Distr.: General
30 May 2018

English only

Economic Commission for Europe

Inland Transport Committee

Working Party on Road Transport

Group of Experts on European Agreement Concerning Work of Crews of Vehicles Engaged in International Road Transport (AETR)

Eighteenth session
Geneva, 4 June 2018
Item 4 of the provisional agenda
TACHOnet

TACHOnet

Submitted by the European Commission

This document is submitted by the European Commission. It replaces Informal document No. 2. It lists provisional rules for the connection of AETR Contracting Parties to TACHOnet.

Note: this draft has been submitted to the UNECE Secretariat as informal document. It has not been approved by the European Commission, and it is therefore only intended for discussion

Rules for the connection of AETR Contracting Parties to TACHOnet (the rules are provisional and subject to discussion with the competent services from the European Commission and with EU Member States)

Article 1

Scope and purpose

1. The present document sets out the terms and conditions regarding the connection of the parties to TACHOnet.

2. The parties connecting to TACHOnet which are not Member States to the EU shall abide by the provisions laid down in [this document].

3 Parties connecting to TACHOnet which are Member States to the EU may connect to TACHOnet under the terms and conditions specified in [this document], in which case they shall abide by the provisions laid down in it.

Article 2

Definitions

a) ‘Contracting party’ means any Contracting party to the AETR;

b) ‘TACHOnet’ means the system for the electronic exchange of information on driver cards between contracting parties.

c) ‘Requesting party’ means the contracting party emitting a TACHOnet request or a notification, which is then routed to the appropriate responding party by the central hub;

d) ‘Responding party’ means the contracting party to whom the TACHOnet request or notification is addressed;

e) ‘Card issuing authority’ or ‘CIA’ means the entity empowered by a contracting party for the issuing and management of tachograph cards;

Article 3

Legal and technical requirements

The contracting parties connecting to TACHOnet shall fulfil the legal and technical requirements set out in [this document], including its Annexes.

Article 4

General responsibilities

1. Neither contracting party may conclude agreements for the access to TACHOnet on behalf of other party or in any other way represent the other contracting party on the basis of [this document]. Neither contracting party acts as the other contracting party's subcontractor in the operations referred to in [this document].

2. The contracting parties shall provide access to their national register on driver cards through TACHOnet, in the way and with the level of service as defined in Annex VI.

3. The parties shall notify each other without delay if they observe disturbances or errors within their domain of responsibility, which may endanger the fulfilling of the normal operation of TACHOnet.

4. Each party shall designate contact persons for TACHOnet. Any change in contact points must be provided to the AETR Secretariat in writing.

Article 5

Tests for connection to TACHOnet

1. The connection of a contracting party to TACHOnet shall be established after the successful completion of the connection, integration and performance tests in accordance with the instructions and under the supervision of the European Commission.

2. In case of failure of the preliminary tests, the European Commission may temporarily put on hold the testing phase. The tests shall resume once the contracting party has communicated to the European Commission the adoption of the necessary technical improvements at national level, allowing the successful performance of the preliminary tests.

3. The maximum duration of the preliminary tests shall be six months.

Article 6

Trust architecture

1. Confidentiality, integrity and non-repudiation of the TACHOnet messages shall be ensured by the TACHOnet trust architecture.

2 The TACHOnet trust architecture shall be based on a public key infrastructure (PKI) service set up by the European Commission, which requirements are laid down in Annex VIII.

3. The following entities shall intervene in the TACHOnet trust architecture:

a) Certification Authority, responsible for the generation of the digital certificates to be delivered by the Registration Authority to the national authorities of the contracting parties (via trusted couriers appointed by them), as well as for setting up the technical infrastructure regarding the issuance, revocation and renewal of digital certificates.

b) Domain Owner, responsible for the operation of the central hub and for the general validation and coordination of the TACHOnet trust architecture.

c) Registration Authority, responsible for registering and approving the requests of issuance, revocation and renewal of digital certificates, and for verifying the identity of the trusted couriers.

d) Trusted Courier, is the person appointed by the national authorities, responsible for handing the public key to the Registration Authority and for getting the corresponding certificate being generated by the Certification Authority.

e) National authority from the contracting party, which shall:

- generate the private keys and the corresponding public keys to be included in the certificates to be generated by the Certification Authority;

- request the digital certificates to the Registration Authority;

- appoint the Trusted Courier.

4. The Certification Authority and the Registration Authority shall be appointed by the European Commission.

5. Any contracting party connecting to TACHOnet must request the issuance of a digital certificate in accordance with Annex VIII, in order to sign and encrypt a TACHOnet message.

6. A certificate may be revoked in accordance with Annex VIII.

Article 7

Data protection and confidentiality

1. The parties, in compliance with data protection laws at international and national level, and in particular with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, shall adopt all necessary technical and organisational measures to guarantee the security of the TACHOnet data and prevent the alteration or loss of, or unauthorised processing of or access to such data (in particular the authenticity, data confidentiality, traceability, integrity, availability and non-repudiation and security of the messages).

2. Each party shall protect its own national systems against illicit use, malicious code, viruses, computer intrusions, infringements and illegal tampering of data and other comparable actions by third parties. The parties agrees to use commercially reasonable efforts to avoid the transmission of any viruses, time bombs, worms or

similar items or any computer programming routines that may interfere with other Party’s computer systems.

Article 8

Costs

1. The parties shall bear their own development and operation costs in conjunction to their own data systems and procedures as required to fulfil the obligations according to [this document].

2. The services specified in Annex I, provided by the central hub, are free of charge.

Article 9

Subcontracting

1. The parties may subcontract any of the services for which they are responsible under [this document].

2. Such subcontracting does not relieve the party from the responsibility pursuant to [this document], including the responsibility for the appropriate level of service in accordance with Annex VI.

ANNEX I

General aspects of TACHOnet

1. General description

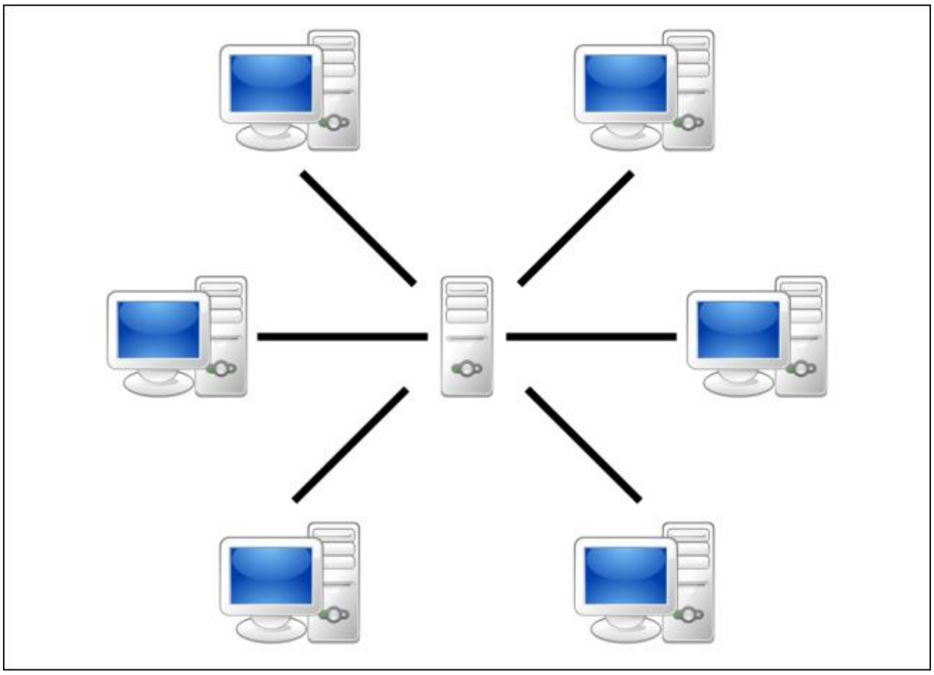
TACHOnet is an electronic system for the exchange of information on driver cards between AETR contracting parties. TACHOnet network routes the requests for information from the requesting parties to the responding parties, as well as the replies from the latter to the former. Contracting parties being part of TACHOnet must connect their national registers on driver cards to the system.

2. Architecture

TACHOnet messaging system shall be composed of the following parts:

1.1. A central hub, which shall be able to receive a request from the requesting party, validate it and process it by forwarding it to the responding parties. The central hub shall wait for each responding party to answer, consolidate all the answers and forward the consolidated response to the requesting Party.

1.2. National systems of the parties, which shall be fitted with an interface capable of both sending requests to the central hub and receiving the corresponding replies. National systems may use propriety or commercial software to transmit and receive messages from the central hub.



3. Management

3.1. The central hub shall be managed by the European Commission, which shall be responsible for the technical operation and maintenance of the central hub.

2.2. The central hub shall not store data for a period exceeding six months, other than the logging and statistical data set out in Annex VII.

2.3. The central hub shall not provide access to personal data, except for authorized European Commission personnel, when necessary for the purpose of monitoring, maintenance and troubleshooting.

2.4. Each contracting party shall be responsible for:

2.4.1. The setup and management of their national systems, including the interface with the central hub.

2.4.2. The installation and maintenance of their national system, both hardware and software, whether proprietary or commercial.

2.4.3. The correct interoperability of their national system with the central hub, including the management of error messages received from the central hub.

2.4.4. Taking all the measures to ensure the confidentiality, integrity and availability of the information.

2.4.5. The operation of the national systems in accordance with the service levels set out in Annex VI.

ANNEX II

Functionalities of TACHOnet

1. The following functionalities shall be provided through TACHOnet messaging system:

1.1. Check Issued Cards (CIC): allows the requesting party to send a Check Issued Cards Request to one or all responding parties, to determine if a card applicant already possesses a driver card issued by the responding parties. The responding parties shall reply to the request by sending a Check Issued Cards Response.

1.2. Check Card Status (CCS): allows the requesting party to ask the responding Party about the details of a card issued by the latter by sending a Check Card Status Request. The responding party shall reply to the request by sending a Check Card Status Response.

1.3. Modify Card Status (MCS): allows the requesting party to notify the responding Party, through a Modify Card Status Request, that the status of a card issued by the latter has changed. The responding party shall reply with a Modify Card Status Acknowledgement.

1.4. Issued Card Driving License (ICDL): allows the requesting party to notify the responding party, through an Issued Card Driving Licence Request, that a card has been issued by the former against a driving licence issued by the latter. The responding party shall reply with an Issued Card Driving Licence Response.

2. Other message types deemed suitable for the efficient functioning of TACHOnet shall be included, for instance error notifications.

3. National systems shall recognize the card statuses listed in the Appendix to this Annex, when using any of the functionalities described in point 1. However, parties are not required to implement an administrative procedure that makes use of all of the listed statuses.

4. When a party receives a response or notification giving a status that is not used in its administrative procedures, the national system shall translate the status on the received message to the appropriate value in that procedure. The message shall not be rejected by the responding party, as long as the status in the message is listed in the Appendix of this Annex.

5. The card status listed in the Appendix to this Annex shall not be used to determine if a driver card is valid for driving. When a party queries the register of the card issuing national authority via the CCS functionality, the response shall contain the dedicated field ‘valid for driving’. The national administrative procedures shall be such that CCS responses always contain the appropriate ‘valid for driving’ value.

Appendix

Card statuses

Card Status	Definition
Application	The CIA has received an application to issue a driver card. This information has been registered and stored in the database with the generated search keys.
Approved	The CIA has approved the application for the tachograph card.
Rejected	The CIA did not approve the application.
Personalised	The tachograph card has been personalised.
Dispatched	The National Authority has dispatched the driver card to the relevant driver or delivering agency.
Handed Over	The National Authority has handed over the driver card to the relevant driver.
Confiscated	The driver card has been taken from the driver by the competent authority.
Suspended	The driver card has been taken temporarily from the driver.
Withdrawn	The CIA has decided to withdraw the driver card. The card has been permanently invalidated.
Surrendered	The tachograph card has been returned to the CIA, and declared no longer needed.
Lost	The tachograph card has been declared lost to the CIA.
Stolen	The tachograph card has been reported stolen to the CIA. A stolen card is considered lost.
Malfunctioning	The tachograph card has been reported as malfunctioning to the CIA.
Expired	The period of validity of the tachograph card has expired.
Replaced	The tachograph card, which has been reported lost, stolen or malfunctioning, has been replaced by a new card. The data on the new card is the same, with the exception of the card number replacement index, which has been increased by one.
Renewed	The tachograph card has been renewed because of a change of administrative data or the validity period coming to an end. The card number of the new card is the same, with the exception of the card number renewal index, which has been increased by one.
In Exchange	The CIA that issued a driver card has received a notification that the procedure to exchange that card for a driver card issued by the CIA of another Party has started.

Card Status	Definition
Exchanged	The CIA that issued a driver card has received a notification that the procedure to exchange that card for a driver card issued by the CIA of another Party has completed.

ANNEX III

Message provisions of TACHOnet

1. General technical requirements

1.1. The central hub shall provide both synchronous and asynchronous interfaces for the exchange of messages. Parties may choose the most suitable technology to interface with their own applications.

1.2. All messages exchanged between the central hub and the national systems must be UTF-8 encoded.

1.3. National systems shall be capable of receiving and processing messages containing Greek or Cyrillic characters.

2. XML messages structure and Schema definition (XSD)

2.1. The general structure of XML messages shall follow the format defined by the XSD schemas installed in the central hub.

