CEF_TACHOnet» en la lista desplegable.

Figura 3

c) La organización completará el formulario de solicitud de certificado de la figura 4 con la información del cuadro 3, haciendo clic en «Next (soft-PSE)» para terminar el proceso.

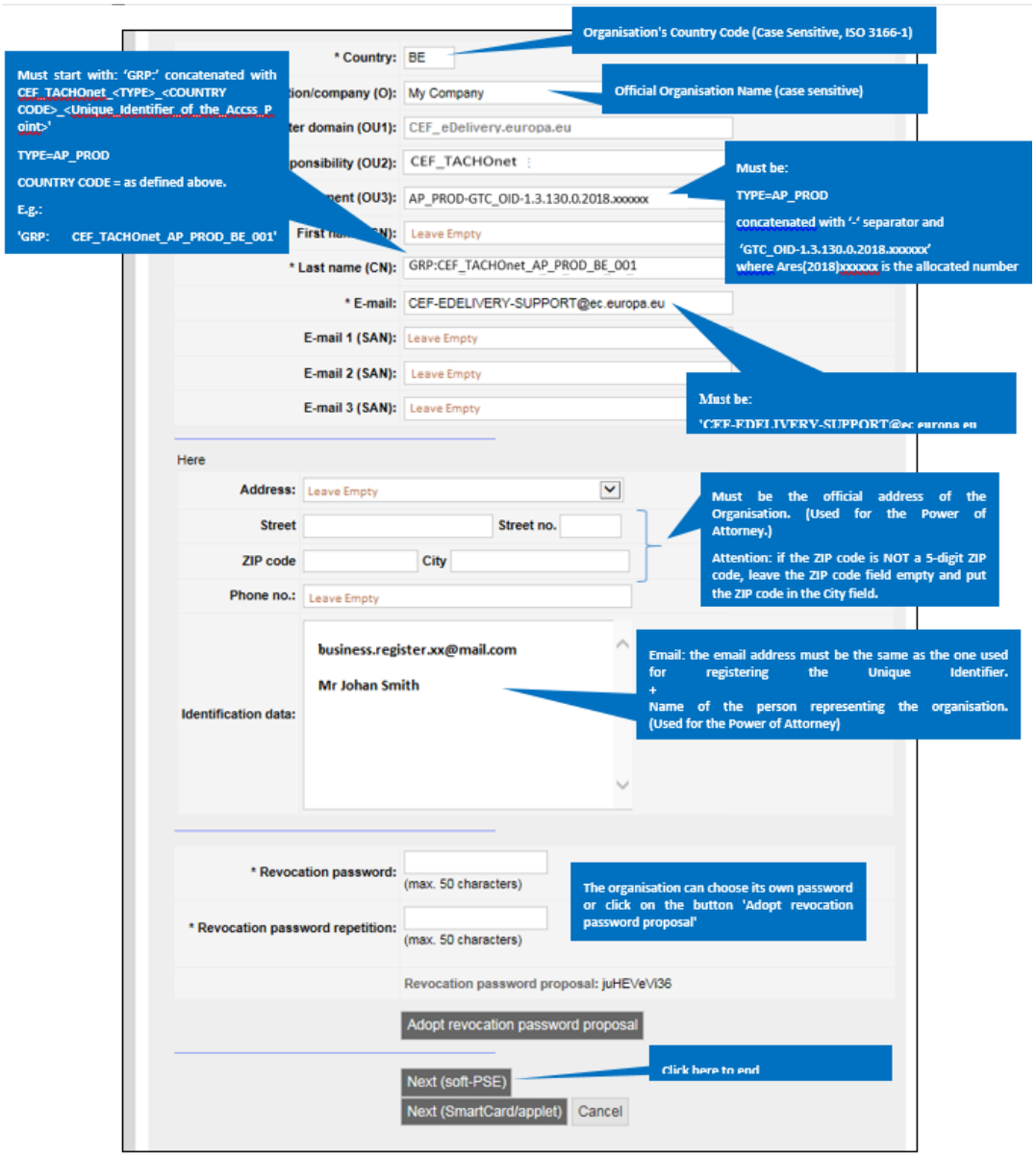

Organisation's Country Code (Case Sensitive, ISO 3166-1)
Official Organisation Name (case sensitive)
Must start with: 'GRP:' concatenated with CEF_TACHOnet_<TYPE>_<COUNTRY CODE>_<Unique_Identifier_of_the_Accss_Point>'
TYPE=AP_PROD
COUNTRY CODE = as defined above.
E.g.:
'GRP: CEF_TACHOnet_AP_PROD_BE_001'
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

