Conselho da
União Europeia

Bruxelas, 5 de novembro de 2018
(OR. en)

13711/18
ADD 1

Dossiê interinstitucional:
2018/0339(NLE)

TRANS 488

NOTA

de:	Secretariado-Geral do Conselho
para:	Delegações
n.º doc. ant.:	ST 13711/18 TRANS 448
n.° doc. Com.:	ST 12727/18 TRANS 426 + ADD 1
Assunto:	Decisão do Conselho sobre a posição a adotar, em nome da União Europeia, no grupo de peritos para o acordo europeu relativo ao trabalho das tripulações de veículos que efetuam transportes rodoviários internacionais da Comissão Económica das Nações Unidas para a Europa

Anexo da Decisão do Conselho em epígrafe.

APÊNDICE

Novo apêndice ao AETR

Apêndice 4

Especificações do sistema TACHOnet

1. Âmbito e objetivo

1.1. O presente apêndice define os termos e condições relativos à ligação das partes contratantes no AETR ao sistema TACHOnet através da plataforma eDelivery.

1.2. As partes contratantes que se ligam ao sistema TACHOnet através da plataforma eDelivery devem obedecer às disposições definidas no presente apêndice.

2. Definições – Para efeitos das presentes especificações, entende-se por:

a) "Parte contratante" ou "parte", qualquer parte contratante no AETR;

b) "eDelivery", o serviço desenvolvido pela Comissão Europeia que torna possível a transmissão de dados entre terceiros por meios eletrónicos e fornece prova do tratamento dos dados transmitidos, nomeadamente a prova do envio e da receção dos mesmos, e que protege os dados transferidos contra o risco de qualquer alteração não autorizada;

c) "TACHOnet", o sistema de intercâmbio eletrónico de informações sobre os cartões de condutor entre as partes contratantes referido no artigo 31.º, n.º 2, do Regulamento (UE) n.º 165/2014;

d) "Plataforma central", o sistema de informação que permite o encaminhamento de mensagens TACHOnet entre partes requerentes e respondentes;

e) "Parte requerente", a parte contratante que emite um pedido ou uma notificação no âmbito do sistema TACHOnet, que é seguidamente encaminhado/a para a parte respondente competente pela plataforma central;

f) "Parte respondente", a parte contratante a quem o pedido ou a notificação TACHOnet é dirigido(a);

g) "Autoridade emissora dos cartões" ou "CIA", a entidade habilitada por uma parte contratante para a emissão e gestão de cartões tacográficos.

3. Responsabilidades gerais

3.1. Nenhuma parte contratante pode celebrar acordos para acesso ao TACHOnet em nome de outra parte ou de qualquer outro modo representar a outra parte contratante com base no presente apêndice. Nenhuma parte contratante age enquanto subcontratante da outra parte contratante nas operações referidas no presente apêndice.

3.2. As partes contratantes concedem acesso aos seus registos nacionais de cartões de condutor através do TACHOnet, nos moldes e com o nível de serviço definidos no subapêndice 4.6.

3.3. As partes contratantes notificam-se mutuamente sem demora caso observem perturbações ou erros no seu domínio de responsabilidade que possam pôr em causa o decorrer do funcionamento normal do TACHOnet.

3.4. Cada parte nomeia pessoas de contacto para o sistema TACHOnet junto do secretariado do AETR. Qualquer alteração nestes pontos de contacto deve ser notificada ao secretariado do AETR por escrito.

4. Ensaios para ligação ao TACHOnet

4.1. A ligação de uma parte contratante ao sistema TACHOnet deve ser estabelecida após a conclusão bem sucedida da interligação, da integração e dos ensaios de desempenho em conformidade com as instruções da Comissão Europeia e sob a sua supervisão.

4.2. Em caso de insucesso dos ensaios preliminares, a Comissão Europeia pode temporariamente suspender a fase de ensaio. Os ensaios serão retomados quando a parte contratante tiver notificado à Comissão Europeia a adoção das necessárias melhorias técnicas a nível nacional para permitir o êxito da execução dos ensaios preliminares.

4.3. A duração máxima dos ensaios preliminares é de seis meses.

5. Arquitetura de confiança

5.1. A confidencialidade, a integridade e a não repudiação das mensagens TACHOnet serão asseguradas pela arquitetura de confiança TACHOnet.

5.2. Esta basear-se-á num serviço PKI de infraestrutura de chave pública, instituído pela Comissão Europeia, cujos requisitos constam dos subapêndices 4.8 e 4.9.

5.3. Intervêm na arquitetura de confiança TACHOnet as seguintes entidades:

a) Autoridade de certificação, responsável pela geração dos certificados digitais emitidos pela autoridade de registo às autoridades nacionais das partes contratantes (via correios fidedignos, por elas nomeados), assim como pela instituição da infraestrutura técnica para a emissão, revogação e renovação dos certificados digitais.

b) Proprietário do domínio, responsável pelo funcionamento da plataforma central referida no subapêndice 4.1 e pela validação e coordenação da arquitetura de confiança TACHOnet.

c) Autoridade de registo, responsável pelo registo e pela aprovação dos pedidos de emissão, revogação e renovação dos certificados digitais, assim como por verificar a identidade dos correios fidedignos.

d) Correio fidedigno, a pessoa nomeada pelas autoridades nacionais, responsável por entregar a chave pública à autoridade de registo e por obter o certificado correspondente gerado pela autoridade de certificação.

e) Autoridade nacional da parte contratante, que:

i) gera as chaves privadas e as chaves públicas correspondentes a incluir nos certificados a gerar pela autoridade de certificação;

ii) pede os certificados digitais à autoridade de certificação;

iii) nomeia o correio fidedigno.

5.4. A autoridade de certificação e a autoridade de registo são nomeadas pela Comissão Europeia.

5.5. Qualquer parte contratante ligada ao TACHOnet deve solicitar a emissão de um certificado digital em conformidade com o subapêndice 4.9 de molde a assinar e encriptar uma mensagem TACHOnet.

5.6. O certificado pode ser revogado em conformidade com o subapêndice 4.9.

6. Proteção dos dados e confidencialidade

6.1. As partes, em conformidade com a legislação relativa à proteção dos dados a nível internacional e nacional, e nomeadamente com a Convenção para a proteção das pessoas singulares no que diz respeito ao tratamento automático de dados pessoais, adotam todas as medidas técnicas e organizacionais necessárias para garantir a segurança dos dados do TACHOnet e impedir a sua alteração ou perda, ou respetivo tratamento ou acesso não autorizados (em especial a autenticidade, a confidencialidade, a rastreabilidade, a integridade, a disponibilidade e a não repudiação e segurança das mensagens).

6.2. Cada parte protege os seus próprios sistemas nacionais contra a utilização ilícita, os códigos maliciosos, os vírus, as intrusões informáticas e a adulteração dos dados e, bem assim, outras ações comparáveis levadas a cabo por terceiros. As partes acordam em envidar esforços comercialmente razoáveis no sentido de impedir a transmissão de quaisquer vírus, bombas-relógio, parasitas ou semelhantes, ou quaisquer programas informáticos que possam interferir com os sistemas informáticos das outras partes.

7. Custos

7.1. As partes contratantes assumem os seus próprios custos de desenvolvimento e funcionamento, relacionados com os seus próprios sistemas de dados e procedimentos, tal como se requer para cumprir as obrigações ao abrigo do presente apêndice.

7.2. Os serviços especificados no subapêndice 4.1 previstos na plataforma central são gratuitos.

8. Subcontratação

8.1. As partes podem subcontratar quaisquer dos serviços pelos quais são responsáveis ao abrigo do presente apêndice.

8.2. Esta subcontratação não isenta a parte da responsabilidade ao abrigo do presente apêndice, incluindo a responsabilidade pelo nível de serviço adequado em conformidade com o subapêndice 4.6.

Subapêndice 4.1

Aspetos gerais do TACHOnet

1. Descrição geral

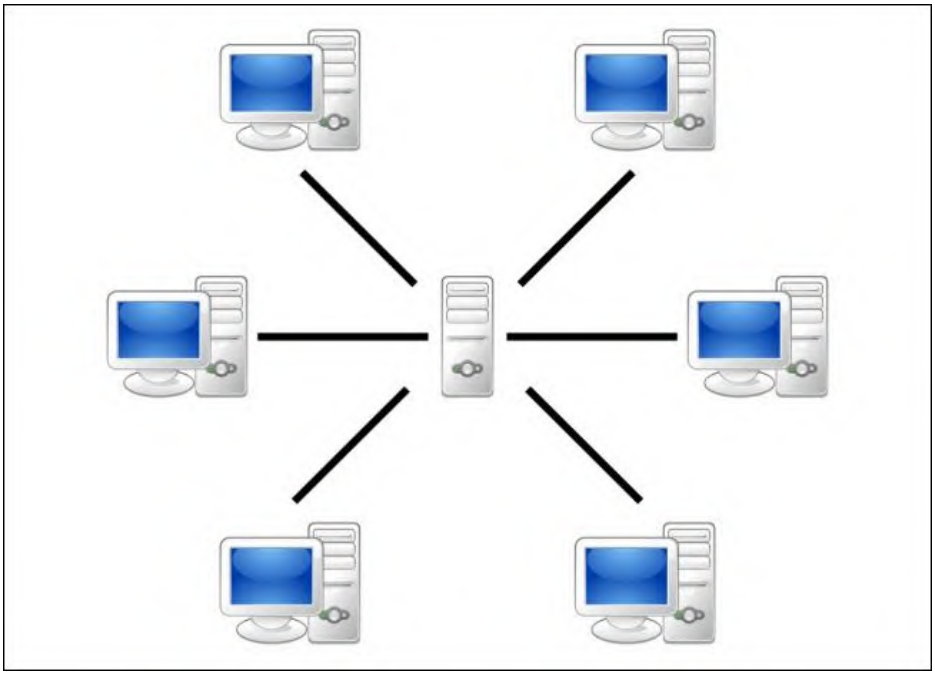
O TACHOnet é um sistema de intercâmbio eletrónico de informações sobre os cartões de condutor entre as partes contratantes no AETR. O TACHOnet encaminha os pedidos de informação das partes requerentes às partes respondentes, assim como as respostas destas últimas às primeiras. As partes contratantes que são parte do TACHOnet devem ligar os seus registos nacionais de cartões de condutor ao sistema.