2.2. The central hub and the national systems shall transmit and receive messages that conform to the message XSD schema.

2.3. National systems shall be capable of sending, receiving and processing all messages corresponding to any of the functionalities set out in Annex I.

2.4. The XML messages shall include at least the minimum requirements laid down in the Appendix to this Annex.

Appendix

Minimum requirements for the content of the XML messages

Common Header		Mandatory
Version	The official version of the XML specifications will be specified through the namespace defined in the message XSD and in the *version* attribute of the Header element of any XML message. The version number ('n.m') will be defined as fixed value in every release of the XML Schema Definition file (xsd).	Yes
Test Identifier	Optional id for testing. The originator of the test will populate the id and all participants in the workflow will forward / return the same id. In production it should be ignored and will not be used if it is supplied.	No
Technical Identifier	A UUID uniquely identifying each individual message. The sender generates a UUID and populates this attribute. This data is not used in any business capacity.	Yes
Workflow Identifier	The workflowId is a UUID and should be generated by the requesting Party. This id is then used in all messages to correlate the workflow.	Yes
Sent At	The date and time (UTC) that the message was sent.	Yes
Timeout	This is an optional date and time (in UTC format) attribute. This value will be set only by the Hub for forwarded requests. This will inform the responding party of the time when the request will be timed out. This value is not required in MS2TCN_<x>_Req and all response messages. It is optional so that the same header definition can be used for all message types regardless of whether or not the timeoutValue attribute is required.	No
From	The ISO 3166-1 Alpha 2 code of the party sending the message or 'EU'.	Yes
To	The ISO 3166-1 Alpha 2 code of the party to which the message is being sent or 'EU'.	Yes

ANNEX IV

Transliteration and NYSIIS (New York State Identification and Intelligence System) Services

1. The NYSIIS algorithm implemented in the central hub shall be used to encode the names of all the drivers in the national register.

2. When searching for a card via the CIC functionality the NYSIIS keys shall be used as the primary search mechanism.

3. Additionally, parties may employ a custom algorithm to return additional results.

4. The search results shall indicate the search mechanism which was used to find a record, either NYSIIS or custom.

5. If a party chooses to record ICDL notifications then the NYSIIS keys contained in the notification shall be recorded as part of the ICDL data.

5.1 When searching the ICDL data the party shall use the NYSIIS keys of the applicant’s name.

ANNEX V

Security requirements

1. HTTPS shall be used for the exchange of messages between the central hub and the national systems.

2. National systems shall use the PKI certificates provided by the European Commission for the purposes of securing the transmission of messages between the national system and the central hub.

3. National systems shall implement, as a minimum, certificates using the SHA-2 (SHA-256) signature hash algorithm and a 2048 bit public key length.

ANNEX VI

Service levels

1. National systems shall fulfil the following minimum level of service:

1.1. They shall be available 24 hours a day, 7 days a week.

1.2. Their availability shall be monitored by a heartbeat message issued from the central hub.

1.3. Their availability rate shall be 98%, according to the following table (the figures have been rounded to the nearest convenient unit):

An availability of	means an unavailability of		
	Daily	Monthly	Yearly
98%	0.5 hours	15 hours	7.5 days

Parties are encouraged to respect the daily availability rate, however it is recognised that certain necessary activities, such as system maintenance, require a down time of more than 30 minutes. However, the monthly and yearly availability rates remain mandatory.

1.4. They shall respond to a minimum of 98% of the requests forwarded to them in one calendar month.

1.5. They shall respond to requests within 10 seconds.

1.6 The global request timeout (time within which the requestor may wait for a response) shall not exceed 20 seconds.

1.7. They shall be able to service a request rate of 6 messages per second.

1.8. National systems may not send requests to the TACHOnet hub at a rate exceeding 2 requests per second.

1.9. Every national system shall be able to cope with potential technical problems of the central hub or national systems in other parties. These include, but are not limited to:

(a) loss of connection to the central hub;

(b) no response to a request;

(c) receipt of responses after message timeout;

(d) receipt of unsolicited messages;

(e) receipt of invalid messages.

2. The central hub shall:

2.1. feature an availability rate of 98%;

2.2. provide to national systems notification of any errors, either via the response message or via a dedicated error message. The national systems, in turn, shall receive these dedicated error messages and have an escalation workflow in place to take any appropriate action to rectify the notified error.

3. Maintenance

Parties shall notify other parties and the European Commission of any routine maintenance activities via the web application, at least one week before the beginning of those activities if technically possible.

ANNEX VII

Logging and Statistics of the data collected at the central hub

1. In order to ensure privacy, the data for statistical purposes shall be anonymous. Data identifying a specific card, driver or driver licence shall not be available for statistical purposes.

2. Logging information shall keep track of all transactions for monitoring and debugging purposes, and allow the generation of statistics about these transactions.

3. Personal data shall not be retained in the logs for more than 6 months. Statistical information shall be retained indefinitely.

4. The statistical data used for reporting shall include:

(a) the requesting party;

(b) the responding party;

(c) the type of message;

(d) the status code of the response;

(e) the date and time of the messages;

(f) the response time.

ANNEX VIII

PKI service for TACHOnet

1. The Directorate General for Informatics of the European Commission (DIGIT) shall make available a PKI service[1] (referred to as "CEF PKI service") to the AETR Contracting Parties connecting to TACHOnet (henceforth the national authorities).

2. The procedure for request and revocation of TACHOnet certificates, as well as the detailed terms and conditions for its usage, are defined in the Appendix

3. Usage of certificates:

3.1. Once the certificate is issued, the national authority[2], shall use the certificate only in the context of TACHOnet. The certificate can be used to:

a) authenticate the origin of data;

b) encrypt data;

c) ensure detection of integrity breaches of data.

3.2. Any usage not explicitly authorised as part of the permitted usages of the certificate is prohibited.

4. Contracting parties shall:

a) Protect their private key against unauthorized use.

b) Refrain from transferring or revealing their private key to third parties, even as representatives.

c) Ensure confidentiality, integrity, and availability of the private keys generated, stored and used for TACHOnet.

d) Refrain from continued use of the private key following expiry of the validity period or revocation of the certificate, other than to view encrypted data (e.g., decrypting e-mails). Expired keys shall be either destroyed or retained in a manner preventing its use.

e) Provide the Registration Authority with the identification of those authorised representatives who are authorized to request revocation of certificates issued to the organisation (revocation requests shall include a revocation request password and details about the events that lead to revocation).

f) Prevent misuse of the private key by requesting the revocation of the associated public key certificate in case of compromise of the private key or of the private key activation data.

[1] A PKI (Public Key Infrastructure) is a set of roles, policies, procedures and systems needed to create, manage, distribute, and revoke digital certificates.

[2] Identified by the "O=" attribute value in the Subject Distinguished Name of the issued certificate

g) Be responsible and hold the obligation of requesting revocation of certificate under circumstances identified in the certification policies (CP) and certification practices statement (CPS) of the Certification Authority.

h) Notify the Registration Authority without delay of loss, theft, or potential compromise of any AETR keys used in the context of TACHOnet.

5. Liabilities

Without prejudice of the liability of the European Commission in contravention of any requirements laid down in applicable national law or with respect to liability for matters which may not be excluded under that law, the European Commission shall not be responsible or liable with regard to:

a) the content of the certificate which lies exclusively with the certificate owner. It shall be the responsibility of the certificate owner to check the accuracy of the certificate content.

b) the use of the certificate by its owner.

Appendix

Public Key Infrastructure

Service Offering Description

PKI for TACHOnet

Table of Contents

1. Introduction

A PKI (Public Key Infrastructure) is a set of roles, policies, procedures and systems needed to create, manage, distribute, and revoke digital certificates[3]. The PKI service of CEF eDelivery enables issuance and management of digital certificates used to ensure confidentiality, integrity and non-repudiation of the information exchanged between the eDelivery components i.e. between Access Points (AP).

The PKI service of CEF eDelivery is based on the Trust Center Services TeleSec Shared Business CA (Certification Authority) for which the Certificate Policy (CP) / Certification Practices Statement (CPS) of TeleSec Shared-Business-CA of T-Systems International GmbH[4] apply.

The CEF PKI service issues certificates that are suitable for securing various business processes within and outside of companies, organisations, public authorities and institutions that require a medium security level to prove the authenticity, integrity and trustworthiness of the end-entity.

In the annex at the end of this document, you will find the procedures to create the Keystores, Truststores and their corresponding configuration in Domibus.

This document provides details on the issuance of the certificates for the Organisations participating to the TACHOnet project.

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

[4] The latest version of the CP and CPS can be downloaded on https://www.telesec.de/en/sbca-en/support/download-area/

2. CERTIFICATE REQUEST PROCESS

This section describes the complete certificate issuance workflow and associated processes that lead to the publication of certificates for use in the TACHOnet project as they are generated by the CEF eDelivery PKI Service.

Remarks:

- *The PKI service Shared Business CA does not support Windows 10. Please only use Windows 7.*
- *Please use Mozilla Firefox whenever possible which works well with the T-Systems Portal.*
- *Google Chrome cannot be used as it has disabled key generation.*

2.1. Roles and Responsibilities

2.1.1. The "Organisation" or the "national authority" requesting the certificate

Entity: National Authority.

Role: Organisation which is requesting the certificates in the context of the TACHOnet project.

Responsibilities:

- Requests the services of the CEF PKI service to get the valid certificates.
- Generate the private keys and the corresponding public keys to be included in the certificates issued by the Certification Authority (CA).
- Download the certificate when approved.
- Sign and send back to the RA
  - The contact persons and trusted couriers identification form;
  - The signed individual Power of Attorney[5].

[5] A power of attorney is a legal document by which the Organisation empowers and authorises the European Commission represented by the identified official responsible for the CEF PKI service the power to request the generation of a certificate on its behalf from the T-Systems International GmbH TeleSec Shared Business CA. See also §5.9 - Contact persons and trusted couriers identification form (sample)

Please print the text of this document on your letterhead, add your organisation stamp and have it signed by an authorised representative of your organisation.

TACHOnet contact persons and trusted couriers identification form

I, *[name and address of the organisation representative]***, certifies that the following information are to be used in the context of the request, generation and retrieval of public key digital certificates for TACHOnet access points supporting the confidentiality, integrity and non-repudiation of the TACHOnet messages:**

Contact person information**:**

Contact person #12	**Contact person #2F**
Name:	Name: t
First names::	First names:n
Mobile phone::	Mobile phone:T
Telephone::	Telephone:m
Email::	Email:
Specimen handwritten signature:	Specimen handwritten signature:

Please duplicate the above table when more than two contact persons are required.

Trusted courier information**:**

Trusted courier #12	**Trusted courier #2i**
Name:	Name: t
First names:	First names:b obile phone:onbbile phone:: mail:aiaail:as assport issuing country:trsssport g country:assport assport number:besssport :umber:sp assport validity end date:atsssport validity end cate th ***Please duplicate the above table when more than two contact persons are required.***
Mobile phone::	Mobile phone:l
Email::	Email:p
Passport issuing country::	Passport issuing country:r
Passport number::	Passport number:i
Passport validity end date::	Passport validity end date:e

Please duplicate the above table when more than two contact persons are required.

Please attach a high resolution copy of page 2 of the passport for all trusted couriers.

Place, date, company stamp or seal of the Organisation:

Signature of the authorised representative:

2.1.2. The Trusted Courier

Entity: A Trusted Courier is a natural person appointed by the responsible for handing the public key to the Registration Authority and for getting the corresponding certificate from the Registration Authority.

Role: Execute the face-to-face presentation against the Registration Authority, representing the Organisation that is requesting the certificates.

Responsibilities:

- Hands over the public key to the Registration Authority during a face-to-face identification and registration process,
- Gets the corresponding certificate from the Registration Authority.

2.1.3. The Domain Owner

Entity: DG MOVE, acting as the TACHOnet project owner.

Role: Entity responsible for the project and project domain, namely the TACHOnet project, in which the certificates will be used. Also referred to as the "Domain owner" or "Sub-domain owner".

Responsibilities:

- General validation and coordination of the TACHOnet trust architecture, including validation of the procedures for the issuance of the certificates;
- Operate the TACHOnet central hub;
- Perform, along with national authorities, the test of connection to TACHOnet.

2.1.4. The Registration Authority

Entity: DG JRC.

Role: The registration authority is the entity responsible for verifying the identity of the trusted courier, for registering and approving the requests of issuance, revocation and renewal of digital certificates.

Responsibilities: Acting as registration authority (RA)

- Assign the unique identifier to the requesting organisation.
- Authenticate the identity of the requesting organisation, its contact points and trusted couriers.

Individual Power of Attorney (sample).

- Communicate with the CEF Support regarding the authenticity of requesting organisation, its contact points and trusted couriers.
- Inform the requesting organisation about the approval or rejection of certificate.

2.1.5. *CEF Support*

Role: CEF PKI Service owner.

Responsibilities:

- Provide for the technical infrastructure for certificate requests by national authorities.
- Validate or reject certificate request.
- Communicate with the registration authority for the identity verification of the requesting organisation, when required.
- Act as the technical single point of contact to the requesting organisation, domain owner, registration authority and provide support for queries related to CEF PKI Services.