Campos obligatorios	Descripción
Country (país)	**C=Código de país**, localización del titular del certificado, verificada mediante una guía pública. Restricciones: 2 caracteres, conforme a la norma ISO 3166-1, alfa-2, distinción entre mayúsculas y minúsculas; ejemplos: DE, BE, NL, Casos específicos: UK (para Gran Bretaña), EL (para Grecia)
Organisation/Company (O) (organización/empresa)	**O = Nombre de la organización del titular del certificado**
Master domain (OU1) (dominio maestro)	**OU=CEF_eDelivery.europa.eu**
Area of responsibility (OU2) (ámbito de responsabilidad)	**OU=CEF_TACHOnet**
Department (OU3) (departamento)	Valor obligatorio por «AREA OF RESPONSIBILITY» El contenido deberá comprobarse utilizando una lista positiva (lista blanca) en el momento de solicitar el certificado. Si la información no se corresponde con la lista, se impedirá la presentación de la solicitud. Formato: **OU=<TYPE>-<GTC_NUMBER>** Donde «<TYPE>» se sustituye por AP_PROD: Access Point in Production environment (punto de acceso en entorno de producción), y donde <GTC_NUMBER> es **GTC_OID-1.3.130.0.2018.xxxxxx,**, donde Ares(2018)xxxxxx es el n.º GTC del proyecto TACHOnet. Por ejemplo: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First name (CN) (nombre)	Debe estar vacío
Last name (CN) (apellidos)	Debe comenzar por «GRP», seguido de un nombre común. Formato: **CN=GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** Por ejemplo: GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail (correo electrónico)	**E=CEF-EDELIVERY-SUPPORT@ec.europa.eu**
E-mail 1 (SAN)	Debe estar vacío
E-mail 2 (SAN)	Debe estar vacío
E-mail 3 (SAN)	Debe estar vacío

Dirección	Debe estar vacío
Street (calle)	Debe ser la dirección oficial de la organización del titular del certificado (la que figura en el poder).
Street no (n.º calle)	Debe ser la dirección oficial de la organización del titular del certificado (la que figura en el poder).
Zip Code (código postal)	Debe ser la dirección oficial de la organización del titular del certificado (la que figura en el poder). **Atención**:Si el código postal NO tiene 5 dígitos, déjese en blanco e insértese en el campo correspondiente a la localidad.
City (localidad)	Debe ser la dirección oficial de la organización del titular del certificado (la que figura en el poder). **Atención**:Si el código postal NO tiene 5 dígitos, déjese en blanco e insértese en el campo correspondiente a la localidad.
Phone no (n.º de teléfono)	Debe estar vacío
Identification data (datos de identificación)	La dirección de correo electrónico debe ser la misma que la utilizada para registrar el identificador único. + Debe ser el nombre de la persona que representa a la organización (la que figura en el poder). + **N.º registro mercantil** (obligatorio solo para organizaciones privadas) **Inscrito en el tribunal cantonal de** (obligatorio solo para organizaciones privadas de Alemania y Austria)
Revocation password (contraseña de revocación)	Campo obligatorio elegido por el solicitante
Revocation password repetition (repetición de la contraseña de revocación)	Repetición del campo obligatorio elegido por el solicitante

Cuadro 3. Detalles completos de cada campo solicitado

d) La longitud de la clave seleccionada será de 2048 (grado alto).

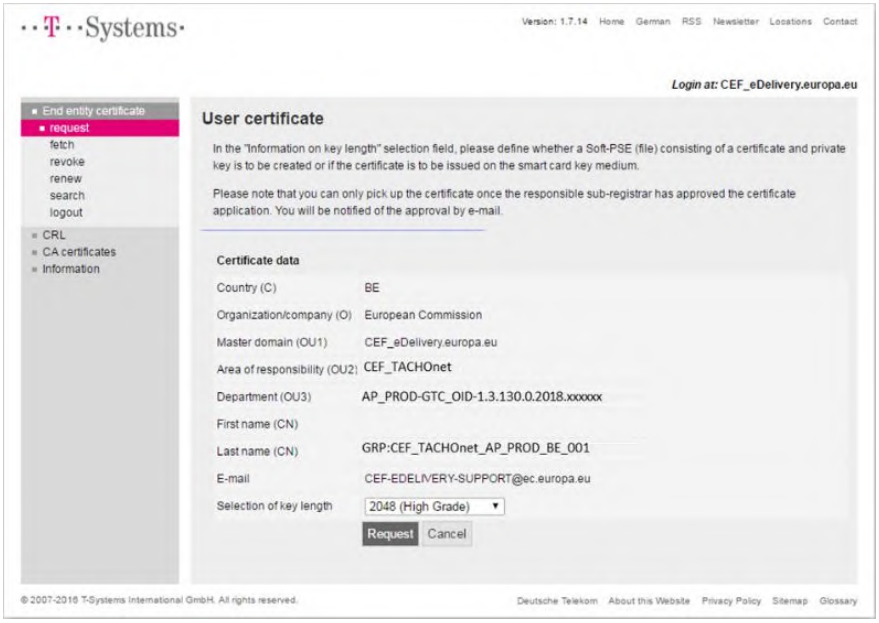


Figura 5

e) La organización registrará el número de referencia para recuperar el certificado.