2. Arquitetura

O sistema de mensagens TACHOnet é composto pelas seguintes partes:

2.1. Uma plataforma central, que deve poder receber um pedido da parte requerente, validá-lo e tratá-lo e transmiti-lo às partes respondentes. A plataforma central deve esperar que cada parte respondente dê a sua resposta, consolidar todas as respostas e transmitir a resposta consolidada à parte requerente.

2.2. Os sistemas nacionais das partes devem estar equipados com uma interface com capacidade tanto para o envio de pedidos para a plataforma central como para a receção das respetivas respostas. Os sistemas nacionais podem recorrer a software próprio ou comercial para transmitir e receber mensagens da plataforma central.



3. Gestão

3.1. A plataforma central será gerida pela Comissão Europeia, que é responsável pela sua exploração e manutenção técnica.

3.2. A plataforma central não deve conservar os dados por um período superior a seis meses, exceto os dados de registo e os dados estatísticos estabelecidos no subapêndice 4.7.

3.3. A plataforma central não dará acesso a dados pessoais, exceto no caso dos funcionários autorizados da Comissão Europeia, quando necessário para efeitos de monitorização, manutenção e resolução de avarias.

3.4. Cada parte contratante é responsável por:

3.4.1. Estabelecer e gerir os seus sistemas nacionais, incluindo a interface com a plataforma central.

3.4.2. Instalar e assegurar a manutenção do seu sistema nacional, incluindo os equipamentos e o software, próprios ou comerciais.

3.4.3. Garantir a interoperabilidade dos seus sistemas nacionais com a plataforma central, incluindo a gestão de mensagens de erro recebidas da plataforma central.

3.4.4. Adotar todas as medidas necessárias para garantir a confidencialidade, a integridade e a disponibilidade da informação.

3.4.5. Explorar os sistemas nacionais de acordo com os níveis de serviço previstos no subapêndice 4.6.

Subapêndice 4.2

Funcionalidades do TACHOnet

1. Serão asseguradas pelo sistema de mensagens TACHOnet as seguintes funcionalidades:

1.1. Verificação dos cartões emitidos (CIC): permite à parte requerente enviar um pedido de verificação dos cartões emitidos a uma ou a todas as partes respondentes, para determinar se um requerente de cartão já possui um cartão de condutor emitido pelas partes respondentes. As partes respondentes darão resposta ao pedido enviando uma resposta ao pedido de verificação dos cartões emitidos.

1.2. Verificação da situação do cartão (CCS): permite à parte requerente solicitar à parte respondente os pormenores de um cartão emitido por esta última através do envio de um pedido de verificação da situação do cartão. A parte respondente tratará o pedido mediante o envio da correspondente resposta.

1.3. Alteração da situação do cartão (MCS): permite à parte requerente notificar a parte respondente, através de um pedido de alteração da situação do cartão, da mudança de situação de um cartão emitido por esta última. A parte respondente deve responder com um aviso de receção do pedido de alteração da situação do cartão.

1.4. Carta de condução de cartão emitido (ICDL): permite à parte requerente notificar a parte respondente, através de um pedido de carta de condução de cartão emitido, de que foi emitido um cartão pela primeira contra uma carta de condução emitida por esta última. A parte respondente deve tratar o pedido mediante o envio da correspondente resposta.

2. Devem ser incluídos outros tipos de mensagem considerados adequados para o funcionamento eficiente do sistema TACHOnet, por exemplo, as notificações de erro.

3. Os sistemas nacionais devem reconhecer as situações do cartão enumeradas no quadro 1, aquando da utilização de qualquer uma das funcionalidades descritas no ponto 1. No entanto, as partes não são obrigadas a aplicar um procedimento administrativo que utilize todas as situações referidas.

4. Sempre que uma parte receber uma resposta ou uma notificação assinalando uma situação que não é utilizada nos seus procedimentos administrativos, o sistema nacional traduzirá a situação constante da mensagem recebida para o valor aplicável nesse procedimento. A mensagem não deve ser rejeitada pela parte respondente, desde que a situação constante da mensagem esteja enumerada no quadro 1.

5. As situações do cartão enumeradas no quadro 1 não devem ser utilizadas para determinar se um cartão de condutor é válido para a condução. Quando uma parte questiona o registo da autoridade nacional emissora dos cartões através da funcionalidade CCS, a resposta deve incluir o domínio específico "válido para condução". Os procedimentos administrativos nacionais devem ser de molde a que as respostas CCS contenham sempre o valor adequado "válido para a condução".

Quadro 1

Situações do cartão

Situação do cartão	**Definição**
Pedido	A CIA recebeu um pedido de emissão de um cartão de condutor. Estas informações foram registadas e armazenadas na base de dados com as chaves de pesquisa geradas.
Aprovado	A CIA aprovou o pedido de cartão tacográfico.
Rejeitado	A CIA não aprovou o pedido.
Personalizado	O cartão tacográfico foi personalizado.
Expedido	A autoridade nacional expediu o cartão de condutor para o condutor em causa ou a agência responsável pela entrega.
Entregue	A autoridade nacional entregou o cartão de condutor ao respetivo condutor.
Confiscado	O cartão de condutor foi retirado ao condutor pela autoridade competente.
Suspenso	O cartão de condutor foi retirado temporariamente ao condutor.
Retirado	A CIA decidiu retirar o cartão de condutor. O cartão foi definitivamente invalidado.
Devolvido	O cartão tacográfico foi devolvido à CIA e declarado desnecessário.
Perdido	O cartão tacográfico foi declarado como perdido à CIA.
Roubado	O cartão tacográfico foi declarado como roubado à CIA. Um cartão roubado é considerado perdido.
Defeituoso	O cartão tacográfico foi comunicado como defeituoso à CIA.
Caducado	O período de validade do cartão tacográfico caducou.
Substituído	O cartão tacográfico, que foi declarado como perdido, roubado ou defeituoso, foi substituído por um novo cartão. Os dados do novo cartão são os mesmos, com exceção do índice de substituição do número do cartão, que foi aumentado de uma unidade.

Renovado	O cartão tacográfico foi renovado porque se verificou uma alteração dos dados administrativos ou porque o período de validade chegou ao fim. O número do novo cartão é o mesmo, com exceção do índice de renovação, que foi aumentado de uma unidade.
Em processo de troca	A CIA que emitiu um cartão de condutor recebeu uma notificação de que teve início o processo de troca desse cartão por um cartão de condutor emitido pela CIA de outra parte.
Trocado	A CIA que emitiu um cartão de condutor recebeu uma notificação de que foi completado o processo de troca desse cartão por um cartão de condutor emitido pela CIA de outra parte.

Subapêndice 4.3

Disposições relativas às mensagens do sistema de mensagens TACHOnet

1. Requisitos técnicos gerais

1.1. A plataforma central deve proporcionar interfaces síncronas e assíncronas para a troca de mensagens. As partes podem escolher a tecnologia mais adequada para interagir com as suas próprias aplicações.

1.2. Todas as mensagens trocadas entre a plataforma central e os sistemas nacionais devem seguir o código UTF-8.

1.3. Os sistemas nacionais devem estar aptos a receber e tratar as mensagens que contenham carateres gregos ou cirílicos.

2. Estrutura das mensagens XML e definição do esquema (XSD)

2.1. A estrutura geral das mensagens XML deve respeitar o formato definido pelos esquemas XSD instalados na plataforma central.

2.2. A plataforma central e os sistemas nacionais devem transmitir e receber mensagens conformes com o esquema de mensagens XSD.

2.3. Os sistemas nacionais devem ser capazes de enviar, receber e tratar todas as mensagens correspondentes a qualquer das funcionalidades definidas no subapêndice 4.2.

2.4. As mensagens XML devem incluir, pelo menos, os requisitos mínimos estabelecidos no quadro 2.

Quadro 2

Requisitos mínimos para o conteúdo das mensagens XML

Cabeçalho comum		**Obrigatório**
Versão	A versão oficial das especificações XML será, indicada através do espaço de nomes definido no XSD da mensagem e no atributo da *versão* do elemento "cabeçalho" das mensagens XML. O número da versão ("n.m") será definido como valor fixo em cada versão do ficheiro de definição do esquema XML (xsd).	Sim
Identificador de teste	Identificador (id) facultativo para teste. O iniciador do teste completa o id e todos os participantes no fluxo de trabalho enviarão/devolverão o mesmo id. Na produção, deve ser ignorado e não será usado se for fornecido.	Não
Identificador técnico	UUID que identifica exclusivamente cada mensagem individual. O remetente cria um UUID e completa este atributo. Estes dados não são utilizados para fins comerciais.	Sim
Identificador do fluxo de trabalho	O identificador do fluxo de trabalho é um UUID e deve ser gerado pela parte requerente. Esse identificador passa a ser utilizado em todas as mensagens para estabelecer uma correlação entre o fluxo de trabalho.	Sim
Enviado em	Data e hora (UTC) a que a mensagem foi enviada.	Sim
Tempo limite de tratamento do pedido	Atributo de data e hora (em formato UTC) facultativo. Este valor será definido pela plataforma central unicamente para os pedidos reencaminhados. Informará a parte respondente do momento em que o tempo limite de tratamento do pedido será ultrapassado. Esse valor não é exigido em MS2TCN_<x>_Req nem nas mensagens de resposta. É facultativo por forma a que seja possível usar a mesma definição de cabeçalho para todos os tipos de mensagem, independentemente de ser ou não necessário indicar um valor para o atributo "tempo limite de tratamento".	Não
De	Código ISO 3166-1 alfa 2 da parte que envia a mensagem ou "UE".	Sim
Para	Código ISO 3166-1 alfa 2 da parte a quem é enviada a mensagem ou "UE".	Sim

Subapêndice 4.4

TRANSLITERAÇÃO E SERVIÇOS NYSIIS (SISTEMA DE INFORMAÇÕES E DE IDENTIFICAÇÃO DO ESTADO DE NOVA IORQUE)

1. O algoritmo NYSIIS aplicado na plataforma central deve ser utilizado para codificar os nomes de todos os condutores no registo nacional.