2.2. Certificate Issuance Workflow

Purpose: Organisation to obtain PKI certificates for the TACHOnet access points.

Actors:

- Organisation operating the access point (AP);
- Domain Owner;
- CEF Support Team.

Process: This process consists of the following sequential steps:

- **Step 1:** Trusted courier identification
- **Step 2:** Certificate request creation;
- **Step 3**: Registration at RA;
- **Step 4:** Certificate generation;
- **Step 5:** Certificate publication;
- **Step 6:** Certificate acceptance.

The overview of the certificate issuance workflow is shown in the diagram below.

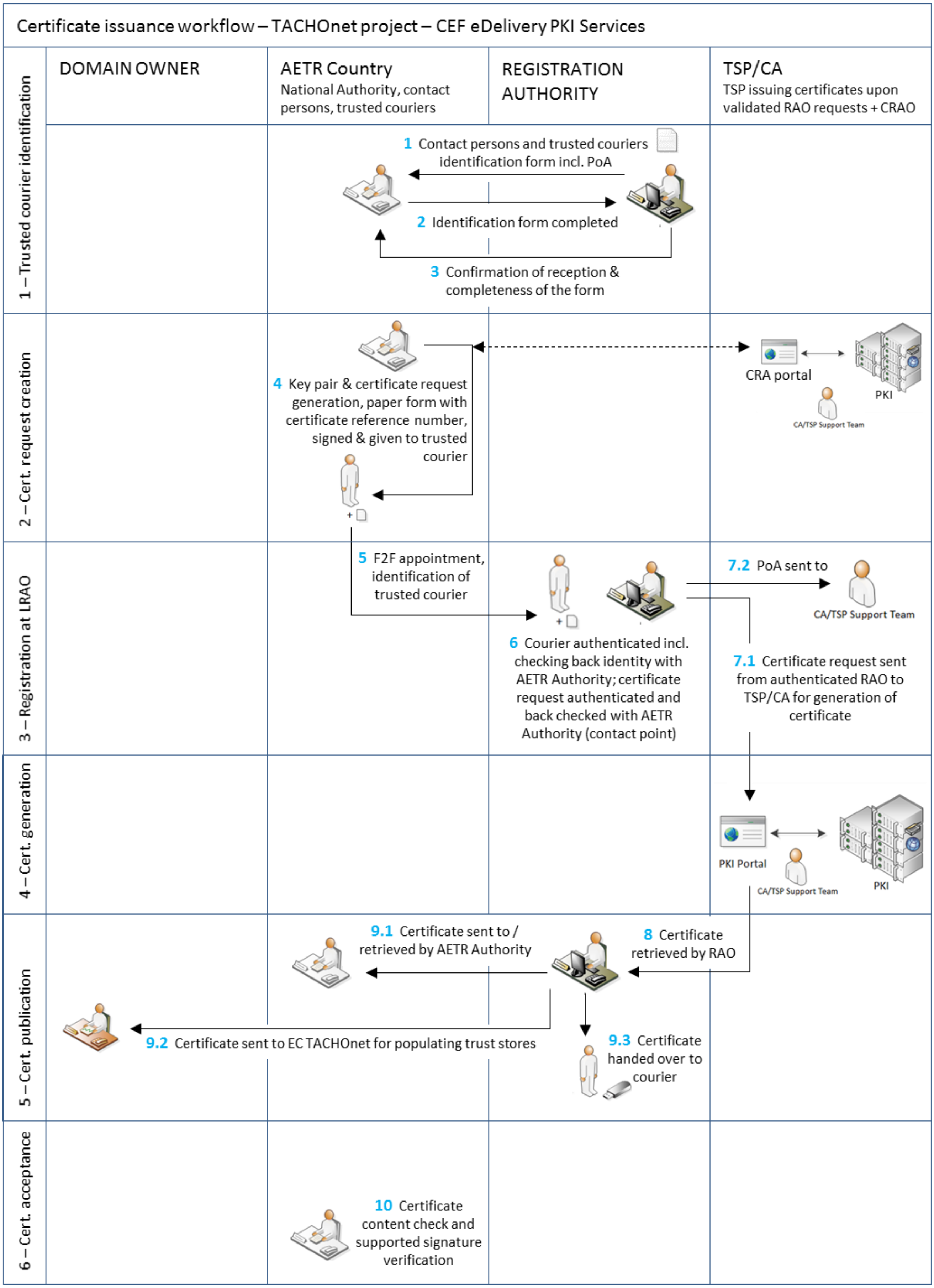

Certificate issuance workflow – TACHOnet project – CEF eDelivery PKI Services
DOMAIN OWNER
AETR Country
National Authority, contact persons, trusted couriers
REGISTRATION AUTHORITY
TSP/CA
TSP issuing certificates upon validated RAO requests + CRAO
1 – Trusted courier identification
1 Contact persons and trusted couriers identification form incl. PoA
2 Identification form completed
3 Confirmation of reception & completeness of the form
2 – Cert. request creation
4 Key pair & certificate request generation, paper form with certificate reference number, signed & given to trusted courier
CRA portal
PKI
CA/TSP Support Team
3 – Registration at LRAO
5 F2F appointment, identification of trusted courier
6 Courier authenticated incl. checking back identity with AETR Authority; certificate request authenticated and back checked with AETR Authority (contact point)
7.2 PoA sent to
CA/TSP Support Team
7.1 Certificate request sent from authenticated RAO to TSP/CA for generation of certificate
4 – Cert. generation
PKI Portal
CA/TSP Support Team
PKI
5 – Cert. publication
9.1 Certificate sent to / retrieved by AETR Authority
8 Certificate retrieved by RAO
9.2 Certificate sent to EC TACHOnet for populating trust stores
9.3 Certificate handed over to courier
6 – Cert. acceptance
10 Certificate content check and supported signature verification

Figure 1 - Certificate issuance workflow

2.2.1. *Step 1: Trusted courier identification*

Purpose: To enable service providers to submit a request for PKI certificates for APs.

Actors:

- Organisation;
- Domain owner.

Process:

1. RA sends to the national authority the contact persons and trusted couriers' identification form[6]. This form also include a power of attorney (PoA) the organisation (AETR Authority) needs to sign.
2. The national authority sends back the completed form and signed PoA to the RA.
3. The RA acknowledges the good reception and completeness of the form.
4. The RA provides a copy/update of the list of contact persons and trusted couriers to the domain owner.

2.2.2. *Step 2: Certificate request creation*

> ***Remark****: The request and the retrieval of the certificate have to be done on the same computer and the same browser.*

Purpose: To enable organisations to create a request for PKI certificates for APs and prepare the face-to-face registration file.

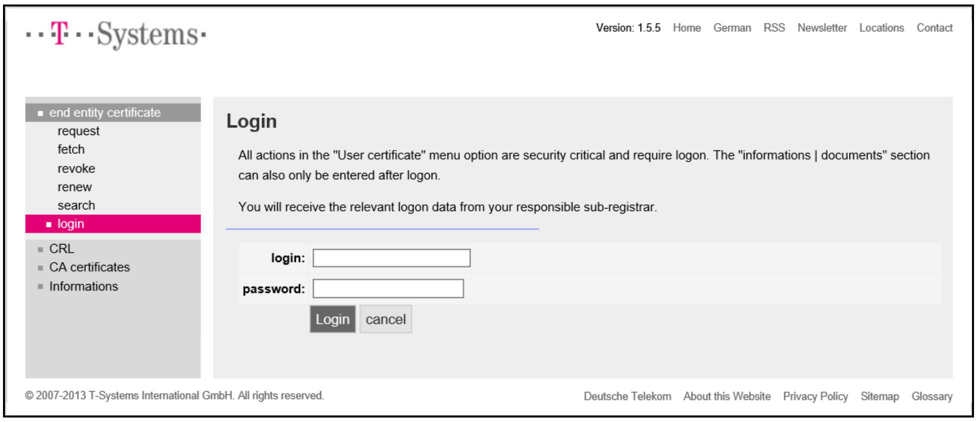
Actors:

- Organisation;
- CEF support team.

Process:

1. An Organisation navigates to the user web interface to request the certificate. The URL is https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en:

[6] See §5.8.


T-Systems
Version: 1.5.5 Home German RSS Newsletter Locations Contact
end entity certificate
request
fetch
revoke
renew
search
login
CRL
CA certificates
Informations
Login
cancel
© 2007-2013 T-Systems International GmbH. All rights reserved.
Deutsche Telekom About this Website Privacy Policy Sitemap Glossary

Login

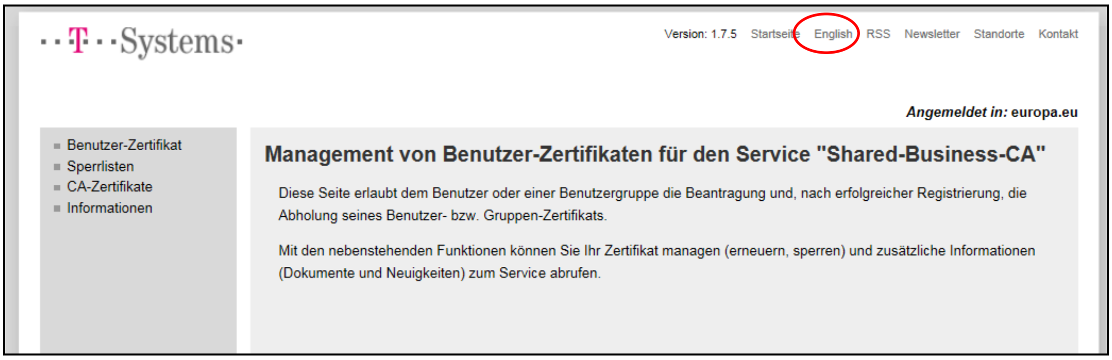
All actions in the "User certificate" menu option are security critical and require logon. The "informations | documents" section can also only be entered after logon.

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

login:

password:

The username is "**sbca/CEF_eDelivery.europa.eu**" and the password is "**digit.333**"
In case that the language changes to German, click on English to change the page's language.


T-Systems
Version: 1.7.5 Startseite English RSS Newsletter Standorte Kontakt
Benutzer-Zertifikat
Sperrlisten
CA-Zertifikate
Informationen

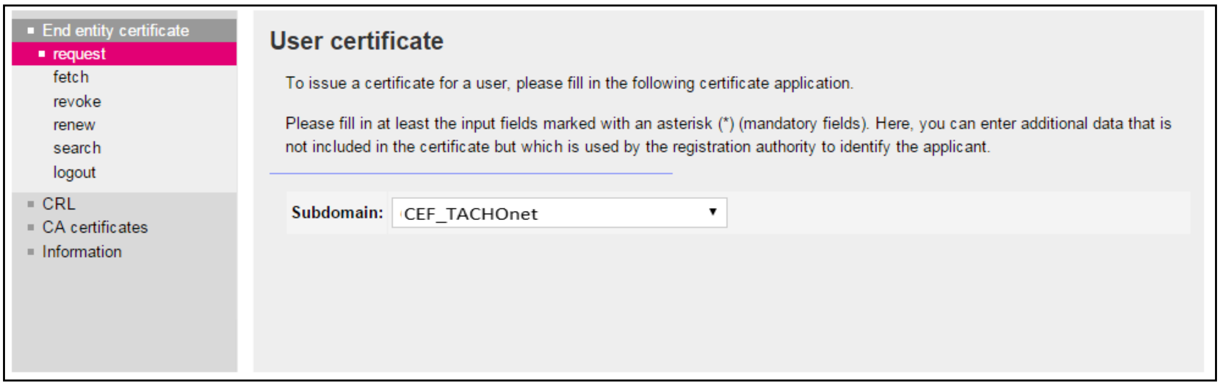
Angemeldet in: europa.eu

Management von Benutzer-Zertifikaten für den Service "Shared-Business-CA"

Diese Seite erlaubt dem Benutzer oder einer Benutzergruppe die Beantragung und, nach erfolgreicher Registrierung, die Abholung seines Benutzer- bzw. Gruppen-Zertifikats.

Mit den nebenstehenden Funktionen können Sie Ihr Zertifikat managen (erneuern, sperren) und zusätzliche Informationen (Dokumente und Neuigkeiten) zum Service abrufen.