Figura 6

f) El equipo de apoyo del CEF comprobará las nuevas solicitudes de certificado y verificará si la información incluida en la solicitud de certificado es válida, es decir, si se ajusta a la convención de nomenclatura que se especifica en el apéndice 5.1 (Convención de nomenclatura de certificados).

g) El equipo de apoyo del CEF comprobará que la información incluida en la solicitud se facilita en un formato válido.

h) Si el control de los puntos 5 o 6 anteriores arroja resultados negativos, el equipo de apoyo del CEF enviará un correo electrónico a la dirección de correo electrónico indicada en los «Datos de identificación» del formulario de solicitud, con copia al titular del dominio, en el que solicitará a la organización que inicie de nuevo el proceso. La solicitud de certificado defectuosa quedará anulada.

i) El equipo de apoyo del CEF enviará un correo electrónico a la autoridad de registro acerca de la validez de la solicitud. El correo electrónico incluirá:

(1) el nombre de la organización, disponible en el campo «Organisation (O)» de la solicitud de certificado;

(2) los datos del certificado, incluido el nombre del punto de acceso para el que debe expedirse el certificado, disponible en el campo «Last Name (CN)» de la solicitud de certificado;

(3) el número de referencia del certificado;

(4) la dirección de la organización, su correo electrónico y el nombre de la persona que la representa.

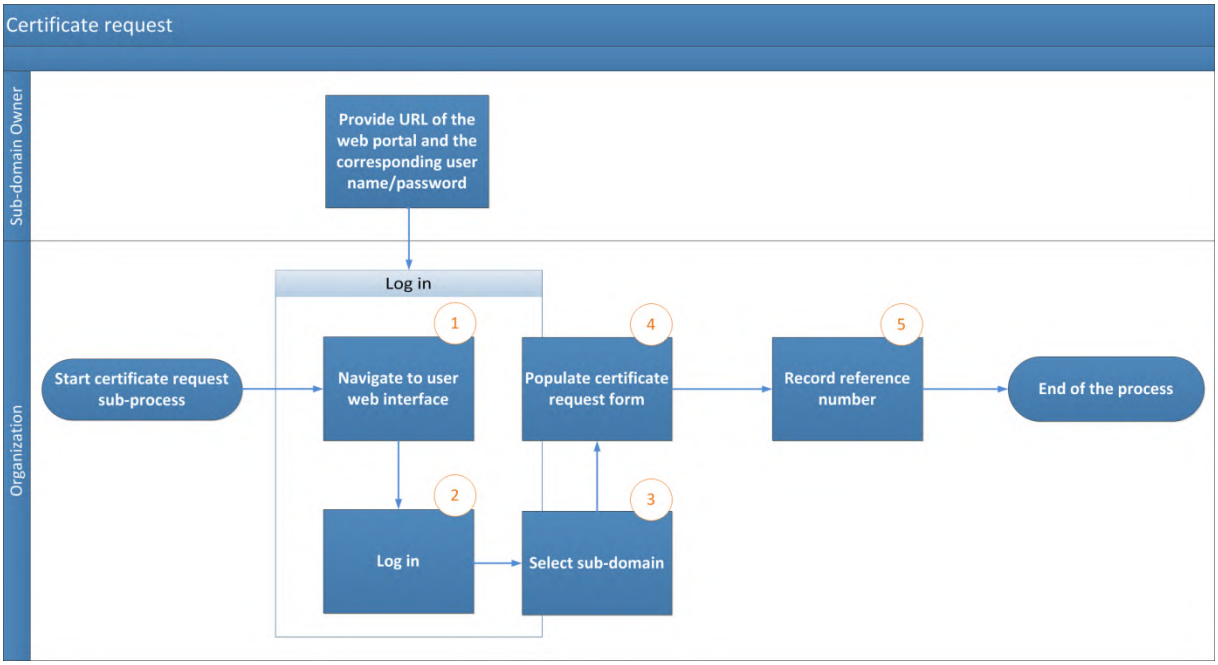


Figura 7 – Proceso de solicitud de certificados

2.2.4. Etapa 3: Registro ante la autoridad de registro (aprobación del certificado)

2.2.4.1. El mensajero de confianza o el punto de contacto concertará una cita con la autoridad de registro por correo electrónico, indicando la identidad del mensajero de confianza que asistirá a la reunión presencial.