2. Para pesquisar um cartão através da funcionalidade CIC, devem ser utilizadas as chaves NYSIIS como principal mecanismo de pesquisa.

3. Para obter mais resultados, as partes podem também usar um algoritmo de pesquisa personalizado.

4. Os resultados da pesquisa devem indicar o mecanismo de pesquisa que foi utilizado para encontrar um registo, quer NYSIIS quer personalizado.

5. No caso de uma parte optar por registar notificações ICDL, as chaves NYSIIS constantes da notificação devem ser registadas como parte dos dados ICDL. Aquando da pesquisa dos dados ICDL, a parte deve utilizar as chaves NYSIIS do nome do requerente.

Subapêndice 4.5

Requisitos de segurança

1. O Protocolo HTTPS deve ser utilizado para o intercâmbio de mensagens entre a plataforma central e os sistemas nacionais.

2. Os sistemas nacionais devem utilizar os certificados digitais referidos nos subapêndices 4.8 e 4.9 para securizar a transmissão de mensagens entre o sistema nacional e a plataforma central.

3. Os sistemas nacionais devem, no mínimo, aplicar certificados que usam o algoritmo hash de assinatura SHA-2 (SHA-256) e uma chave pública de 2048 bits de comprimento.

Subapêndice 4.6

Níveis de serviço

1. Os sistemas nacionais devem oferecer os seguintes níveis de serviço mínimos:

1.1. Estar disponíveis 24 horas por dia, 7 dias por semana.

1.2. Ter a disponibilidade controlada por uma mensagem heartbeat emitida a partir da plataforma central.

1.3. Ter uma taxa de disponibilidade de 98 %, de acordo com o quadro abaixo (valores arredondados à unidade mais próxima):

Uma disponibilidade de	equivalente a uma indisponibilidade de		
	Diária	Mensal	Anual
98%	0,5 horas	15 horas	7,5 dias

As partes são incentivadas a respeitar a taxa de disponibilidade diária, embora se reconheça que certas atividades necessárias, tais como a manutenção do sistema, exigem um tempo de indisponibilidade de mais de 30 minutos. As taxas de disponibilidade mensal e anual continuam, no entanto, a ser obrigatórias.

1.4. Devem responder a um mínimo de 98 % dos pedidos que lhes foram transmitidos durante um mês civil.

1.5. Devem responder aos pedidos no prazo de 10 segundos.

1.6. O tempo limite de tratamento do pedido (intervalo durante o qual o requerente pode aguardar uma resposta) não deve exceder 20 segundos.

1.7. Devem estar em condições de responder a uma taxa de pedidos de 6 mensagens por segundo.

1.8. Os sistemas nacionais não podem enviar pedidos para a plataforma TACHOnet a uma taxa superior a 2 pedidos por segundo.

1.9. Os sistemas nacionais devem dispor de capacidade para fazer face a potenciais problemas técnicos da plataforma central ou dos sistemas nacionais das outras partes. Estes incluem, numa lista não exaustiva:

a) a perda da ligação à plataforma central;

b) a ausência de resposta a um pedido;

c) a receção de respostas uma vez ultrapassado o tempo limite da mensagem;

d) a receção de mensagens não solicitadas;

e) a receção de mensagens inválidas;

2. A plataforma central deve:

2.1. apresentar uma taxa de disponibilidade de 98 %;

2.2. notificar os sistemas nacionais de quaisquer erros, quer através da mensagem de resposta quer através de uma mensagem específica de erro. Por sua vez, os sistemas nacionais devem receber essas mensagens específicas de erro e dispor de um fluxo de trabalho escalonado para tomar todas as medidas necessárias para corrigir o erro notificado.

3. Manutenção

As partes devem notificar as outras partes e a Comissão Europeia das operações de manutenção de rotina via a aplicação Web, se tecnicamente possível com uma antecedência mínima de uma semana antes do início das operações.

Subapêndice 4.7

Registo e estatísticas dos dados recolhidos na plataforma central

1. Para garantir a privacidade, os dados utilizados para fins estatísticos devem ser anónimos. Dados que identifiquem um determinado cartão, condutor ou carta de condução não devem estar disponíveis para fins estatísticos.

2. Todas as transações devem ser registadas para efeitos de monitorização e depuração e os dados de registo correspondentes devem permitir produzir estatísticas sobre essas transações.

3. Os dados pessoais não devem ser conservados nos registos mais de 6 meses. A informação estatística deve ser mantida indefinidamente.

4. Os dados estatísticos utilizados para a comunicação de informações devem incluir:

   a) a parte requerente;

   b) a parte respondente;

   c) o tipo de mensagem;

   d) o código da situação da resposta;

   e) a data e hora das mensagens;

   f) o tempo de resposta.

Subapêndice 4.8

Disposições gerais relativas às chaves e aos certificados digitais para utilização no sistema TACHOnet

1. A Direção-Geral da Informática da Comissão Europeia (DIGIT) disponibiliza um serviço de PKI[1] (designado por "serviço PKI MIE") às partes contratantes no AETR com ligação ao sistema TACHOnet (em seguida, as autoridades nacionais) através da plataforma eDelivery.

2. O procedimento para pedido e revogação de certificados digitais, assim como os termos e condições pormenorizados da sua utilização, encontram-se definidos no apêndice.

3. Utilização dos certificados:

3.1. Tendo o certificado sido emitido, a autoridade nacional[2] deve utilizá-lo apenas no contexto do sistema TACHOnet. O certificado pode ser utilizado para:

   a) autenticar a origem dos dados;

   b) encriptar dados;

   c) assegurar a deteção de quebras da integridade dos dados.

3.2. Qualquer utilização não explicitamente autorizada como parte das utilizações permitidas do certificado é proibida.

4. As partes contratantes:

   a) protegem a sua chave privada contra qualquer utilização não autorizada;

   b) evitam a transferência ou a revelação das chaves privadas a terceiros, mesmo representantes;

---

1 Uma PKI (infraestrutura de chave pública) é composta por um conjunto de papéis, políticas, processos e sistemas necessários para criar, gerir, distribuir e revogar certificados digitais.

2 Identificado pelo valor do atributo "O=" no Nome Distintivo do Sujeito do certificado emitido.

c) asseguram a confidencialidade, a integridade e a disponibilidade das chaves privadas geradas, armazenadas e utilizadas no sistema TACHOnet;

d) evitam a utilização prolongada das chaves privadas depois de expirado o período de validade ou de revogação do certificado, exceto para visualização de dados encriptados (por exemplo, para desencriptagem de correio eletrónico). As chaves expiradas devem ser quer destruídas quer conservadas de maneira a impedir a sua utilização;

e) fornecem à autoridade de registo a identificação dos representantes autorizados a pedir a revogação dos certificados emitidos à organização (os pedidos de revogação devem incluir uma senha de pedido de revogação e dados sobre os incidentes que levaram à revogação);

f) impedem a utilização abusiva das chaves privadas solicitando a revogação do certificado de chave pública associado em caso de comprometimento da chave privada ou dos dados de ativação da chave privada;

g) devem ser responsáveis e honrar a obrigação de pedir a revogação do certificado nas circunstâncias identificadas nas políticas de certificação (CP) e na declaração de práticas de certificação (CPS) da autoridade de certificação;

h) notificam a autoridade de registo sem demora da perda, roubo ou potencial comprometimento de quaisquer chaves AETR utilizadas no contexto do sistema TACHOnet.

5. Responsabilidades

Sem prejuízo da responsabilidade da Comissão Europeia, de uma forma que contrarie o disposto na legislação nacional aplicável e sem excluir a sua responsabilidade nos casos em que tal não é permitido por essa legislação, a Comissão Europeia não pode ser responsabilizada relativamente:

a) ao teor do certificado, cuja responsabilidade é exclusivamente do seu proprietário. É da responsabilidade do proprietário do certificado verificar a exatidão do teor do certificado;

b) à utilização feita do certificado pelo seu proprietário.

Subapêndice 4.9

Descrição do serviço PKI para utilização no sistema TACHOnet

1. Introdução

Uma PKI (infraestrutura de chave pública) é composta por um conjunto de papéis, políticas, processos e sistemas necessários para criar, gerir, distribuir e revogar certificados digitais[3]. O serviço PKI MIE da plataforma eDelivery permite a emissão e a gestão de certificados digitais utilizados para assegurar a confidencialidade, a integridade e a não repudiação das informações trocadas entre pontos de acesso (AP).

O serviço PKI da plataforma eDelivery é baseado nos serviços Trust Center da autoridade de certificação TeleSec Shared Business CA, aos quais se aplicam a política de certificação (CP) / a declaração de práticas de certificação (CPS) da autoridade de certificação TeleSec Shared Business da T-Systems International GmbH[4].