2. The Organisation clicks on "request" on the left side of the panel and selects "CEF_TACHOnet” in the dropdown list;



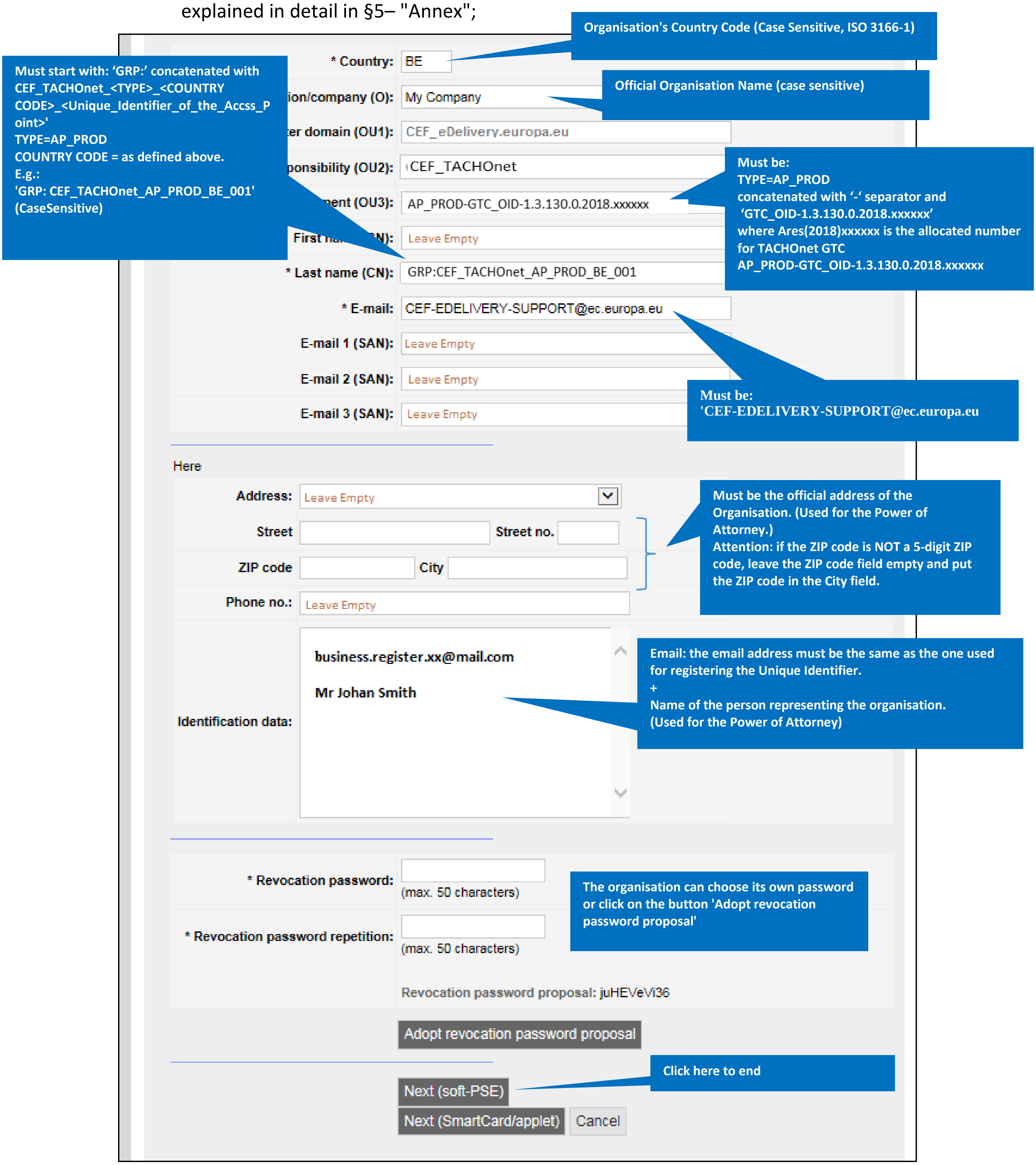
User certificate

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

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

Subdomain: CEF_TACHOnet

3. The Organisation populates the certificate request form as illustrated below and as explained in detail in §5– "Annex";



* Country: BE

ion/company (O): My Company

er domain (OU1): CEF_eDelivery.europa.eu

ponsibility (OU2): CEF_TACHOnet

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

First na (GN): Leave Empty

* Last name (CN): GRP:CEF_TACHOnet_AP_PROD_BE_001

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

E-mail 1 (SAN): Leave Empty

E-mail 2 (SAN): Leave Empty

E-mail 3 (SAN): Leave Empty

Here

Address: Leave Empty

Street | Street no.

ZIP code | City

Phone no.: Leave Empty

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

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'
(CaseSensitive)

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 for TACHOnet GTC
AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx

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'

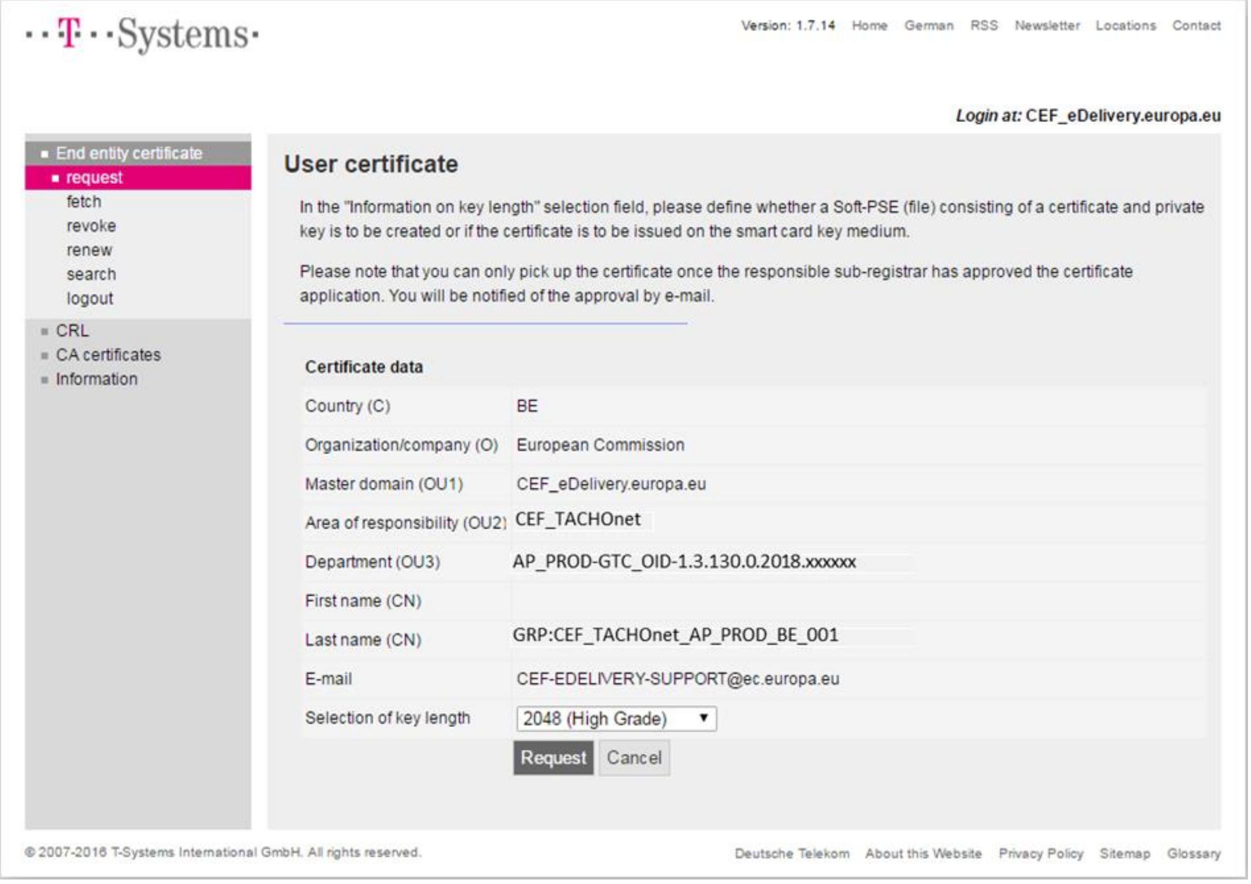
Click here to end

The Organisation must click on 'Next (soft-PSE)'

The complete details of each requested field is shown in the following table:

Requested Fields	Description
Country	**C=Country Code**, location of certificate owner, verified using a public directory; Constraints: 2 characters, in accordance to ISO 3166-1, alpha-2, Case Sensitive; Examples: DE, BE, NL, Specific cases: UK (for Great-Britain), EL (for Greece)
Organisation/Company (O)	**O=Organization name of the certificate owner**
Master domain (OU1)	**OU=CEF_eDelivery.europa.eu**
Area of responsibility (OU2)	**OU=CEF_TACHOnet**
Department (OU3)	Mandatory value per "AREA OF RESPONSIBILITY" The content must be checked using a positive list (white list) when the certificate is requested. If the information does not correspond to the list, the request is prevented. Format: **OU=<TYPE>-<GTC_NUMBER>** Where "<TYPE>" is replaced by AP_PROD: Access Point in Production environment. And where <GTC_NUMBER> is **GTC_OID-1.3.130.0.2018.xxxxxx**, where Ares(2018)xxxxxx is the GTC number for the TACHOnet project. e.g.: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First name (CN)	Must be Empty
Last name (CN)	Must start with "GRP:", followed by a common name. Format: **CN=GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** e.g.: GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail	**E=CEF-EDELIVERY-SUPPORT@ec.europa.eu**
E-mail 1 (SAN)	Must be Empty
E-mail 2 (SAN)	Must be Empty
E-mail 3 (SAN)	Must be Empty
Address	Must be Empty
Street	Must be the official address of the Organisation of the Certificate Owner. (Used for the Power of Attorney.)
Street no.	Must be the official address of the Organisation of the Certificate Owner. (Used for the Power of Attorney.)
Zip Code	Must be the official address of the Organisation of the Certificate Owner. (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.
City	Must be the official address of the Organisation of the Certificate Owner. (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.
Phone no	Must be Empty
Identification data	The email address must be the same as the one used for registering the Unique Identifier. + Must be the name of the person representing the organisation. (Used for the Power of Attorney) + **Commercial Register No** (only mandatory for private organisations) **Entered at the Local Court of** (only required for German and Austrian private organisations)
Revocation password	Mandatory field chosen by the requestor
Revocation password repetition	Mandatory field chosen by the requestor repeated

Selection of key length 2048(High Grade) must be chosen.



Login at: CEF_eDelivery.europa.eu

User certificate

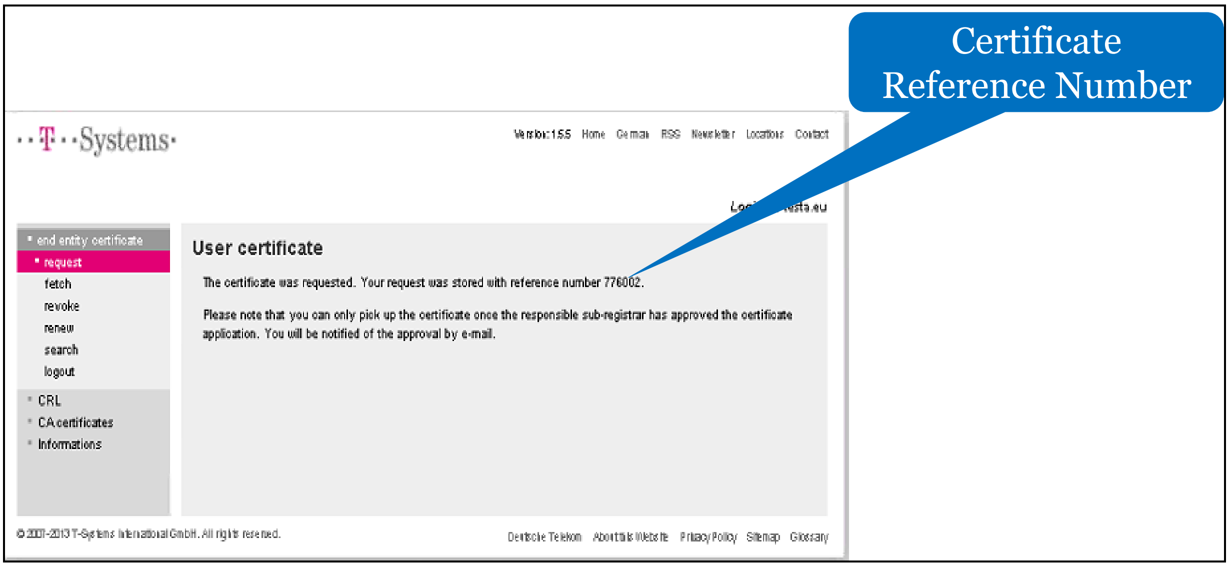
In the "Information on key length" selection field, please define whether a Soft-PSE (file) consisting of a certificate and private key is to be created or if the certificate is to be issued on the smart card key medium.

Please note that you can only pick up the certificate once the responsible sub-registrar has approved the certificate application. You will be notified of the approval by e-mail.

Certificate data

Country (C)	BE
Organization/company (O)	European Commission
Master domain (OU1)	CEF_eDelivery.europa.eu
Area of responsibility (OU2)	CEF_TACHOnet
Department (OU3)	AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First name (CN)	
Last name (CN)	GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail	CEF-EDELIVERY-SUPPORT@ec.europa.eu
Selection of key length	2048 (High Grade) ▾

4. **Important**: the Organisation **needs to record** the reference number to retrieve the certificate;



Certificate Reference Number

User certificate

The certificate was requested. Your request was stored with reference number 776002.

Please note that you can only pick up the certificate once the responsible sub-registrar has approved the certificate application. You will be notified of the approval by e-mail.

5. CEF Support Team, who operates the sub-RA, checks for new requests of certificates and verifies if the information in the certificate request is valid, i.e. that it conforms to the naming convention specified in the §5.1 - Certificate Naming Convention.