2.2.4.2. La organización preparará la documentación, que consistirá en:

a) el poder, cumplimentado y firmado;

b) una copia del pasaporte válido del mensajero de confianza que asistirá a la reunión presencial; esta copia deberá estar firmada por uno de los puntos de contacto identificados de la organización en la etapa 1;

c) el formulario de solicitud de certificado en papel, firmado por uno de los puntos de contacto de la organización.

2.2.4.3. La autoridad de registro recibirá al mensajero de confianza, que previamente se someterá a un control de identidad en la recepción del edificio. La autoridad de registro llevará a cabo el registro presencial de la solicitud de certificado:

a) identificando y autenticando al mensajero de confianza;

b) comprobando que la apariencia física del mensajero de confianza se corresponde con la fotografía de su pasaporte;

c) comprobando la validez del pasaporte presentado por el mensajero de confianza;

d) cotejando el pasaporte validado presentado por el mensajero de confianza y la copia del pasaporte válido del mensajero de confianza firmada por uno de los puntos de contacto identificados de la organización; la firma se autenticará cotejándola con el «formulario de identificación de mensajeros de confianza y puntos de contacto» original;

e) comprobando el poder cumplimentado y firmado;

f) cotejando el formulario de solicitud de certificado en papel y su firma con el «formulario de identificación de mensajeros de confianza y puntos de contacto» original;

g) llamando al punto de contacto firmante para comprobar de nuevo la identidad del mensajero de confianza y el contenido de la solicitud de certificado.

2.2.4.4. La autoridad de registro confirmará al equipo de apoyo del CEF que la autoridad nacional está efectivamente autorizada para explotar los componentes para los que solicita los certificados y que el correspondiente proceso de registro presencial se ha realizado satisfactoriamente. La confirmación se enviará mediante un correo electrónico seguro del certificado «CommiSign», al que se adjuntará una copia escaneada de la documentación autenticada presencialmente y de la lista de comprobación del proceso firmada y realizada por la autoridad de registro.

2.2.4.5. Si la autoridad de registro confirma la validez de la solicitud, el proceso continuará con arreglo a lo establecido en los apartados 2.2.4.6 y 2.2.4.7. En caso contrario, se denegará la expedición del certificado y se informará a la organización.

2.2.4.6. El equipo de apoyo del CEF aprobará la solicitud de certificado y notificará a la autoridad de registro la aprobación del certificado.

2.2.4.7. La autoridad de registro notificará a la organización que el certificado puede recuperarse a través del portal del usuario.