O serviço PKI emite certificados que são adequados para a securização de vários processos de atividade empresarial dentro e fora de empresas, organizações, autoridades e instituições públicas, que requerem um nível de segurança médio a fim de provar a autenticidade, a integridade e a fiabilidade da entidade no final da cadeia.

2. Processo de pedido de certificado

2.1. Papéis e responsabilidades

2.1.1. "Organização" ou "Autoridade nacional" que pedem o certificado

2.1.1.1. A autoridade nacional deve pedir os certificados no contexto do projeto TACHOnet.

2.1.1.2 A autoridade nacional deve:

a) pedir os certificados ao serviço PKI MIE;

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

[4] A mais recente versão das CP/CPS está disponível em https://www.telesec.de/en/sbca-en/support/download-area/

b) gerar as chaves privadas e as chaves públicas correspondentes a incluir nos certificados gerados pela autoridade de certificação;

c) descarregar o certificado quando aprovado;

d) assinar e devolver à autoridade de registo:

i) o formulário de identificação das pessoas de contacto e dos correios fidedignos,

ii) a procuração individual assinada.[5]

2.1.2. Correios fidedignos

2.1.2.1. A autoridade nacional nomeia um correio fidedigno.

2.1.2.2. O correio fidedigno deve:

a) entregar a chave pública à autoridade de registo durante um processo de identificação e registo em presença;

b) obter o certificado correspondente da autoridade de registo.

2.1.3. Proprietário do domínio

2.1.3.1. O proprietário do domínio é a DG MOVE.

2.1.3.2. O proprietário do domínio deve:

a) validar e coordenar a rede TACHOnet e a arquitetura de confiança TACHOnet, incluindo os procedimentos de validação para emissão dos certificados;

b) explorar a plataforma central TACHOnet e coordenar a atividade das partes relativa ao funcionamento do sistema TACHOnet;

c) executar, juntamente com as autoridades nacionais, os ensaios para ligação ao TACHOnet.

[5] Uma procuração é um documento legal por meio do qual a organização capacita e autoriza a Comissão Europeia, representada pelo funcionário identificado responsável pelo serviço PKI MIE, a pedir a geração de um certificado em seu nome à CA TeleSec Shared Business da T-Systems International GmbH. Ver igualmente o ponto 6.

2.1.4. Autoridade de registo

2.1.4.1. O Centro Comum de Investigação (JRC) é a autoridade de registo.

2.1.4.2. A autoridade de registo é responsável pela verificação da identidade dos correios fidedignos, pelo registo e aprovação dos pedidos de emissão, revogação e renovação dos certificados digitais.

2.1.4.3. A autoridade de registo deve:

a) atribuir um identificador único à autoridade nacional;

b) autenticar a identidade da autoridade nacional, os seus pontos de contacto e correios fidedignos;

c) comunicar com o balcão de apoio do MIE sobre a autenticidade da autoridade nacional, os seus pontos de contacto e correios fidedignos;

d) informar a autoridade nacional sobre a aprovação ou rejeição do certificado.

2.1.5. Autoridade de certificação

2.1.5.1. A autoridade de certificação é responsável pela prestação da infraestrutura técnica para o pedido, a emissão e a revogação dos certificados digitais.

2.1.5.2. A autoridade de certificação deve:

a) providenciar a infraestrutura técnica para os pedidos de certificado por parte das autoridades nacionais;

b) validar ou rejeitar pedidos de certificado;

c) comunicar com a autoridade de registo com vista à verificação da identidade da organização requerente, sempre que necessário.

2.2. Emissão do certificado

2.2.1. A emissão do certificado deve ter lugar em conformidade com as seguintes etapas sequenciais, representadas na figura 1:

a) **Etapa 1:** Identificação do correio fidedigno;

b) **Etapa 2:** Criação do pedido de certificado;

c) **Etapa 3:** Registo junto da autoridade de registo;

d) **Etapa 4:** Geração do certificado;

e) **Etapa 5:** Publicação do certificado;

f) **Etapa 6:** Aceitação do certificado.

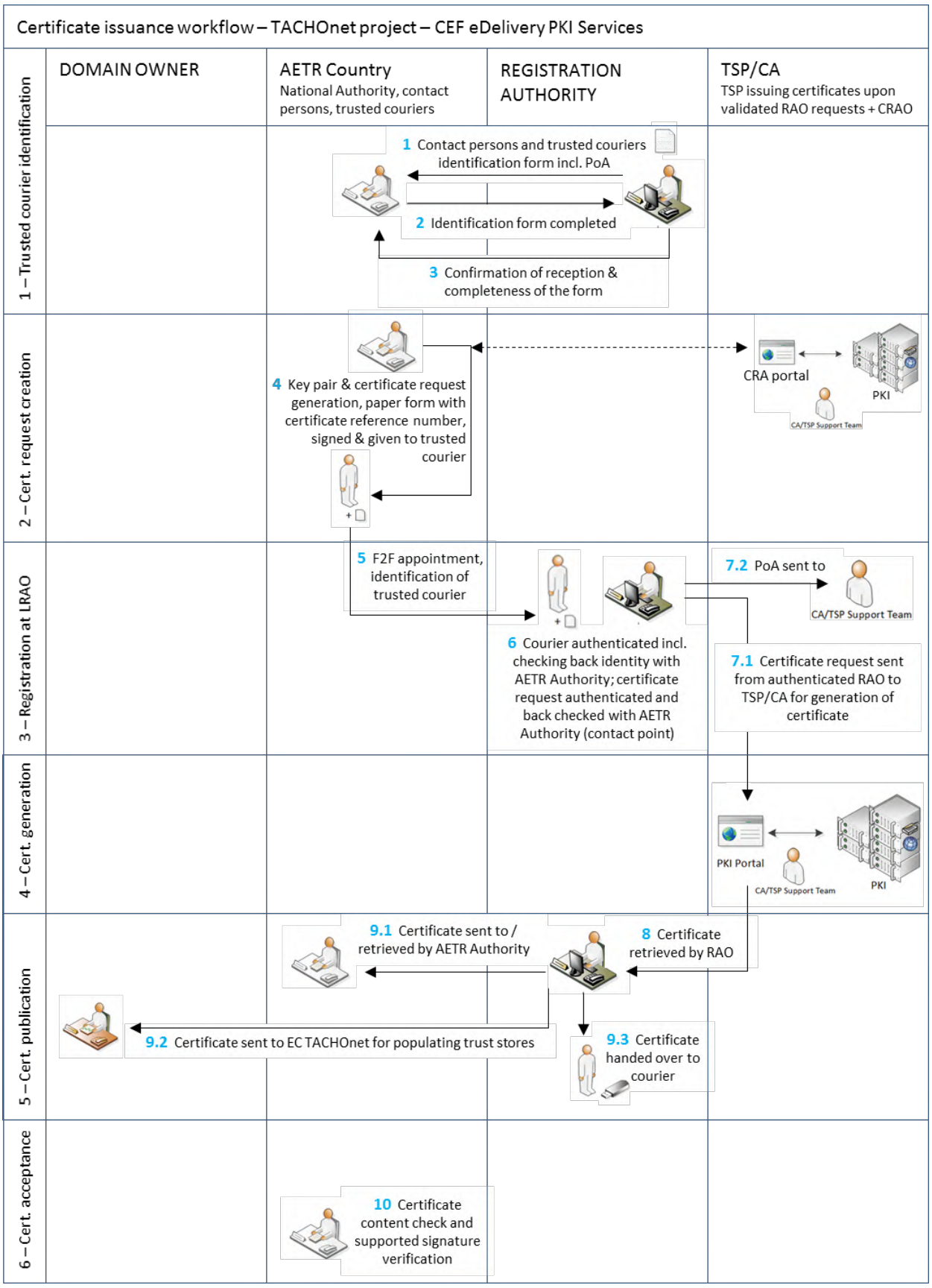


Figura 1 – Fluxo de trabalho da emissão do certificado

2.2.2. Etapa 1: Identificação do correio fidedigno

Para identificação do correio fidedigno segue-se o seguinte processo:

a) A autoridade de registo envia à autoridade nacional o formulário de identificação de pessoas de contacto e de correios fidedignos[6]. Este formulário inclui também uma procuração que deve ser assinada pela organização (autoridade AETR).

b) A autoridade nacional devolve os formulários preenchidos e a procuração assinada à autoridade de registo.

c) A autoridade de registo deve acusar a boa receção e declarar completo o formulário.

d) A autoridade de registo deve providenciar uma cópia atualizada da lista de pessoas de contacto e correios fidedignos ao proprietário do domínio.