6. CEF Support Team verifies that the information entered in the request is in a valid format.
7. When either check from points (5.) or (6.) above fails, CEF Support Team sends an email to the email address provided in the "Identification data" of the request form, with the Domain Owner in cc, in which the Organisation is requested to start the process again. The failed certificate request is cancelled.
8. CEF Support Team sends an email to <lrao-cert-edelivery@tachonet.eu> to inform the Registration Authority Officer (RAO) about the validity of the request. The email shall include:
   - The name of the requestor (organisation), available in the field "Organisation (O)" of the certificate request;
   - The certificate data (see last screenshot figure in point (3) above) including the name of the AP for which the certificate is to be issued, available in the field "Last Name (CN)" of the certificate request;
   - The certificate reference number;
   - The address of the requestor (organisation), its email and the name of the person representing the organisation.
9. End of the process.

The overview of the Certificate Request process is shown in the diagram below.

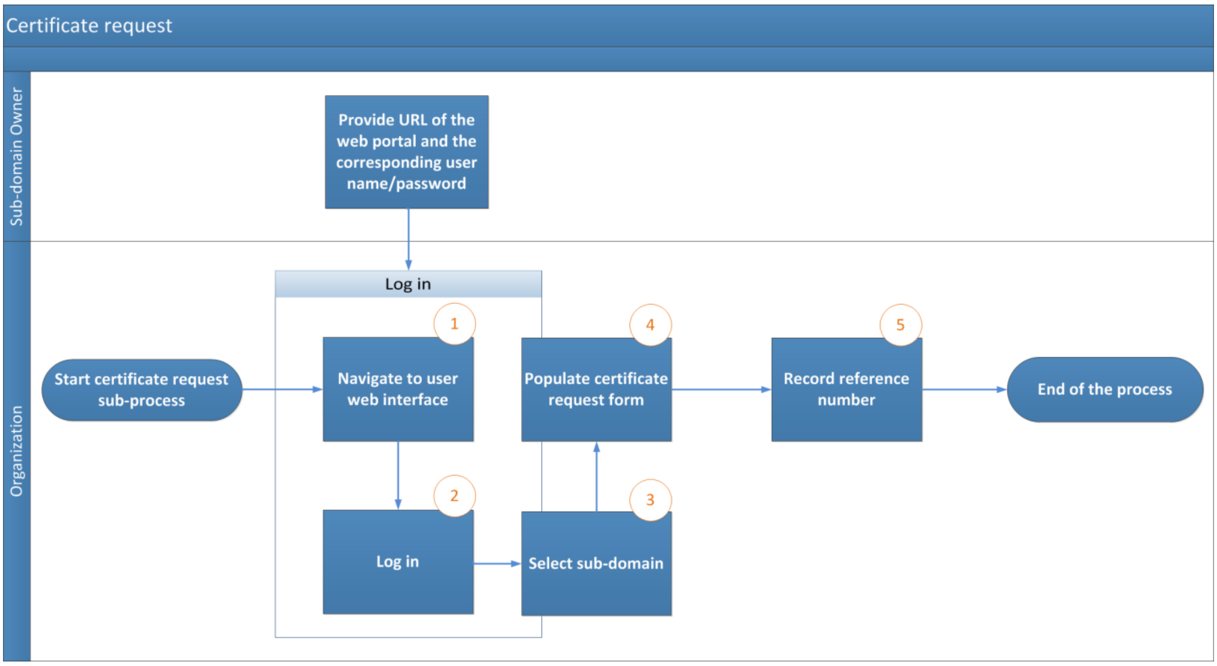

Certificate request
Sub-domain Owner
Organization
Provide URL of the web portal and the corresponding user name/password
Log in
Start certificate request sub-process
1
Navigate to user web interface
2
Log in
3
Select sub-domain
4
Populate certificate request form
5
Record reference number
End of the process

Figure 2 – Certificate request

2.2.3. Step 3: Registration at RAO (Certificate approval)

Purpose: Ensure that the certificate requestor is authorized to get the certificates in a given sub-domain.

Actors:

- CEF Support Team;
- Registration Authority Officers - RAO;
- Organisation (AETR Authority, trusted courier, contact point)

Process:

1. The trusted courier or contact point makes an appointment with the RAO via email exchange identifying the trusted courier who will proceed to the face-to-face (Organisation email: as per trusted courier identification form – step 1; Domain RAO email: <lrao-cert-edelivery@tachonet.eu>).

2. The Organisation prepares the face-to-face documentary package consisting in:

    a. The filled-in and signed power of attorney (see §5.9);

    b. A copy of the valid passport of the trusted courier who will perform the face-to-face. This copy must be signed by one of the step 1 identified Organisation points of contact;

    c. The certificate request paper form (see § 5.10) signed by one of the Organisation points of contact.

3. The RAO receptions the trusted courier after identity screening at the building reception. The RAO conduct the face-to-face registration of the certificate request by:

    a. Identifying and authenticating the trusted courier:

        i. Verifying the trusted courier physical appearance against the passport presented by the trusted courier;

        ii. Verifying the validity of the passport presented by the trusted courier;

        iii. Verifying the validated passport presented by the trusted courier against the copy of the valid passport of the trusted courier signed by one of the step 1 identified Organisation points of contact. Signature is authenticated against the original “trusted courier and contact points identification form”;

    b. Verifying the filled-in and signed power of attorney;

    c. Verifying certificate request paper form and its signature against the original “trusted courier and contact points identification form”;

   d. Calling the signatory contact point to double check the identity of the trusted courier and the content of the certificate request.

4. The RAO confirms to the CEF Support Team that the certificate requestor is indeed authorized to operate the components for which it is asking the certificates and that the corresponding face-to-face registration process was successful. The confirmation must be sent using a "CommiSign" certificate secure email with as attachments a scanned copy of the authenticated face-to-face documentary package and of the signed RAO process check list (see §5.11).

5. If the RAO confirms the validity of the request, the process continues; If not (5b), the certificate issuance is rejected and the Organisation informed;

6. CEF Support Team approves the certificate request.

7. CEF Support Team notifies the RAO of the approval of the certificate.

8. The RAO notifies the Organisation that the certificate can be retrieved via the user portal. The RAO hands over a copy of the certificate to the trusted courier.

9. End of the process.

The overview of the certificate approval process is shown in the diagram below.

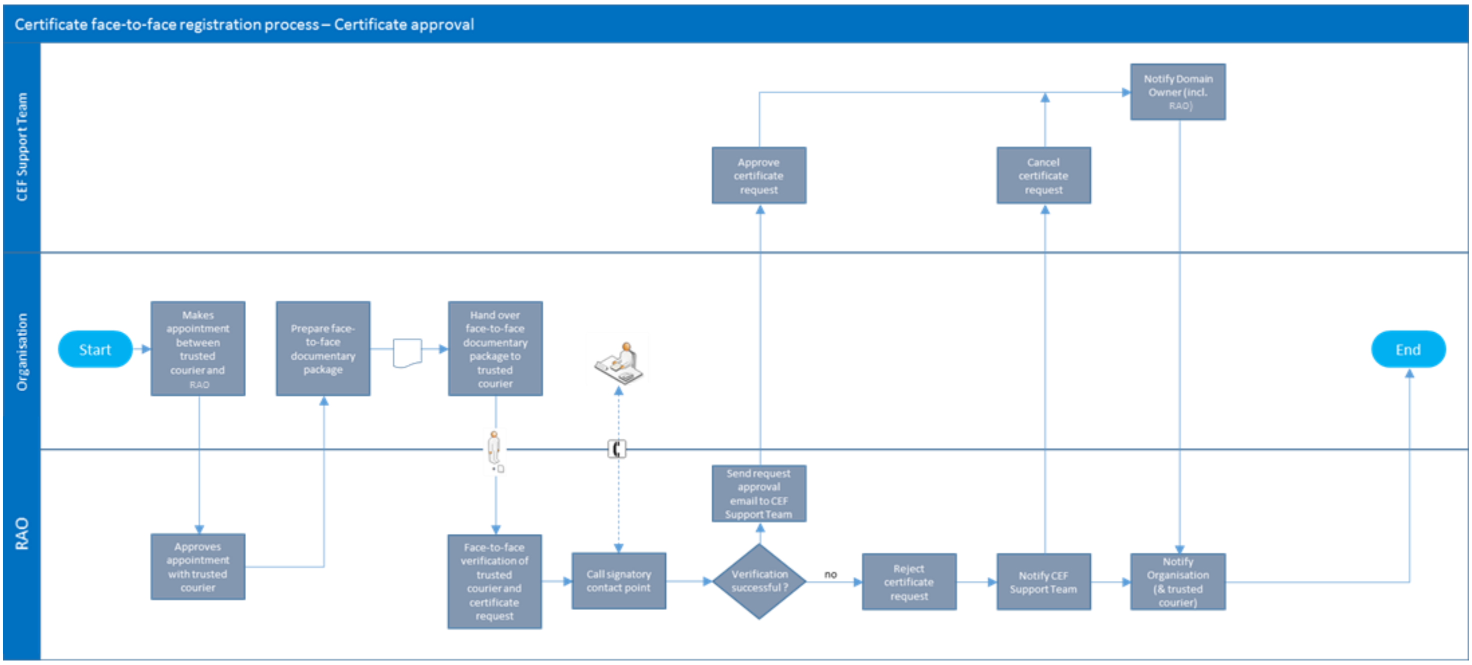

Certificate face-to-face registration process – Certificate approval
CEF Support Team
Organisation
RAO
Start
Makes appointment between trusted courier and RAO
Prepare face-to-face documentary package
Hand over face-to-face documentary package to trusted courier
Approves appointment with trusted courier
Face-to-face verification of trusted courier and certificate request
Call signatory contact point
Verification successful ?
no
Send request approval email to CEF Support Team
Approve certificate request
Reject certificate request
Notify CEF Support Team
Cancel certificate request
Notify Domain Owner (incl. RAO)
Notify Organisation (& trusted courier)
End

Figure 2 - Certificate approval

2.2.4. Step 3: Certificate generation

Purpose: Generation of the requested certificate.

Actors:

- CEF Support Team;

Process:

1. Upon approval of the certificate request, the certificate is generated.

2.2.5. Step 4: Certificate publication & retrieval

Purpose: Distribute and/or download the certificate for AP.

Actors:

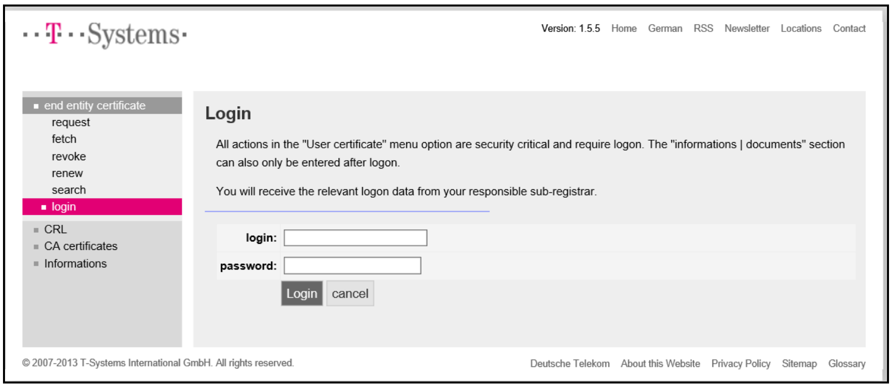
- CEF Support Team;
- Domain Owner;
- RAO;
- Organisation (AETR Authority, trusted courier, contact point)

Process:

1. Following approval of the certificate request, the RAO may retrieve the certificate and hand over a copy to the trusted courier.

2. An Organisation receives the notification from Domain Owner or from the RAO that the certificates can be retrieved;

   a. An Organisation navigates to the user portal and logs in. The URL is https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en:



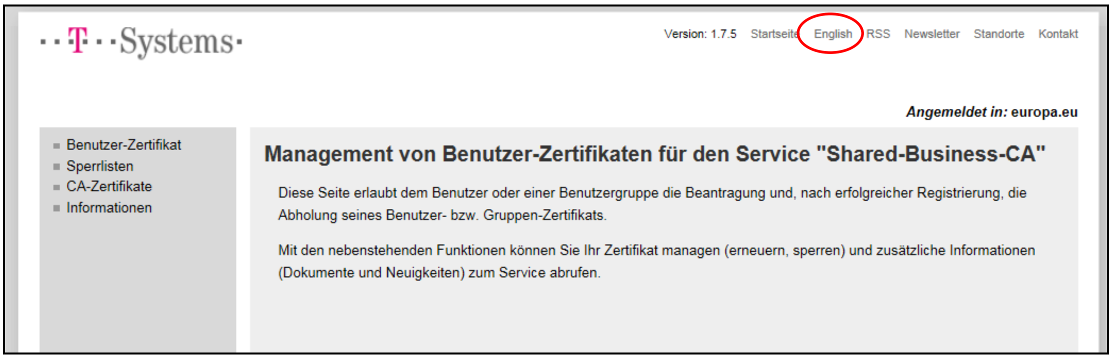
All actions in the "User certificate" menu option are security critical and require logon. The "informations | documents" section can also only be entered after logon.

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

© 2007-2013 T-Systems International GmbH. All rights reserved.

The username is "**sbca/CEF_eDelivery.europa.eu**" and the password is "**digit.333**"

In case that the language changes to German, click on English to change the page's language.