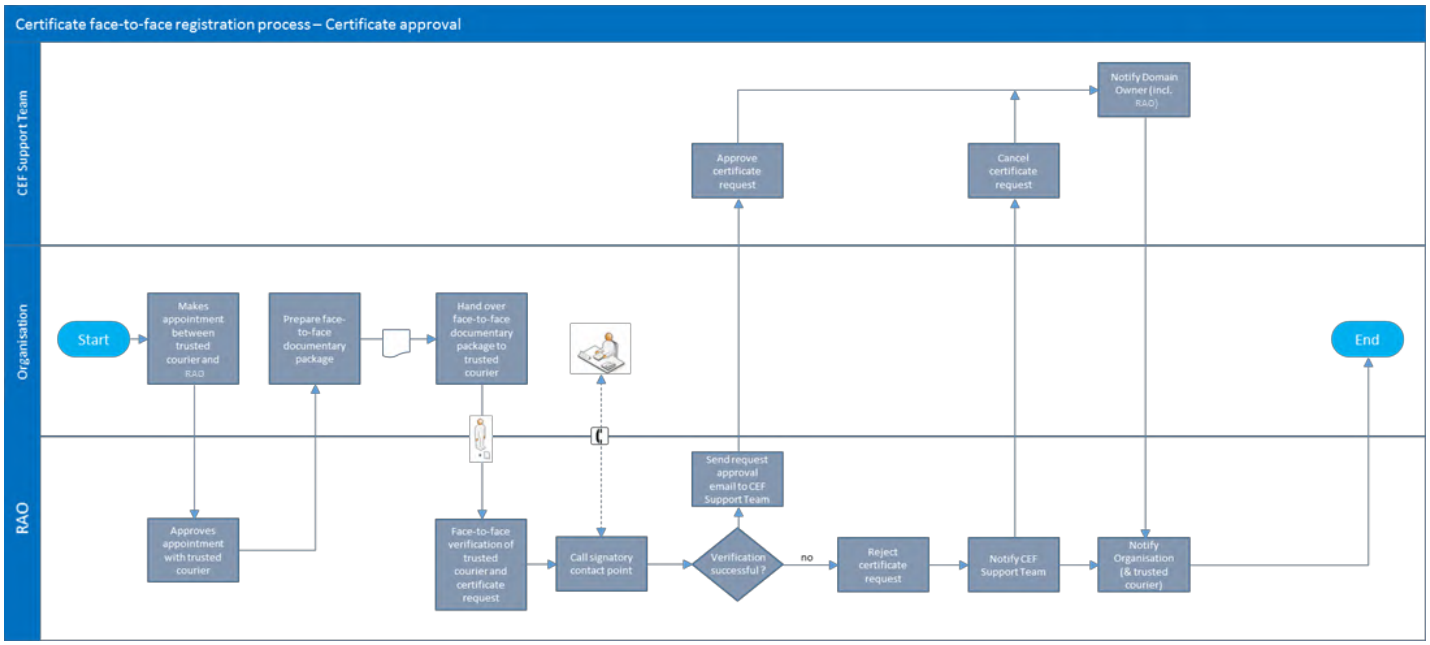


Figura 8 — Aprobación del certificado

2.2.5. Etapa 4: Generación del certificado

Una vez aprobada la solicitud de certificado, se procederá a generar el certificado.

2.2.6. Etapa 5: Publicación y recuperación de certificados

2.2.6.1. Tras la aprobación de la solicitud de certificado, la autoridad de registro recuperará el certificado y entregará una copia del mismo al mensajero de confianza.

2.2.6.2. La autoridad de registro notificará a la organización que puede recuperar los certificados.

2.2.6.3. Desde el portal del usuario en https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en la organización iniciará sesión con el nombre de usuario «**sbca/CEF_eDelivery.europa.eu**» y la contraseña «**digit.333**».

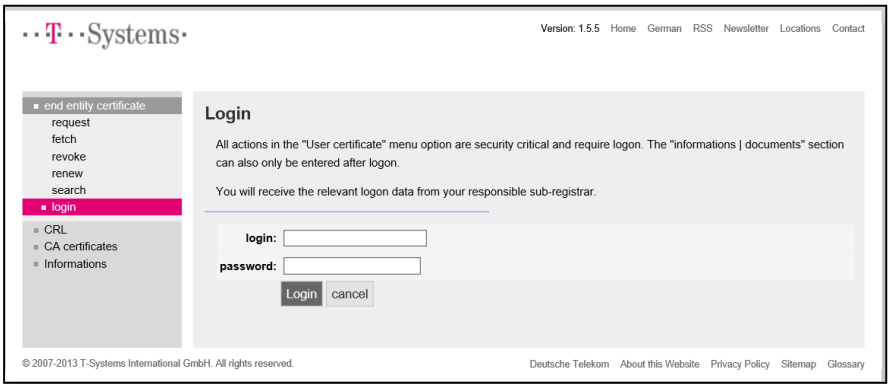


Figura 9

2.2.6.4. La organización pulsará el botón «fetch» de la parte izquierda e introducirá el número de referencia registrado durante el proceso de solicitud del certificado.