2.2.3. Etapa 2: Criação do pedido de certificado

2.2.3.1. O pedido e a receção do certificado devem ser feitos a partir do mesmo computador e com o mesmo programa.

2.2.3.2. Para criação do pedido de certificado, segue-se o seguinte processo:

a) A organização deve navegar até à interface Web de utilizador para pedir o certificado através do endereço https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en: , e deve inserir o nome de utilizador **'sbca/CEF_eDelivery.europa.eu'** e a senha **'digit.333'**

6 Ver ponto 5.

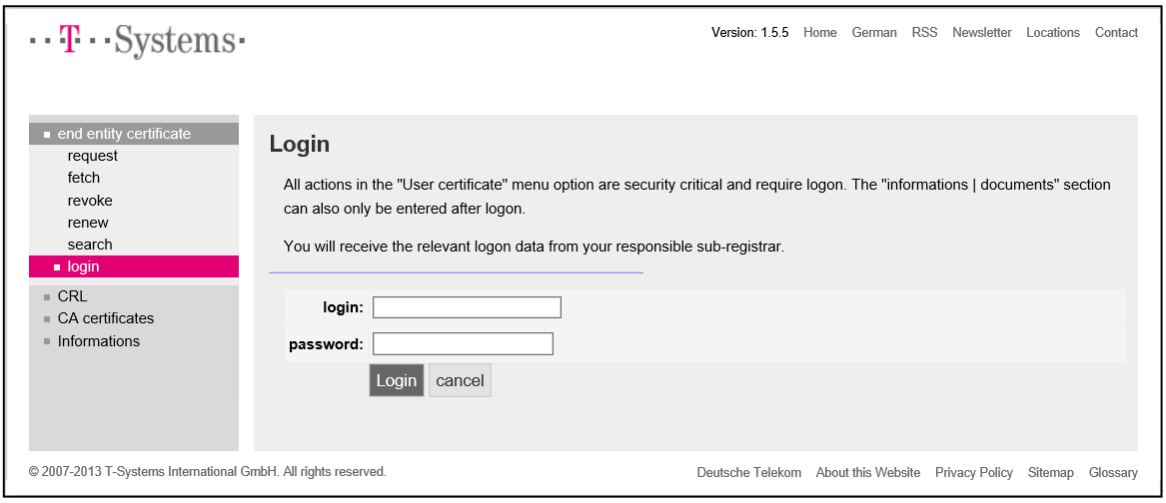


Figura 2

b) A organização deve clicar em "pedido" no lado esquerdo do painel e selecionar "CEF_TACHOnet" no menu pendente.

Figura 3

c) A organização deve completar o formulário de pedido de certificado constante da figura 4 com as informações do quadro 3, clicando em "Next (soft-PSE)" para terminar o processo.

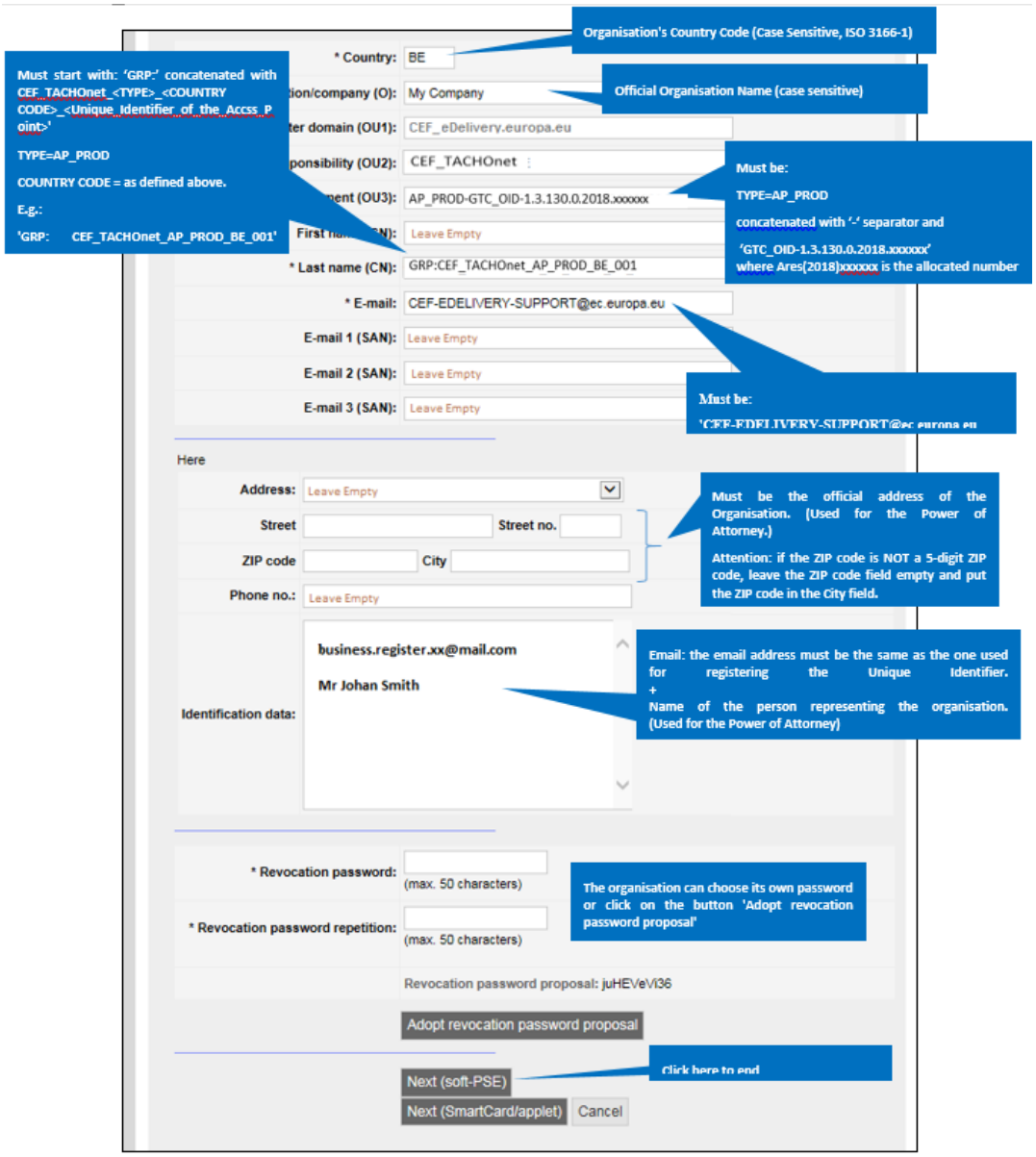

Organisation's Country Code (Case Sensitive, ISO 3166-1)
Official Organisation Name (case sensitive)
Must start with: 'GRP:' concatenated with CEF_TACHOnet_<TYPE>_<COUNTRY CODE>_<Unique_Identifier_of_the_Accss_Point>'
TYPE=AP_PROD
COUNTRY CODE = as defined above.
E.g.:
'GRP: CEF_TACHOnet_AP_PROD_BE_001'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

Figura 4

Campos pedidos	Descrição
País	**C=Código de país**, localização do proprietário do certificado, verificada utilizando um diretório público; Restrições: 2 carateres, conformes à norma ISO 3166-1, alfa-2, sensível às maiúsculas/minúsculas; Exemplos: DE, BE, NL, Casos específicos: UK (para a Grã-Bretanha), EL (para a Grécia)
Organização/Empresa (O)	**O=Nome da organização do proprietário do certificado**
Domínio principal (OU1)	**OU=CEF_eDelivery.europa.eu**
Área de responsabilidade (OU2)	**OU=CEF_TACHOnet**
Departamento (OU3)	Valor obrigatório por "ÁREA DE RESPONSABILIDADE" O teor deve ser verificado utilizando uma lista positiva (lista branca) sempre que o certificado é pedido. Se as informações não corresponderem à lista, o pedido é interrompido. Formato: **OU=<TYPE>-<GTC_NUMBER>** Em que "<TYPE>" é substituído por AP_PROD: Ponto de acesso em ambiente de produção. E em que <GTC_NUMBER> é **GTC_OID--1.3.130.0.2018.xxxxxx**, onde Ares(2018)xxxxxx é o número GTC do projeto TACHOnet. Por exemplo: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
Nome(s) próprio(s) (CN)	Deve ficar vazio
Apelido(s) (CN)	Deve começar por "GRP:", seguido de um nome comum. Formato: **CN=GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** Por exemplo: GRP:CEF_TACHOnet_AP_PROD_BE_001
Correio eletrónico	**E=CEF-EDELIVERY-SUPPORT@ec.europa.eu**
Correio eletrónico 1 (SAN)	Deve ficar vazio
Correio eletrónico 2 (SAN)	Deve ficar vazio
Correio eletrónico 3 (SAN)	Deve ficar vazio

Endereço	Deve ficar vazio
Rua	Deve ser o endereço oficial da organização do proprietário do certificado. (Usado na procuração.)
Número	Deve ser o endereço oficial da organização do proprietário do certificado. (Usado na procuração.)
Código postal	Deve ser o endereço oficial da organização do proprietário do certificado. (Usado na procuração.) **Atenção**: se o código postal NÃO tiver 5 dígitos, deixar o campo respetivo vazio e colocar o código postal no campo relativo à Cidade.
Cidade	Deve ser o endereço oficial da organização do proprietário do certificado. (Usado na procuração.) **Atenção**: se o código postal NÃO tiver 5 dígitos, deixar o campo respetivo vazio e colocar o código postal no campo relativo à Cidade.
Telefone	Deve ficar vazio
Dados de identificação	O endereço de correio eletrónico deve ser o mesmo do que o utilizado para registar o identificador único. + Deve ser o nome da pessoa que representa a organização. (Usado na procuração.) + **Registo Comercial N.º** (só obrigatório nas organizações privadas) **Inserido no Tribunal de** primeira instância local (só obrigatório nas organizações privadas alemãs e austríacas)
Senha de revogação	Campo obrigatório escolhido pelo requerente
Repetição da senha de revogação	Repetição do campo obrigatório escolhido pelo requerente

Quadro 3. Preencher dados de cada campo pedido

d) O comprimento selecionado é de 2048 (High Grade).