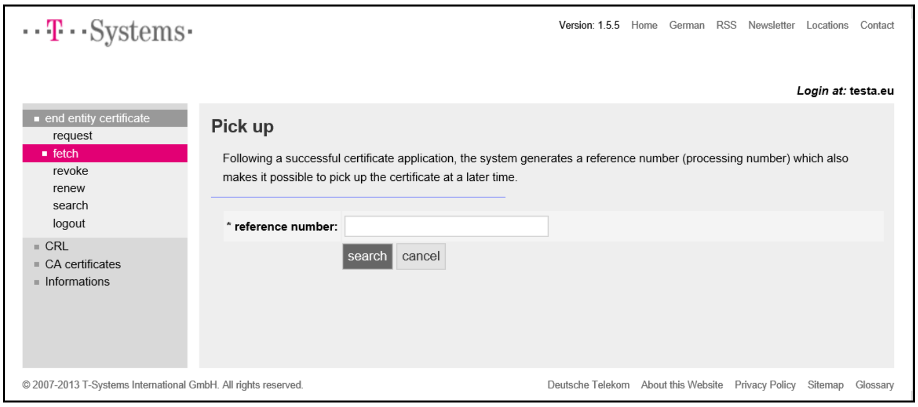
Angemeldet in: europa.eu

Management von Benutzer-Zertifikaten für den Service "Shared-Business-CA"

Diese Seite erlaubt dem Benutzer oder einer Benutzergruppe die Beantragung und, nach erfolgreicher Registrierung, die Abholung seines Benutzer- bzw. Gruppen-Zertifikats.

Mit den nebenstehenden Funktionen können Sie Ihr Zertifikat managen (erneuern, sperren) und zusätzliche Informationen (Dokumente und Neuigkeiten) zum Service abrufen.

b. An Organisation clicks on the "fetch" button on the left-hand side and provides the reference number recorded during the certificate request process;


··T··Systems·
Version: 1.5.5 Home German RSS Newsletter Locations Contact
end entity certificate
request
fetch
revoke
renew
search
logout
CRL
CA certificates
Informations
search
cancel
Deutsche Telekom About this Website Privacy Policy Sitemap Glossary

Login at: testa.eu

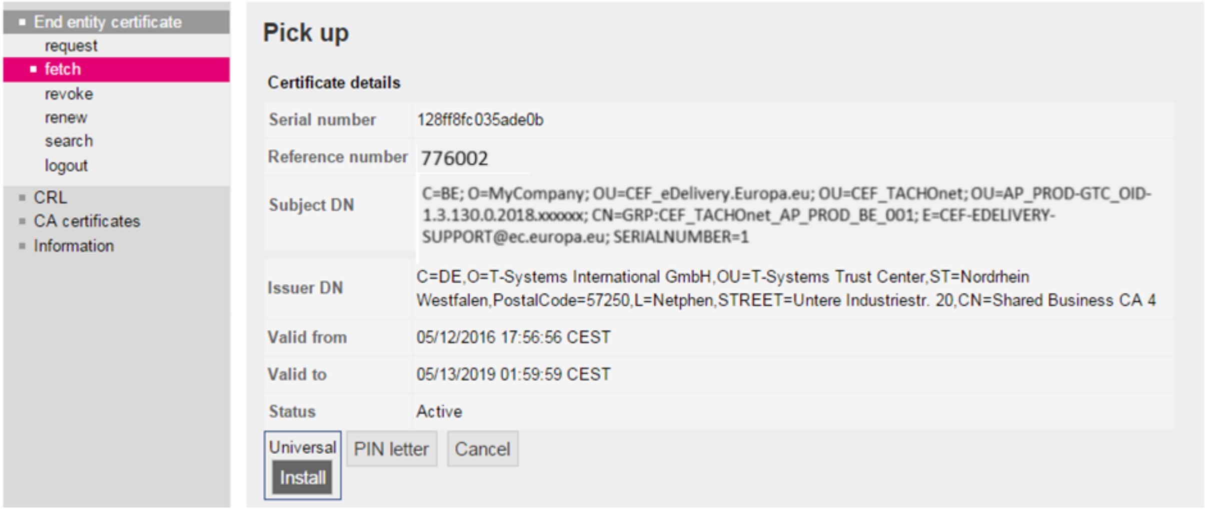
Pick up

Following a successful certificate application, the system generates a reference number (processing number) which also makes it possible to pick up the certificate at a later time.

* reference number:

© 2007-2013 T-Systems International GmbH. All rights reserved.

c. The requestor installs certificates by clicking on the install button;



Pick up

Certificate details

Serial number	128ff8fc035ade0b
Reference number	776002
Subject DN	C=BE; O=MyCompany; OU=CEF_eDelivery.Europa.eu; OU=CEF_TACHOnet; OU=AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx; CN=GRP:CEF_TACHOnet_AP_PROD_BE_001; E=CEF-EDELIVERY-SUPPORT@ec.europa.eu; SERIALNUMBER=1
Issuer DN	C=DE,O=T-Systems International GmbH,OU=T-Systems Trust Center,ST=Nordrhein Westfalen,PostalCode=57250,L=Netphen,STREET=Untere Industriestr. 20,CN=Shared Business CA 4
Valid from	05/12/2016 17:56:56 CEST
Valid to	05/13/2019 01:59:59 CEST
Status	Active

d. End of the process, the certificate is now installed in the repository used by your current browser.

The certificate needs now to be installed on the Access Point. As this is implementation-specific, the Organisation needs to refer to its Access Point provider to obtain the description of this process.

The following steps are needed for the certificate installation on the Access Point:

1. Export the private key and the certificate,
2. Create the keystore and the truststore,
3. Install the keystore and the truststore on the access point.

More information can be found in §5 – "Annex".

The overview of the certificate retrieval process by the Organisation is shown in the diagram below.

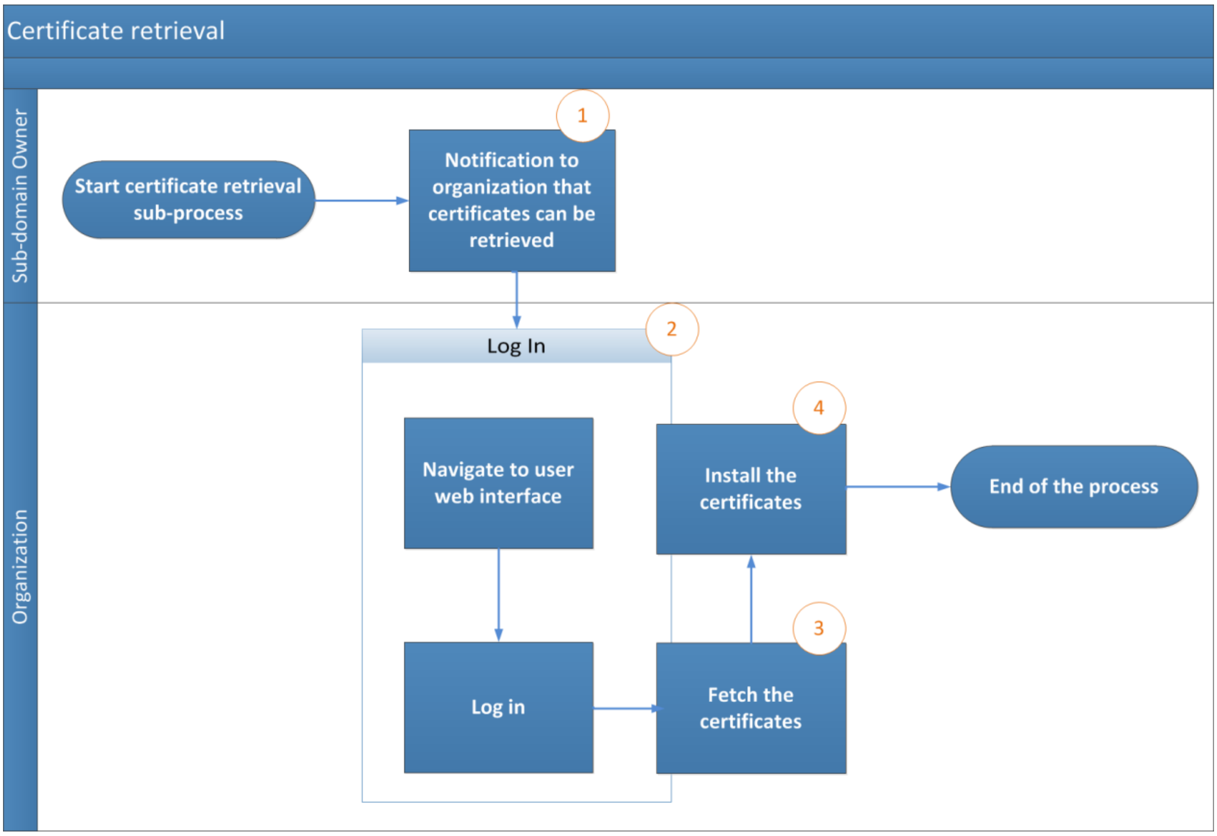

Certificate retrieval
Sub-domain Owner
Organization
Start certificate retrieval sub-process
1
Notification to organization that certificates can be retrieved
2
Log In
Navigate to user web interface
Log in
3
Fetch the certificates
4
Install the certificates
End of the process

Figure 3 - Certificate retrieval

3. CERTIFICATE REVOCATION PROCESS

Purpose: Revoke a certificate for the AP.

Actors:

- Organization;
- CEF eDelivery Sub-domain Owner;
- RAO;
- CEF Support Team.

Process:

1. An Organization, a CEF eDelivery sub-domain owner (including an RAO of that or on behalf of that CEF eDelivery sub-domain owner), submits a revocation request through the user web portal;
2. The sub-RA operated by the CEF Support Team executes the certificate revocation.

The overview of the revocation of a service provider process is shown in the diagram below.

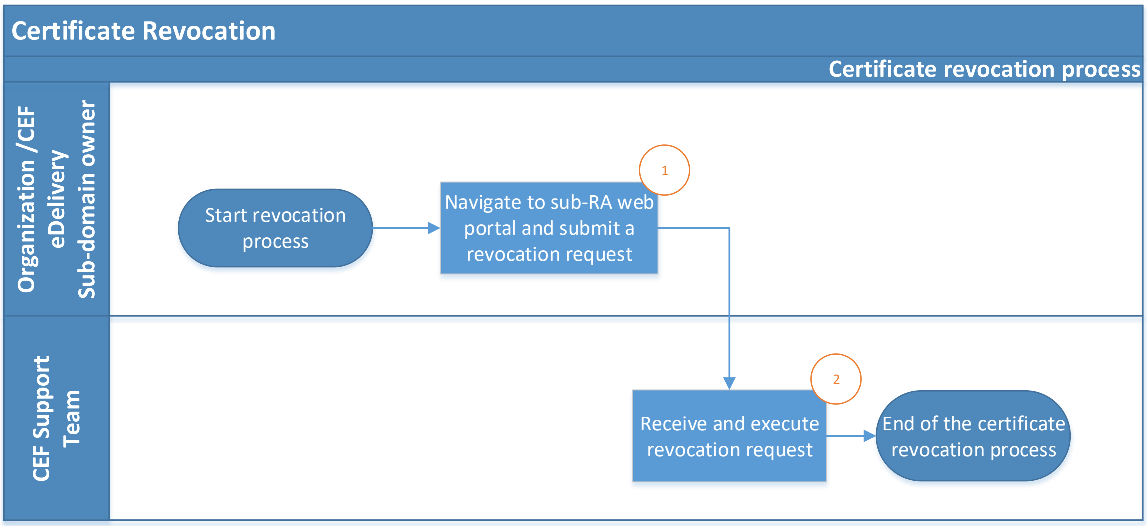

Certificate Revocation
Certificate revocation process
Organization /CEF eDelivery Sub-domain owner
CEF Support Team
Start revocation process
Navigate to sub-RA web portal and submit a revocation request
1
Receive and execute revocation request
2
End of the certificate revocation process

Figure 4 - Certificate revocation

4. GLOSSARY

The key terms used in this Component Offering Description are defined in the CEF Definitions section on the CEF Digital Single Web Portal:

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

The key acronyms used in this Component Offering Description are defined in the CEF Glossary on the CEF Digital Single Web Portal:

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

5. Annexes

5.1. Certificate Naming Convention

This annex contains the information that supports proper understanding and execution of the processes described in §2 – "CERTIFICATE REQUEST PROCESS".

In order to achieve separation per area of responsibility, the CEF eDelivery PKI service uses the naming convention in the certificate metadata.

In particular, the naming assignment listed below must be used when requesting **end-entity user certificates**. Permitted characters for the fields are **a-z A-Z 0-9, ' ( ) + , . / : = ? -**.