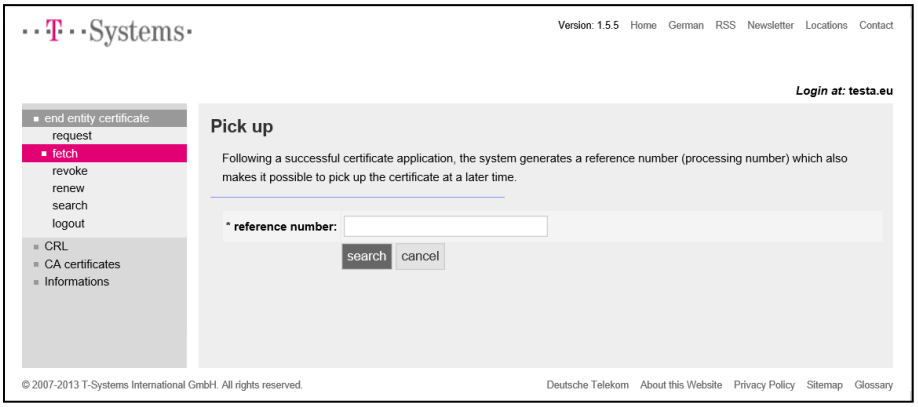


Figura 10

2.2.6.5. La organización instalará los certificados pulsando el botón «install».

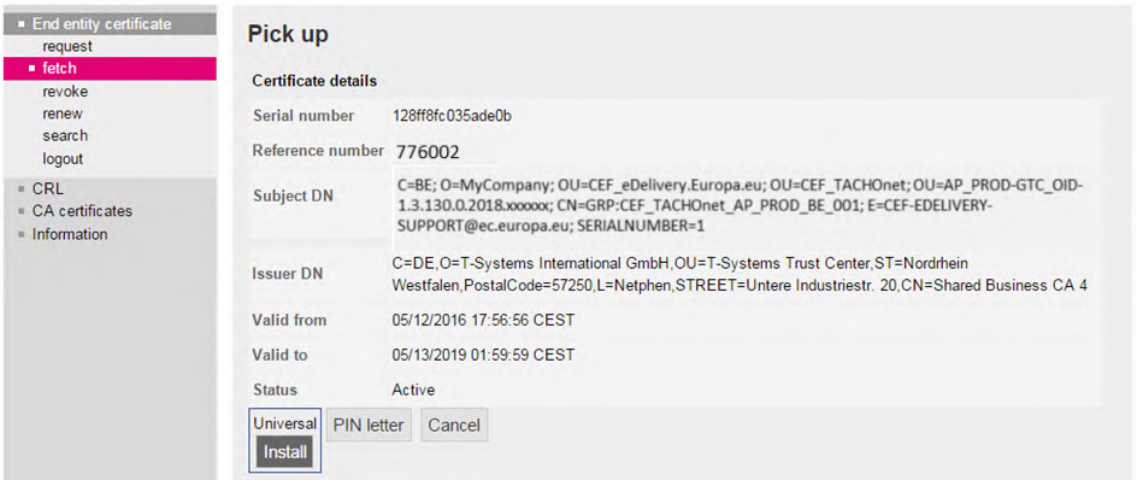


Figura 11

2.2.6.6. El certificado se instalará en el punto de acceso. Al tratarse de una instalación específica de la aplicación, la organización se remitirá a su proveedor de punto de acceso para obtener la descripción de este proceso.

2.2.6.7. Para la instalación de certificados en el punto de acceso deben seguirse los pasos siguientes:

a) exportar la clave privada y el certificado,

b) crear el almacén de claves y el almacén de confianza,

c) instalar el almacén de claves y el almacén de confianza en el punto de acceso.