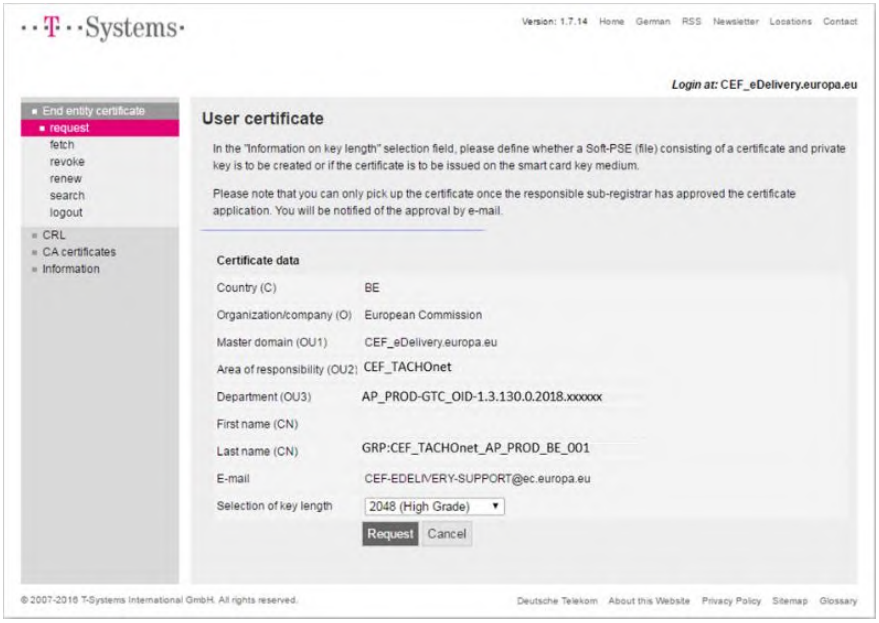


Figura 5

e) A organização deve registar o número de referência para receber o certificado.

Figura 6

f) O balcão de apoio do MIE deve verificar os novos pedidos de certificados e verificar se as informações no pedido de certificado são válidas, ou seja, se cumprem a convenção de nomeação especificada no apêndice 5.1 da Convenção de Nomeação de Certificados.

g) O balcão de apoio do MIE deve verificar que as informações inseridas no pedido se encontram num formato válido.

h) Quando alguma das verificações dos pontos 5 ou 6 falhar, o balcão de apoio do MIE envia uma mensagem eletrónica para o endereço previsto nos "Dados de identificação" do formulário de pedido, com o proprietário do domínio em cc, na qual se pede à organização que reinicie todo o processo. O pedido de certificado gorado é cancelado.

i) O balcão de apoio do MIE envia uma mensagem eletrónica à autoridade de registo acerca da validade do pedido. Este correio eletrónico deve incluir:

    1) o nome da organização, disponível no campo "Organização (O)" do pedido de certificado;

    2) os dados do certificado, incluindo o nome do ponto de acesso (AP) para o qual o certificado é emitido, disponível no campo "Apelido (CN)" do pedido de certificado;

    3) o número de referência do certificado;

    4) o endereço da organização, endereço de correio eletrónico e nome da pessoa que a representa.

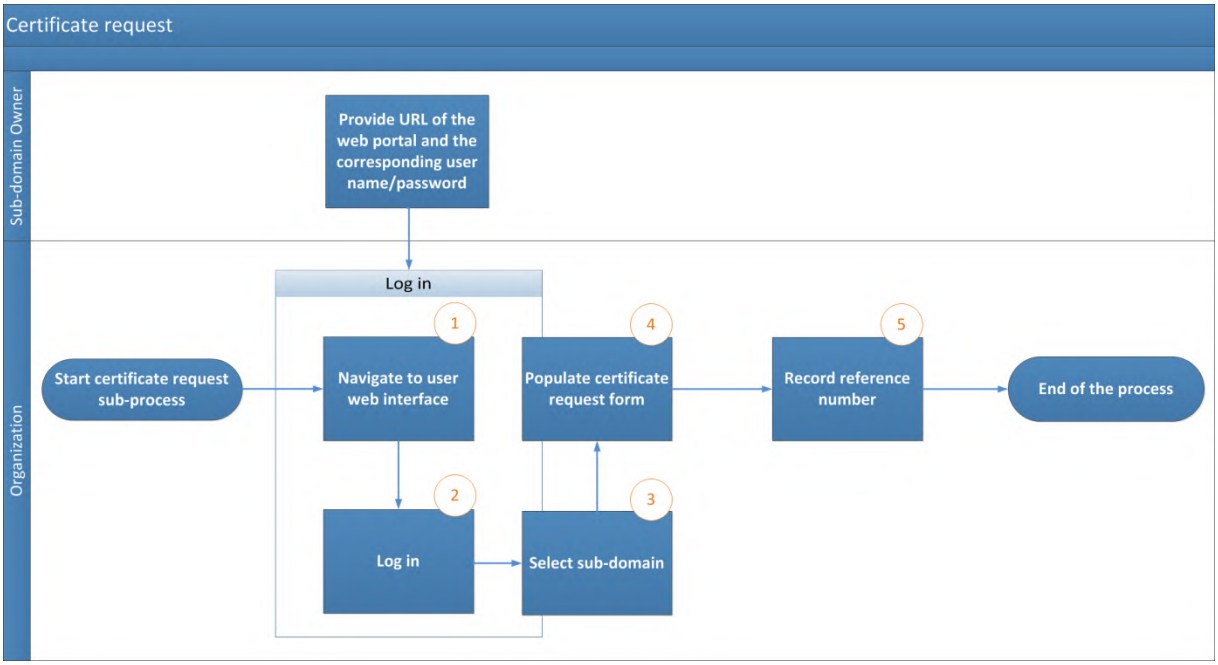


Figura 7 – Processo de pedido de certificado

2.2.4. Etapa 3: Registo junto da autoridade de registo (Aprovação do certificado)

2.2.4.1. O correio fidedigno ou ponto de contacto deve marcar uma reunião com a autoridade de registo através de uma troca de mensagens eletrónicas, identificando o correio fidedigno que será presente à reunião face-a-face.

2.2.4.2. A organização prepara o pacote de documentação que deve consistir no seguinte:

a) procuração preenchida e assinada;

b) cópia do passaporte válido do correio fidedigno que estará presente na reunião. Esta cópia deve ser assinada por um dos pontos de contacto da organização identificados na etapa 1;

c) formulário em papel do pedido de certificado assinado por um dos pontos de contacto da organização.

2.2.4.3. A autoridade de registo recebe o correio fidedigno após um rastreio de identidade na receção do edifício. A autoridade de registo procede ao registo face-a-face do pedido de certificado nos seguintes moldes:

a) identificação e autenticação do correio fidedigno;

b) verificação da aparência física do correio fidedigno contra passaporte apresentado pelo correio fidedigno;

c) verificação da validade do passaporte apresentado pelo correio fidedigno;

d) verificação do passaporte validado apresentado pelo correio fidedigno contra cópia do passaporte válido do correio fidedigno assinada por um dos pontos de contacto identificados da organização. A assinatura é autenticada contra o formulário original de identificação dos pontos de contacto e dos correios fidedignos;

e) verificação da procuração preenchida e assinada;

f) verificação do formulário em papel do pedido de certificado e da respetiva assinatura contra o formulário original de identificação dos pontos de contacto e dos correios fidedignos;

g) chamada a efetuar ao ponto de contacto signatário para voltar a verificar a identidade do correio fidedigno e o teor do pedido de certificado.

2.2.4.4. A autoridade de registo deve confirmar ao balcão de apoio do MIE que a autoridade nacional se encontra de facto autorizada a operar os componentes dos quais pede certificados e que o processo de registo face-a-face correspondente foi bem sucedido. A confirmação deve ser enviada por mensagem eletrónica securizada através de um certificado "CommiSign", juntando uma cópia digitalizada do pacote de documentação autenticada face-a-face e da lista de verificação do processo de assinatura empregue pela autoridade de registo.

2.2.4.5. Se a autoridade de registo confirmar a validade do pedido, o processo deve continuar tal como definido nos pontos 2.2.4.6 e 2.2.4.7. Caso contrário, a emissão de certificados deve ser rejeitada e a organização deve ser informada.

2.2.4.6. O balcão de apoio do MIE deve aprovar o pedido de certificado e deve notificar a autoridade de registo da aprovação do certificado.

2.2.4.7. A autoridade de registo notifica a organização de que o certificado pode ser recebido através do portal de utilizadores.