1. **Country Code (C)**
   - *Description*: originating country of the service provider.
   - *Constraints: 2 characters, in accordance to ISO 3166-1, alpha-2, Case Sensitive;*
   - *Examples: DE, BE, NL.*
2. **Name of the Organisation (O)**
   - *Description: contains the name of the Organisation authorized to operate APs;*
   - *It is a legal entity approved by the corresponding eDelivery sub-owner;*
   - *Constraints: must be the* ***name of the service provider (the requestor – see §2.1 Roles and Responsibilities) organisation as it appears in official registers*** *(Case sensitive).*
   - *Example: Corp_A.*
3. **Master Domain/client (OU1)**
   - *Description: name of the master domain.*
   - *Constraints: has a fixed value*: **"CEF_eDelivery.europa.eu"**
4. **Area of Responsibility (OU2)**
   - *Description: the business sub-domain in which CEF eDelivery is used.*
   - *Constraints: has a fixed value*: **"CEF_TACHOnet"**.
5. **Department (OU3)**
   - *Description: identifier of the access point and the environment (test, production, acceptance);*
     1. *Format: OU=<TYPE>-<GTC_NUMBER>*
        ➔ where "<TYPE>" is replaced by AP_PROD, access point in production => AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
        ➔ where <GTC_NUMBER> is: "GTC_OID-1.3.130.0.2018.xxxxxx", where Ares(2018)xxxxxx is the number of the GTC signed by TACHOnet.
6. **First Name:** must be left empty;
7. **Last Name (CN):**
   - *Description:* a unique identifier of the subject to which the certificate is issued*;*

- *Constraints:*
    1. Maximum 64 characters;
    2. Must be "GRP:" concatenated with a common name with the following format: <CEF_TACHOnet>_<TYPE>_<COUNTRY CODE>_<UNIQUE ID>
       where <**TYPE>** is AP_PROD, Access Point in production and UNIQUE ID is a unique identifier.
       Examples: GRP: CEF_TACHOnet_AP_PROD_BE_001
    3. Case Sensitive.

8. **Email Address:** Must contain CEF-EDELIVERY-SUPPORT@ec.europa.eu, case sensitive;
9. **E-mail 1, e-mail 2, e-mail 3:** must be left empty.
10. **Address**: must be left empty.
11. **Street, Street no., ZIP code & City**: 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, put the ZIP code in the City field and leave the ZIP code field empty.
12. **Phone no**.: must be left empty.
13. **Identification data**:
    - **Email address:** the email address must be the same as the one used for registering the Unique Identifier
    - **Name of the person representing the organisation**
    - **Mandatory only for private organisations: Commercial Register No**
    - **Mandatory only for private organisations in Austria or Germany: Entered at the Local Court of**

Please note that the email address needs to be identical to the one used to register the SubmitterID for TACHOnet. The email will be checked and if the same email is not provided, the certificate request will be refused. By relying on the certificate naming convention described above, the certificate validation process is implemented to ensure that only inter-sub-domain certificates are trusted.

5.2. The certificate validation process

The certificate validation is implemented by each CEF eDelivery component and is part of the CEF eDelivery source code.

All the certificates trusted by the CEF eDelivery component AP are listed in its local trust store. The certificate validation process therefore verifies if the certificate is listed in the local trust store of the verifying component and if the certificate itself is valid, e.g. authentic, not revoked and not expired. The process is described in the diagram and the supporting table below.

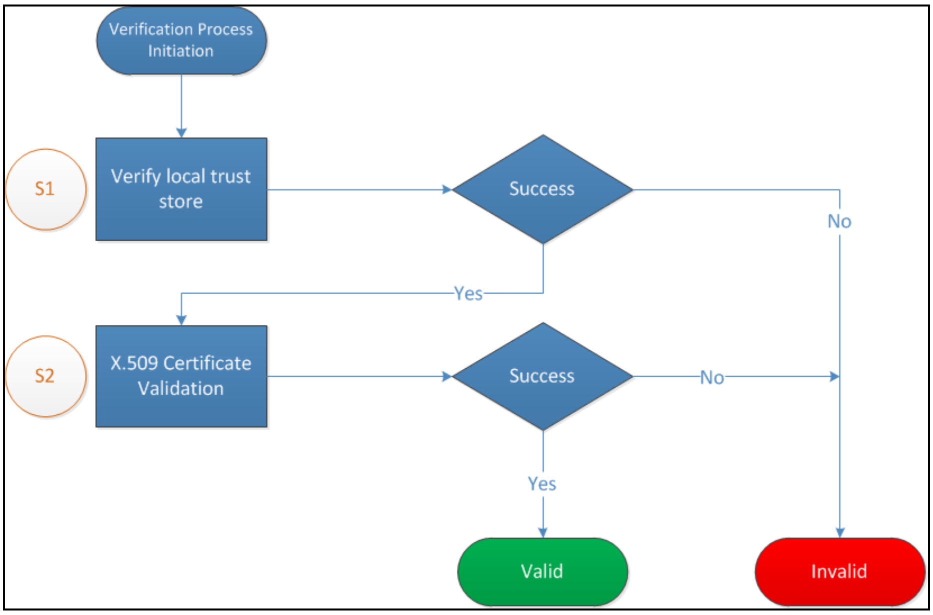


Figure 5 - Certificate validation in the CEF eDelivery PKI

The diagram in Figure 5 is further explained in the table below.

S1: Verify local trust store	The verifying component first checks if the certificate is in its local trust store.
S2: X.509 Certificate Validation	As T-Systems publishes a directory from where the issued certificates can be retrieved, it can be leveraged to keep the trust stores up-to-date. The directory services support LDAP communication protocol. The standard certificate validation in accordance to the ETSI standard[7] that includes the verification of the expiration date, revocation status, and sub-CA signature on the certificate.

Table 1 - Certificate Validation Steps

Remark:

> *As the certificates for all the domains are issued by the same sub-CA, the certificate policy is the same for all the sub-domains. This means that the algorithms and key lengths are fixed. The keys are 2048 bits long and the signature algorithm is SHA256RSA.*

[7] https://www.etsi.org/deliver/etsi_ts/102800_102899/102853/01.01.02_60/ts_102853v010102p.pdf

5.3. Private Key

The export of the private key depends on how your Internet Browser manages the certificates.

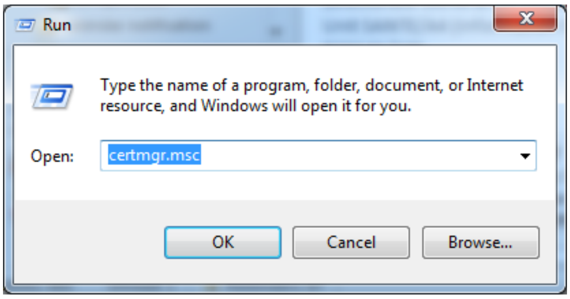
In this annex, we propose 2 procedures:

- On Microsoft Windows (Windows 10 is not yet supported) browser which don't have own certificate repository but uses the Windows one.
- On any OS for Mozilla Firefox users.

5.3.1. Private Key: Export for Windows users

After the installation of the PKI certificate, you can export your private key. Follow the steps below:

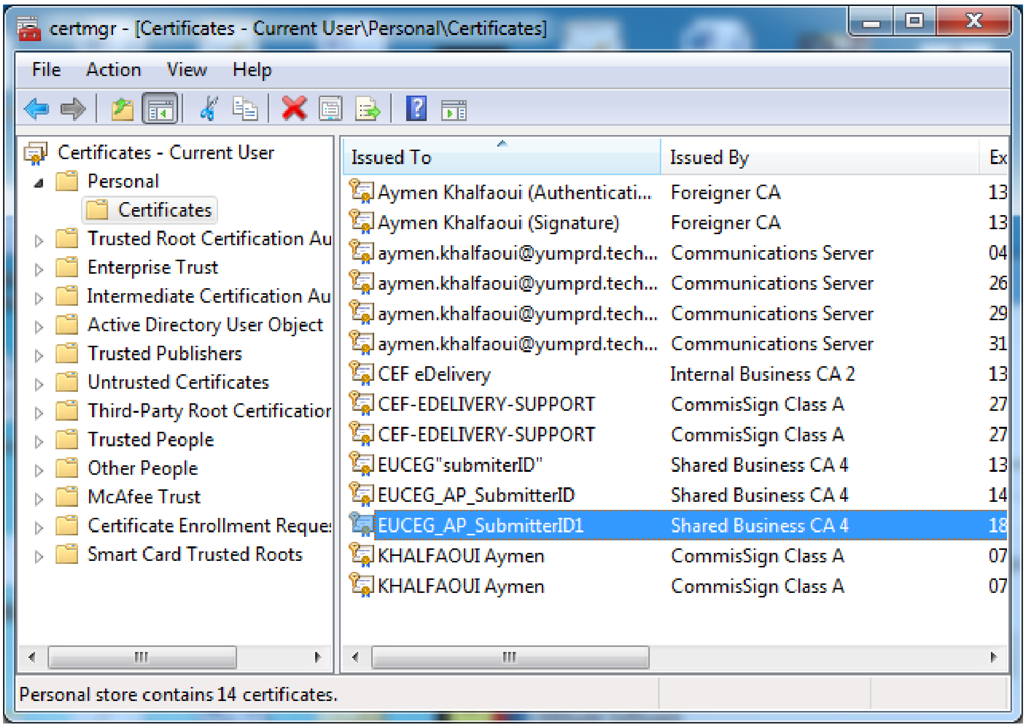
1- Run **certmgr.msc**



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: certmgr.msc

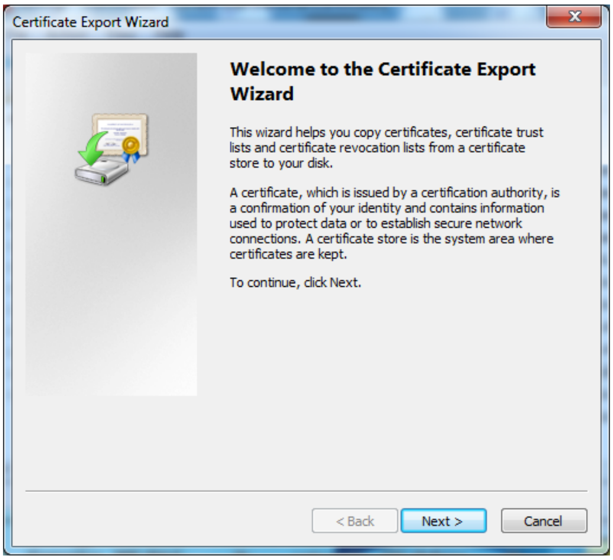
2- Open Personal certificates and choose the one that you want to export (example below):


certmgr - [Certificates - Current User\Personal\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Other People
McAfee Trust
Certificate Enrollment Reque:
Smart Card Trusted Roots

Issued To	Issued By	Ex
Aymen Khalfaoui (Authenticati...	Foreigner CA	13
Aymen Khalfaoui (Signature)	Foreigner CA	13
aymen.khalfaoui@yumprd.tech...	Communications Server	04
aymen.khalfaoui@yumprd.tech...	Communications Server	26
aymen.khalfaoui@yumprd.tech...	Communications Server	29
aymen.khalfaoui@yumprd.tech...	Communications Server	31
CEF eDelivery	Internal Business CA 2	13
CEF-EDELIVERY-SUPPORT	CommisSign Class A	27
CEF-EDELIVERY-SUPPORT	CommisSign Class A	27
EUCEG"submiterID"	Shared Business CA 4	13
EUCEG_AP_SubmitterID	Shared Business CA 4	14
EUCEG_AP_SubmitterID1	Shared Business CA 4	18
KHALFAOUI Aymen	CommisSign Class A	07
KHALFAOUI Aymen	CommisSign Class A	07

Personal store contains 14 certificates.

3- Right click on the "certificate > All tasks > Export"



Certificate Export Wizard

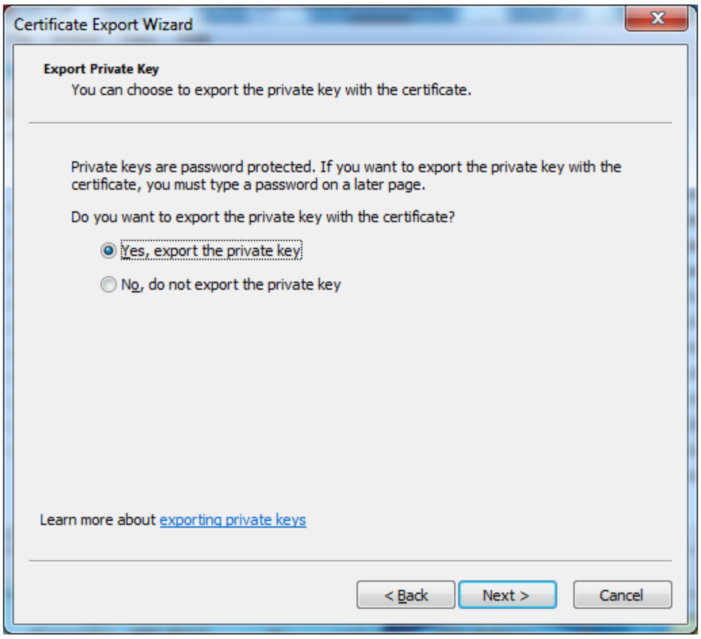
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

4- Select yes, export the private key



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

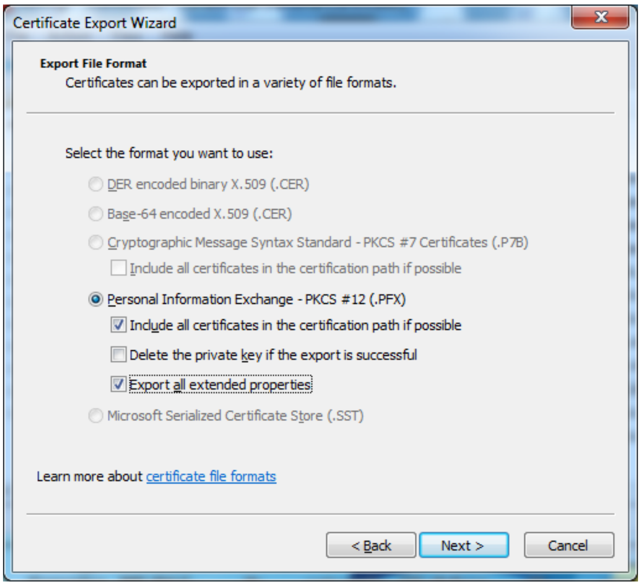
Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