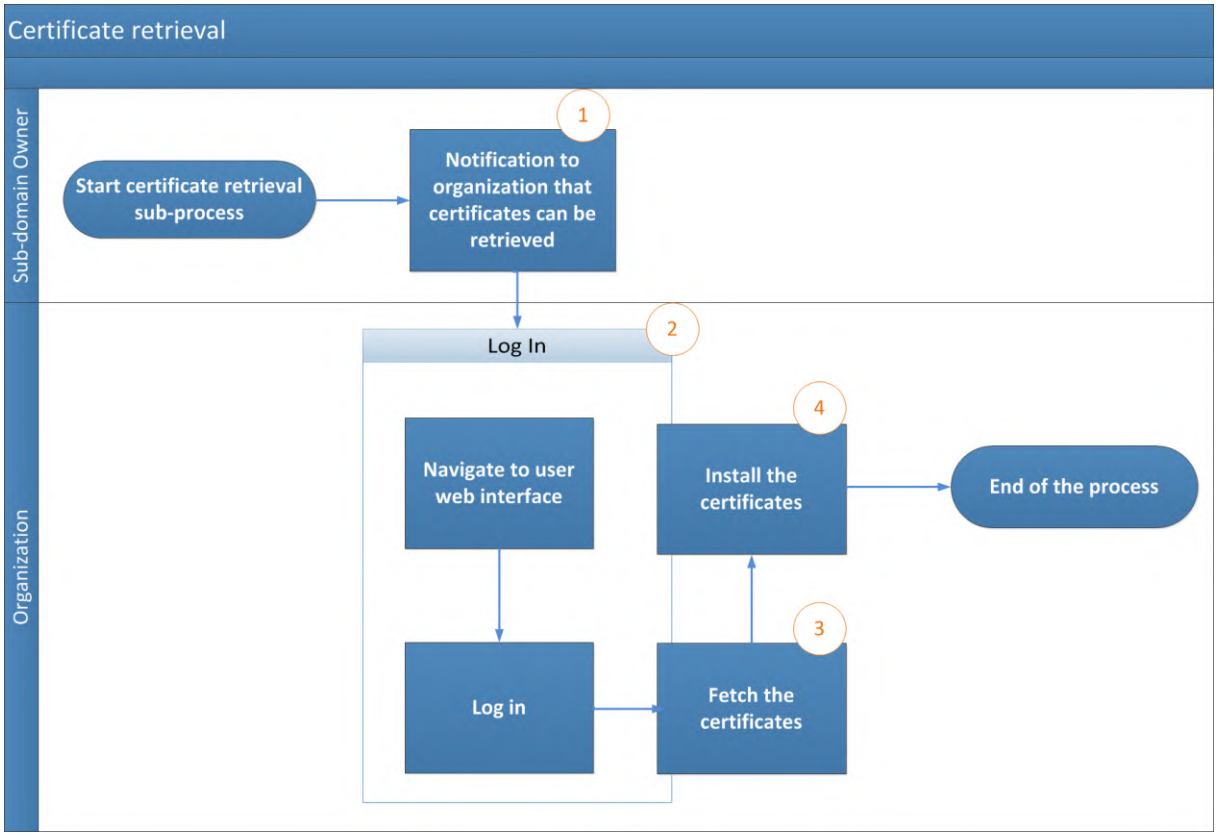


Figura 12 - Recuperación del certificado

3. Proceso de revocación de certificados

3.1. La organización presentará una solicitud de revocación a través del portal web de usuarios.

3.2. El equipo de apoyo del CEF ejecutará la revocación del certificado.

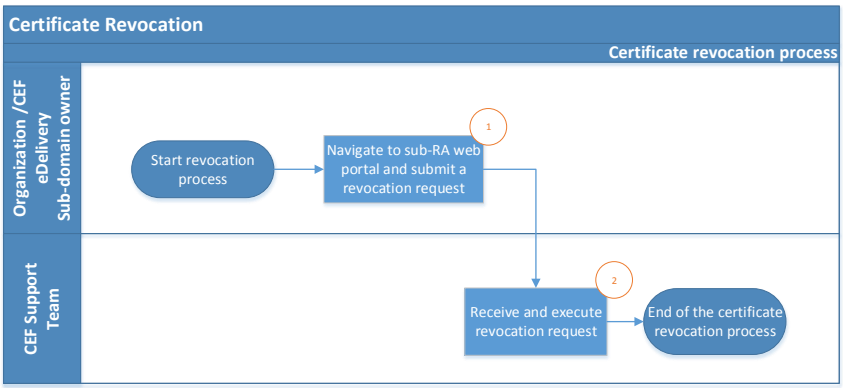


Figura 13 — Revocación del certificado

4. Condiciones generales del servicio CEF PKI

4.1. Contexto

En su calidad de proveedor de soluciones del módulo eDelivery del Mecanismo «Conectar Europa», la DG DIGIT pondrá a disposición de las Partes Contratantes en el AETR un servicio PKI [7](«servicio CEF PKI»). El servicio CEF PKI será utilizado por las autoridades nacionales («usuarios finales») que participan en TACHOnet.

La DG DIGIT utiliza el servicio de PKI en el marco de la solución TeleSec Shared-Business CA («SBCA»), operada en el centro de confianza de la unidad del grupo T-Systems International GmbH («T-Systems»[8]). La DG DIGIT desempeña la función de registrador principal del dominio «CEF_eDelivery.europa.eu» de la SBCA. En el desempeño de esta función, la DG DIGIT crea subdominios dentro del dominio «CEF_eDelivery.europa.eu» para cada proyecto que utiliza el servicio CEF PKI.

El presente documento contiene información detallada sobre las condiciones del subdominio TACHOnet. La DG DIGIT desempeña la función de subregistrador de este subdominio. En calidad de tal, expide, revoca y renueva los certificados de este proyecto.

4.2. Cláusula de exención de responsabilidad

La Comisión Europea no asume responsabilidad alguna en relación con el contenido del certificado, que recae exclusivamente en el titular del certificado. Corresponde a dicho titular comprobar la exactitud del contenido del certificado.

La Comisión Europea no asume responsabilidad alguna en relación con el uso del certificado por parte de su titular, puesto que este es una tercera entidad jurídica ajena a la Comisión Europea.

---

7 Una PKI (infraestructura de clave pública) es el conjunto de funciones, políticas, procedimientos y sistemas necesarios para crear, gestionar, distribuir y revocar certificados digitales.

8 La misión de confianza del operador del centro de confianza, situado en el centro de confianza de T-Systems, también incluye la función de autoridad de registro interno

La presente cláusula de exención de responsabilidad no tiene por objeto limitar la responsabilidad de la Comisión Europea en contravención de cualesquiera requisitos establecidos en la legislación nacional aplicable, ni excluir su responsabilidad en los casos en que no pueda excluirse en virtud de dicha legislación.

4.3. Usos autorizados o prohibidos de los certificados

4.3.1. Utilización autorizada de certificados

Una vez expedido el certificado,[9] su titular lo utilizará únicamente en el contexto de TACHOnet. En este contexto, el certificado puede utilizarse para:

- autenticar la procedencia de los datos;
- encriptar los datos;
- garantizar la detección de las violaciones de integridad de los datos.

4.3.2. Utilización prohibida de certificados

Queda prohibido todo uso no autorizado expresamente dentro de los usos permitidos del certificado.

4.4. Obligaciones adicionales del titular del certificado

T-Systems establece las condiciones detalladas de la SBCA en la política de certificación/declaración de prácticas de certificación (CP/CPS en sus siglas en inglés) del servicio SBCA[10]. Este documento incluye especificaciones de seguridad y directrices relativas a los aspectos técnicos y organizativos y describe las actividades del operador del centro de confianza en las funciones de autoridad de certificación (CA) y autoridad de registro (AR), así como de tercero delegado por la autoridad de registro.