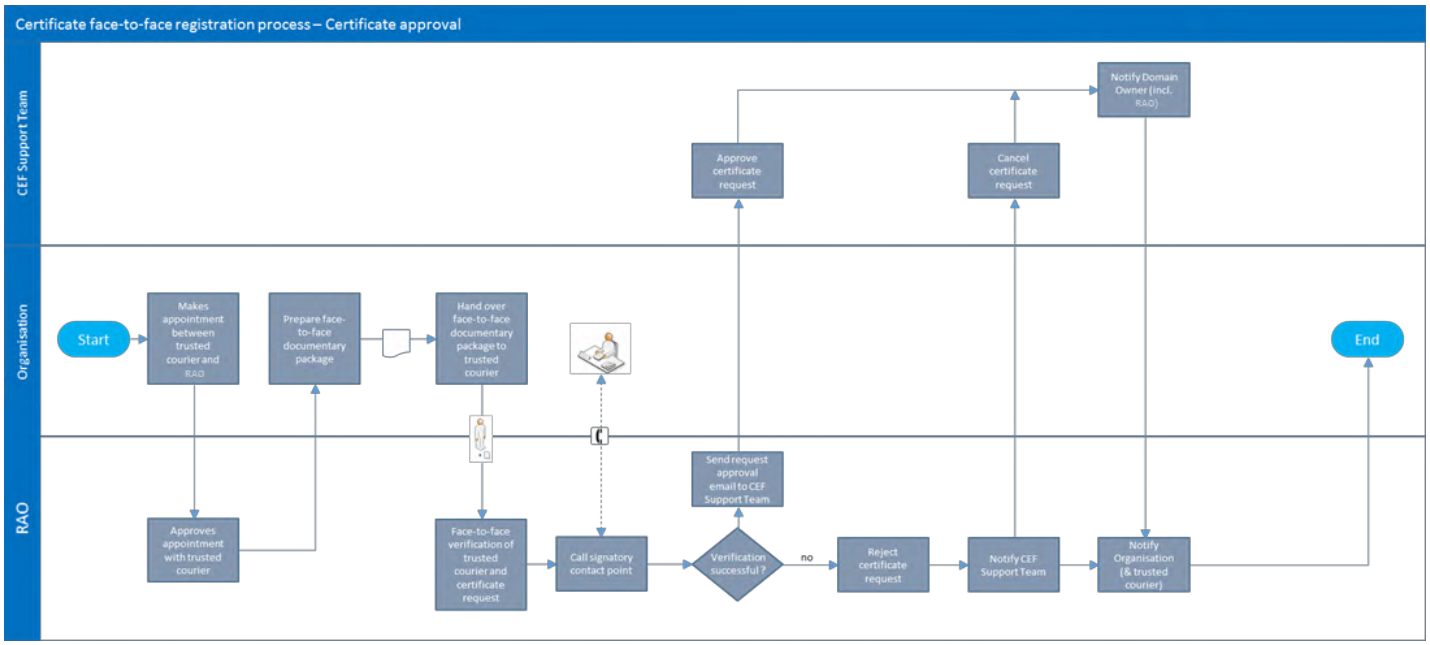


Figura 8 – Aprovação do certificado

2.2.5. Etapa 4: Geração do certificado

Após aprovação do pedido de certificado, o certificado é gerado.

2.2.6. Etapa 5: Publicação e receção do certificado

2.2.6.1. Após aprovação do pedido de certificado, a autoridade de registo pode proceder à receção do certificado e deve entregar uma cópia ao correio fidedigno.

2.2.6.2. A organização recebe a notificação da parte da autoridade de registo e os certificados podem ser rececionados.

2.2.6.3. A organização deve navegar até ao portal de utilizadores em https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en e deve conectar-se com o nome de utilizador "**sbca/CEF_eDelivery.europa.eu**" e a senha "**digit.333**".

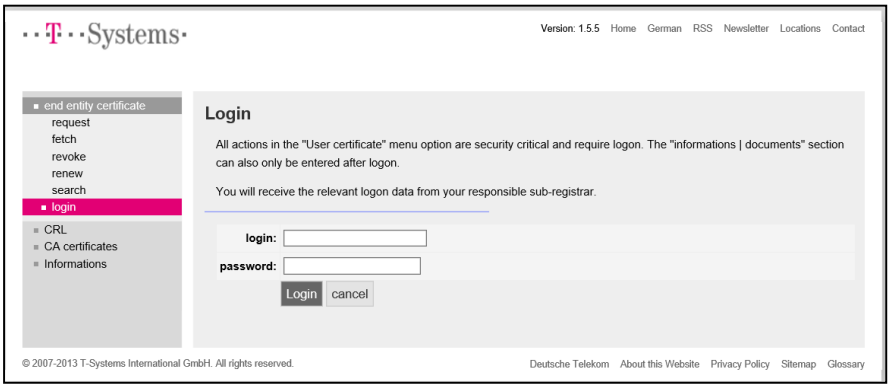


Figura 9

2.2.6.4. A organização deve clicar no botão "obter" no lado esquerdo e deve indicar o número de referência registado durante o processo de pedido de certificado;

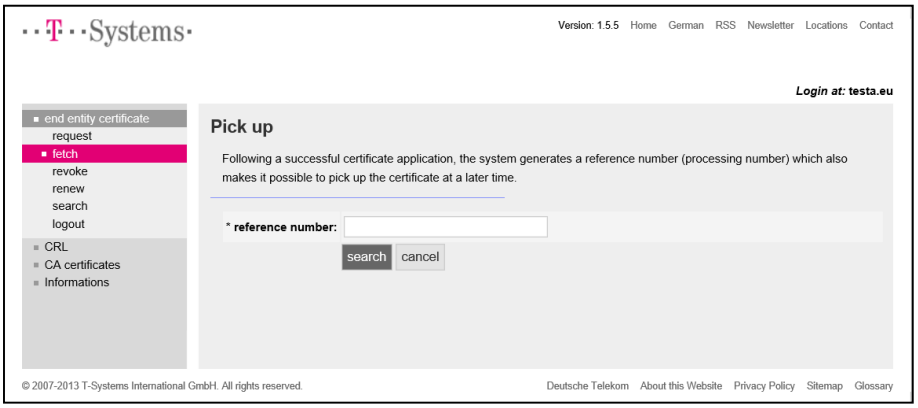


Figura 10

2.2.6.5. A organização deve instalar os certificados clicando no botão "instalar";

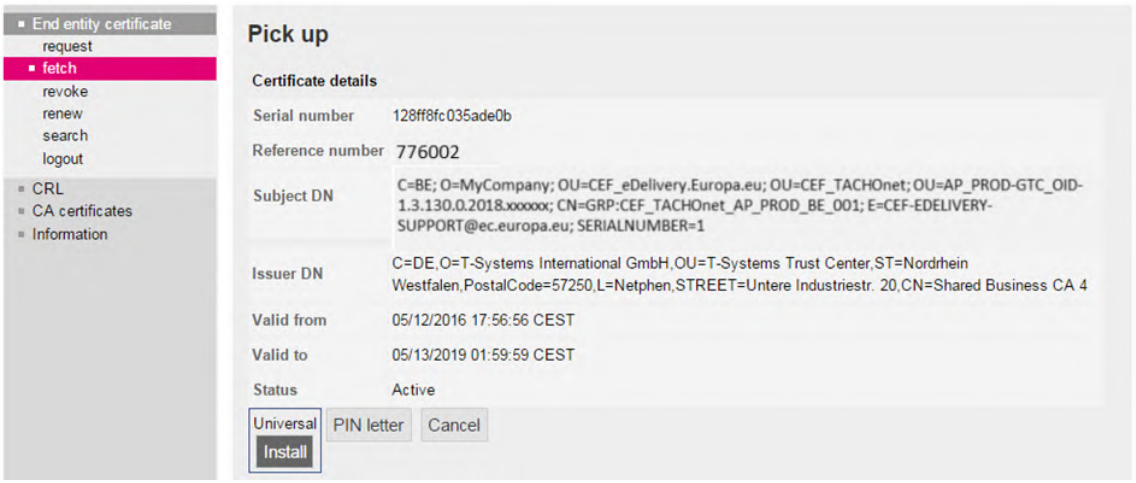


Figura 11

2.2.6.6. O certificado deve ser instalado no ponto de acesso. Como tal depende de cada programa, a organização deve contactar o seu fornecedor de ponto de acesso para obter uma descrição deste processo.

2.2.6.7. São necessárias as seguintes etapas para a instalação do certificado no ponto de acesso:

a) exportar a chave privada e o certificado,

b) criar a keystore e a truststore,

c) instalar a keystore e a truststore no ponto de acesso.

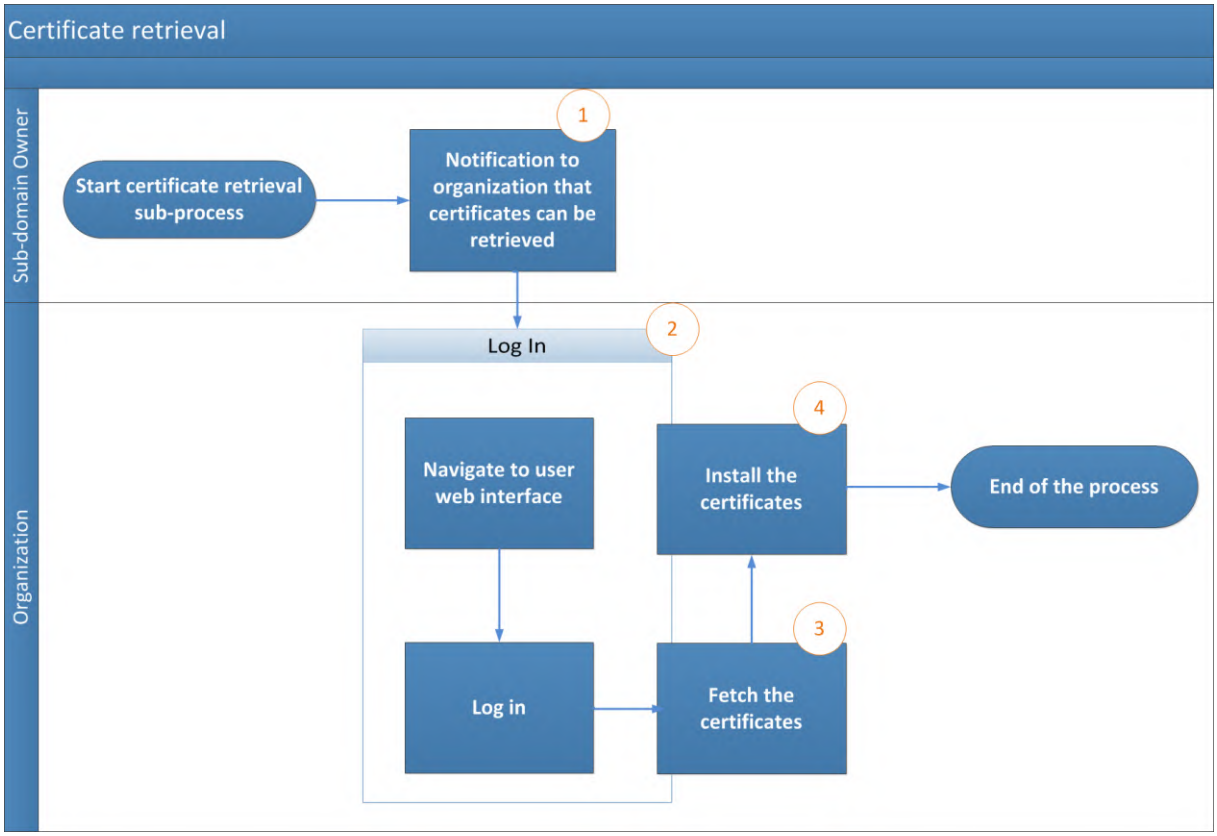


Figura 12 – Receção do certificado

3. Processo de revogação do certificado

3.1. A organização deve apresentar um pedido de revogação através do portal Web de utilizadores;

3.2. O balcão de apoio do MIE executa a revogação do certificado.

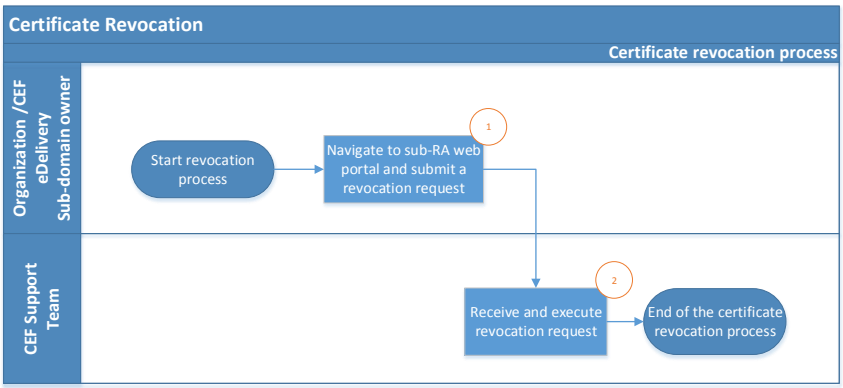


Figura 13 – Revogação do certificado

4. Termos e condições gerais do serviço PKI MIE

4.1. Contexto

Na sua capacidade de solucionador do eDelivery Building Block do Mecanismo Interligar a Europa, a DIGIT disponibiliza um serviço PKI [7]("serviço PKI MIE") às partes contratantes no AETR. O serviço PKI MIE será utilizado pelas autoridades nacionais ("utilizadores finais") que participam no projeto TACHOnet.

A DIGIT compartilha a PKI no âmbito da solução TeleSec Shared-Business-CA ("SBCA") operada no Trust Center da unidade do grupo T-Systems International GmbH ("T-Systems"[8]) A DIGIT desempenha o papel de Master Registrar do domínio "CEF_eDelivery.europa.eu" da SBCA. Neste papel, a DIGIT cria subdomínios no âmbito do domínio "CEF_eDelivery.europa.eu" para cada projeto utilizando o serviço PKI MIE.

Este documento fornece dados sobre os termos e condições do subdomínio TACHOnet. A DIGIT desempenha o papel de sub-Registrar deste subdomínio. Nesta capacidade, emite, revoga e renova os certificados deste projeto.

4.2. Exoneração de responsabilidade

A Comissão Europeia não aceita qualquer responsabilidade relativamente ao teor do certificado, que é da inteira responsabilidade do seu proprietário. É da responsabilidade do proprietário do certificado verificar a exatidão do teor do certificado.

A Comissão Europeia não aceita qualquer responsabilidade relativamente à utilização do certificado pelo seu proprietário, que é uma entidade jurídica terceira fora da Comissão Europeia.

[7]Uma PKI (infraestrutura de chave pública) é composta por um conjunto de papéis, políticas, processos e sistemas necessários para criar, gerir, distribuir e revogar certificados digitais.

[8]O papel fidedigno do operador do Trust Center, localizado no T-Systems Trust Center, também desempenha a tarefa de autoridade de registo interna.

O presente aviso legal não visa limitar a responsabilidade da Comissão Europeia em violação do disposto na legislação nacional aplicável, nem declinar a sua responsabilidade nos casos em que a legislação não o permita.

4.3. Utilizações de certificados autorizadas/proibidas

4.3.1. Utilizações de certificados permitidas

Tendo o certificado sido emitido, o proprietário do certificado[9] deve utilizá-lo apenas no contexto do sistema TACHOnet. Neste contexto, o certificado pode ser utilizado para:

- autenticar a origem dos dados;
- encriptar dados;
- assegurar a deteção de quebras da integridade dos dados.

4.3.2. Utilizações de certificados proibidas

Qualquer utilização não explicitamente autorizada como parte das utilizações permitidas do certificado é proibida.

4.4. Obrigações adicionais do proprietário do certificado

Os termos e condições pormenorizados da SBCA são definidos pela T-Systems na política de certificação (CP)/declaração de práticas de certificação (CPS) do serviço SBCA[10]. Este documento inclui especificações e orientações de segurança relativas a aspetos técnicos e organizativos e descreve as atividades do operador do Trust Center nos papéis de autoridade de certificação (CA) e autoridade de registo (RA), assim como no de terceira parte delegada da autoridade de registo.

Só as entidades autorizadas a participar no projeto TACHOnet podem pedir um certificado.

[9] Identificado pelo valor do atributo "O=" no Nome Distintivo do Sujeito do certificado emitido.

[10] A mais recente versão das CP/CPS SBCA da T-Systems está disponível em https://www.telesec.de/en/sbca-en/support/download-area/.

Relativamente à aceitação do certificado, aplica-se o ponto 4.4.1 da política de certificação e da declaração de práticas de certificação ("CP/CPS") SBCA, sendo que os termos e disposições de utilização descritos no presente documento são considerados aceites pela organização à qual o certificado é emitido ("O=") quando primeiramente utilizado.

Relativamente à publicação do certificado, aplica-se o ponto 2.2 das CP/CPS SBCA.

Todos os proprietários de certificado devem respeitar as seguintes condições:

1) protegem a sua chave privada contra qualquer utilização não autorizada;

2) evitam a transferência ou a revelação das chaves privadas a terceiros, mesmo representantes;

3) evitam a utilização prolongada das chaves privadas depois de expirado o período de validade ou de revogação do certificado, exceto para visualização de dados encriptados (por exemplo, para desencriptagem de correio eletrónico).

4) o proprietário do certificado é responsável por copiar ou reenviar a chave ao utilizador final;

5) o proprietário do certificado deve obrigar o utilizador final a cumprir os presentes termos e condições, incluindo as CP/CPS SBCA, sempre que manuseia a chave privada.

6) O proprietário do certificado deve providenciar a identificação dos representantes autorizados a pedir a revogação dos certificados emitidos à organização juntamente com os pormenores dos incidentes que conduziram à revogação e com a senha de revogação.

7) Nos certificados associados a grupos de pessoas e funções e/ou pessoas coletivas, depois de uma pessoa abandonar o grupo de utilizadores finais (por exemplo, fim do vínculo laboral), o proprietário do certificado deve impedir a utilização abusiva da chave privada através da revogação do certificado.

8) O proprietário do certificado é responsável, devendo solicitar a revogação do certificado nas circunstâncias referidas no ponto 4.9.1 das CP/CPS SBCA.

Relativamente à renovação ou reemissão de chave de certificados, aplica-se o ponto 4.6 ou 4.7 das CP/CPS SBCA.

Relativamente à alteração do certificado, aplica-se o ponto 4.8 das CP/CPS SBCA.

Relativamente à revogação do certificado, aplica-se o ponto 4.9 das CP/CPS SBCA.

5. Formulário de identificação das pessoas de contacto e dos correios fidedignos (amostra)

Eu, *abaixo assinado [nome e endereço da organização representante]*, **certifico que as informações seguintes devem ser utilizadas no contexto do pedido, geração e receção de certificados digitais de chave pública para pontos de acesso TACHOnet que apoiem a confidencialidade, a integridade e o não repúdio das mensagens TACHOnet:**

Dados da pessoa de contacto**:**

– **Pessoa de contacto #1**	– **Pessoa de contacto #2**
– Nome:	– Nome:
– Nome próprio:	– Nome próprio:
– Telemóvel:	– Telemóvel:
– Telefone:	– Telefone:
– Endereço eletrónico:	– Endereço eletrónico:
– Exemplo de assinatura manuscrita: –	– Exemplo de assinatura manuscrita: – – –

Identificação do correio fidedigno**:**

– **Correio fidedigno #1**	– **Correio fidedigno #2**
– Nome:	– Nome:
– Nome próprio:	– Nome próprio:
– Telemóvel:	– Telemóvel:
– Endereço eletrónico:	– Endereço eletrónico:
– País de emissão do passaporte:	– País de emissão do passaporte:
– Número do passaporte:	– Número do passaporte:
– Data de final de validade do passaporte:	– Data de final de validade do passaporte:

Lugar, data, carimbo da empresa ou selo da organização:

Assinatura do representante autorizado:

6. Documentos

6.1. Procuração individual (modelo)

Pode encontrar uma amostra da procuração individual que deve ser assinada e apresentada pelo correio fidedigno durante o registo face-a-face na organização da autoridade de registo aqui:

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. Formulário em papel do pedido de certificado (modelo)

Pode encontrar um modelo do formulário em papel do pedido de certificado que deve ser assinado e apresentado pelo correio fidedigno durante o registo face-a-face na organização da autoridade de registo aqui:

7. Glossário

Os principais termos utilizados no presente subapêndice são definidos na secção de definições MIE do Portal Web Digital MIE:

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

Os principais acrónimos utilizados neste subapêndice são definidos no Glossário MIE do Portal Web Digital MIE:

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