Solo las entidades autorizadas para participar en TACHOnet pueden solicitar un certificado.

---

9 Identificado por el valor de atributo «O=» en el Nombre Distintivo de Firmante (Subject Distinguished Name) del certificado expedido

10 La versión más reciente de la CP/CPS del servicio SBCA de T-Systems está disponible en https://www.telesec.de/en/sbca-en/support/download-area/..

Por lo que se refiere a la aceptación del certificado, se aplica la cláusula 4.4.1 de la política de certificación y la declaración de prácticas de certificación («CP/CPS») de la SBCA; además, las condiciones de uso y las disposiciones descritas en el presente documento se consideran aceptadas por la organización a la que se expide el certificado («O=») cuando este se utiliza por primera vez.

En cuanto a la publicación del certificado, es de aplicación la cláusula 2.2 de la CP/CPS de la SBCA.

Todos los titulares de certificados deberán cumplir los requisitos siguientes:

(1) proteger su clave privada contra usos no autorizados;

(2) abstenerse de transferir o revelar a su clave privada a terceros, ni siquiera en calidad de representantes;

(3) abstenerse de hacer uso continuado de la clave privada tras la expiración del período de validez o la revocación del certificado, salvo para visualizar datos encriptados (por ejemplo, descifrar correos electrónicos);

(4) el titular del certificado es responsable de la copia o transmisión de la clave a la entidad o entidades finales;

(5) el titular del certificado debe obligar a la entidad final/a todas las entidades finales a cumplir las presentes condiciones, incluida la CP/CPS de la SBCA, en relación con la clave privada;

(6) el titular del certificado debe facilitar la identificación de los representantes autorizados facultados para solicitar la revocación de certificados expedidos a la organización, con información detallada sobre los hechos que dieron lugar a la revocación y la contraseña de revocación;

(7) en el caso de los certificados asociados a grupos de personas y a funciones o personas jurídicas, cuando una persona abandone el grupo de entidades finales (por ejemplo, terminación de la relación laboral), el titular del certificado deberá evitar el uso indebido de la clave privada revocando el certificado;

(8) corresponderá al titular del certificado solicitar la revocación del certificado en las circunstancias mencionadas en la cláusula 4.9.1 de la CP/CPS de la SBCA.

En cuanto a la renovación o creación de nuevas claves de los certificados, se aplicarán las cláusulas 4.6 o 4.7 de la CP/CPS de la SBCA.

En cuanto a la modificación de certificados, se aplicará la cláusula 4.8 de la CP/CPS de la SBCA.

En cuanto a la revocación de certificados, se aplicará la cláusula 4.9 de la CP/CPS de la SBCA.

5. Formulario de identificación de personas de contacto y mensajeros de confianza (modelo)

El abajo firmante*, [nombre y dirección del representante de la organización]* **certifica que la información siguiente debe utilizarse en el contexto de la solicitud, generación y recuperación de certificados digitales de clave pública para los puntos de acceso de TACHOnet en apoyo de la confidencialidad, integridad y no repudio de los mensajes de TACHOnet:**

Información de la persona de contacto:

– **Persona de contacto #1**	– **Persona de contacto #2**
– Apellidos:	– Apellidos:
– Nombre:	– Nombre:
– Teléfono móvil:	– Teléfono móvil:
– Teléfono:	– Teléfono:
– Dirección de correo electrónico:	– Dirección de correo electrónico:
– Firma manuscrita: Firma manuscrita: –	– Firma manuscrita: Firma manuscrita: – – –

Mensajero de confianza #1

– **Mensajero de confianza #2**	– **Apellidos:**
– Apellidos:	– Apellidos:
– Nombre:	– Nombre:
– Teléfono móvil:	– Teléfono móvil:
– Dirección de correo electrónico:	– Dirección de correo electrónico:
– País de expedición del pasaporte:	– País de expedición del pasaporte:
– Número de pasaporte:	– Número de pasaporte:
– Fecha de caducidad del pasaporte:	– Fecha de caducidad del pasaporte:

Lugar, fecha, sello de la empresa o sello de la organización:

Firma del representante autorizado:

6. Documentos

6.1. Poder individual (modelo)

Puede consultarse aquí un modelo del poder individual que deberá firmar y presentar el mensajero de confianza durante el registro presencial ante la autoridad de registro (RAO):

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. Formulario de solicitud de certificado en papel (modelo)

Puede consultarse aquí un modelo de formulario en papel de solicitud de certificado, que deberá firmar y presentar el mensajero de confianza durante el registro presencial ante la autoridad de registro (RAO):

7. Glosario (únicamente en inglés)

Los principales términos empleados en este subapéndice se definen en la sección de definiciones del portal web único digital del CEF:

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

Los principales acrónimos empleados en este subapéndice se definen en el glosario CEF del portal web único digital del CEF:

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