Learn more about exporting private keys

5- Select both **include all certificates…** and **Export all….** As shown below



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

☑ Include all certificates in the certification path if possible

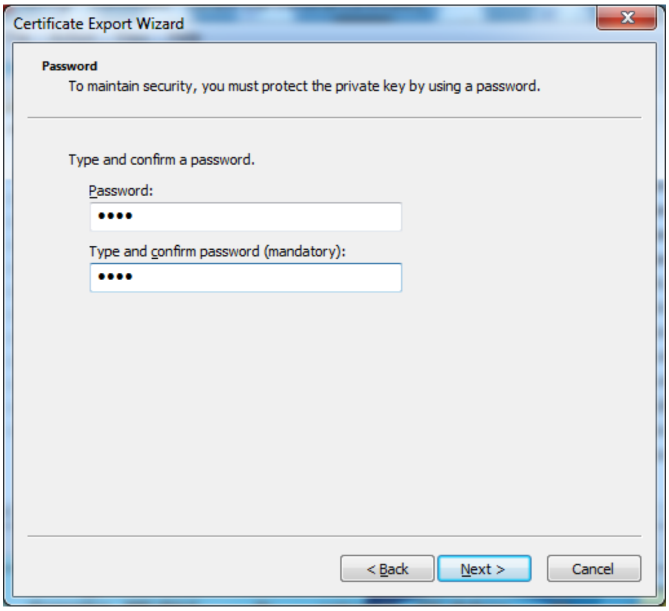
□ Delete the private key if the export is successful

☑ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

6- Set a password



Certificate Export Wizard

Password

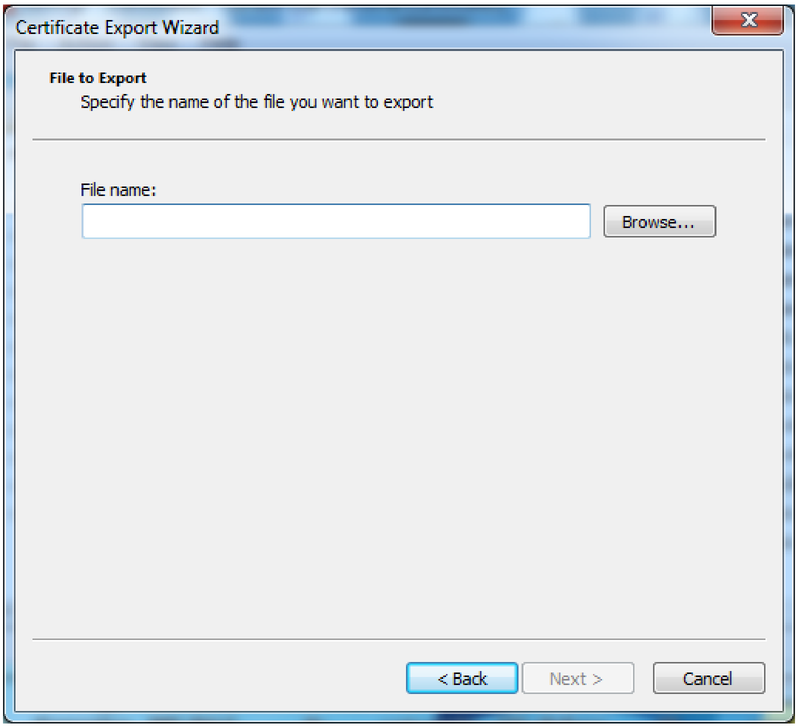
To maintain security, you must protect the private key by using a password.

Type and confirm a password.

Password: ••••

Type and confirm password (mandatory): ••••

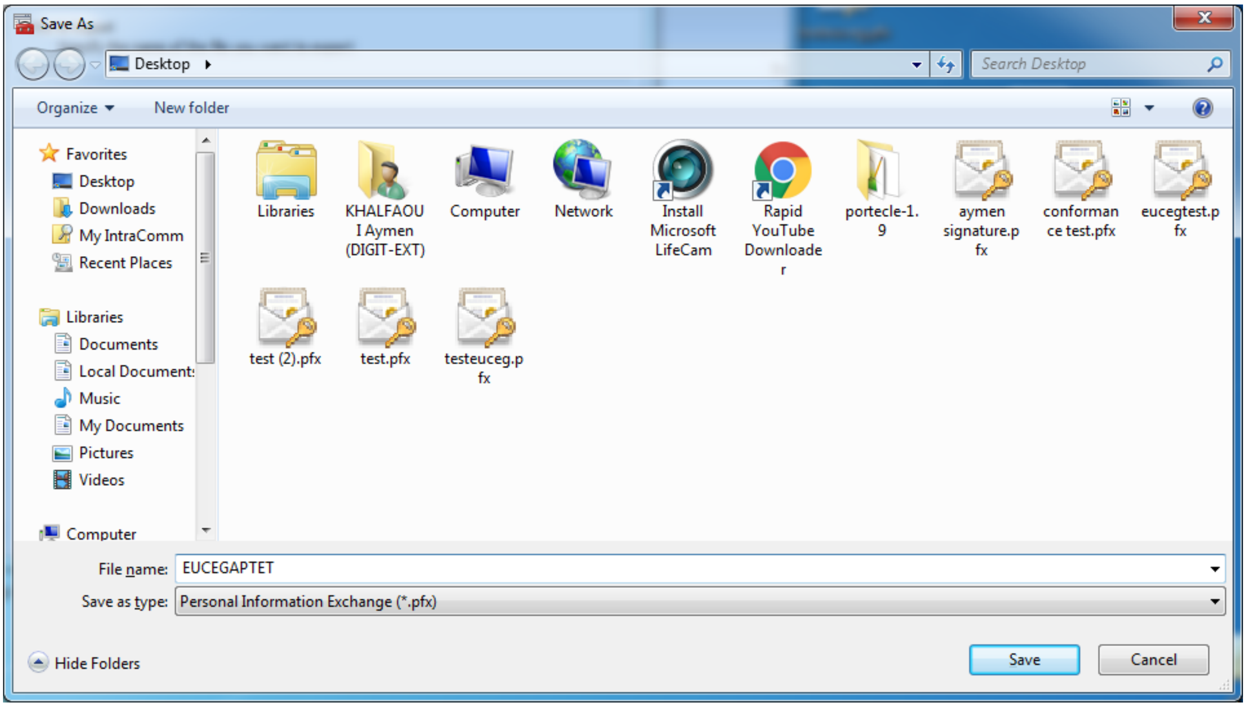
7- Choose where to export it



File to Export
Specify the name of the file you want to export

File name:

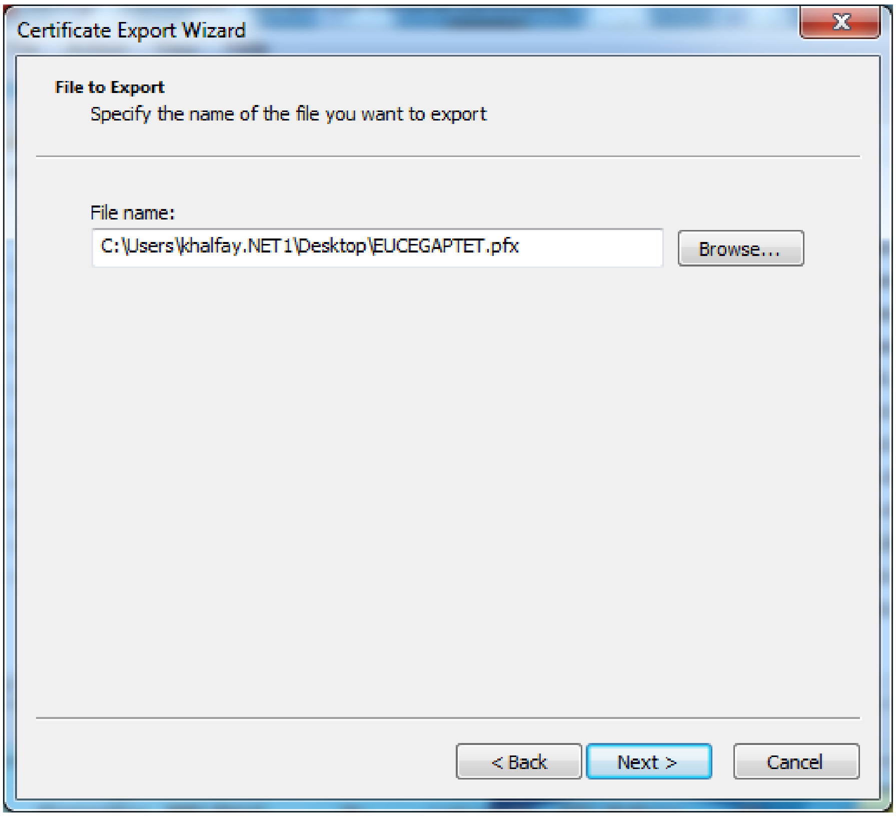
8- Choose a name:



File name: EUCEGAPTET

Save as type: Personal Information Exchange (*.pfx)

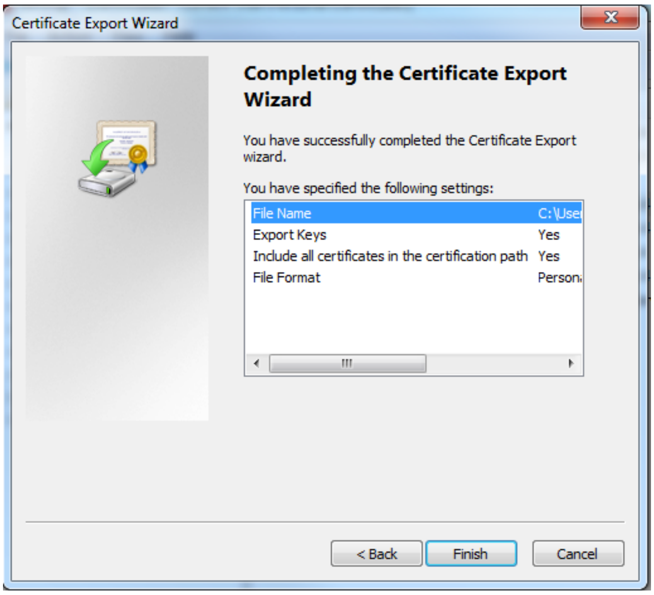
9- Click on **Next**:



File to Export
Specify the name of the file you want to export

File name:
C:\Users\khalfay.NET1\Desktop\EUCEGAPTET.pfx

10- Click on **Finish**:

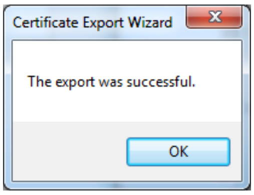


Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Use
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Person

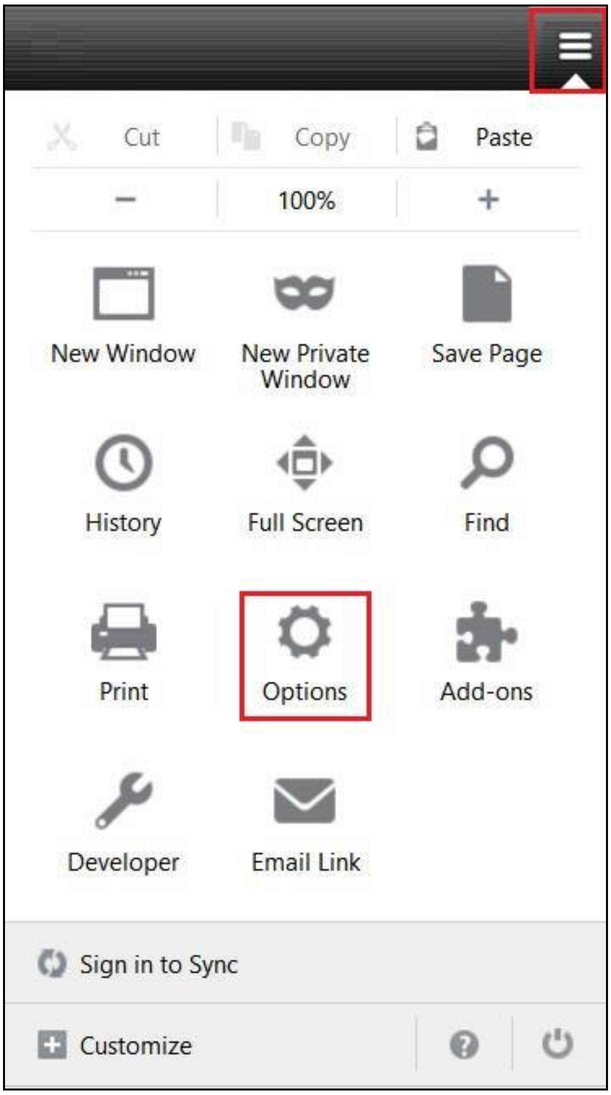


The export was successful.

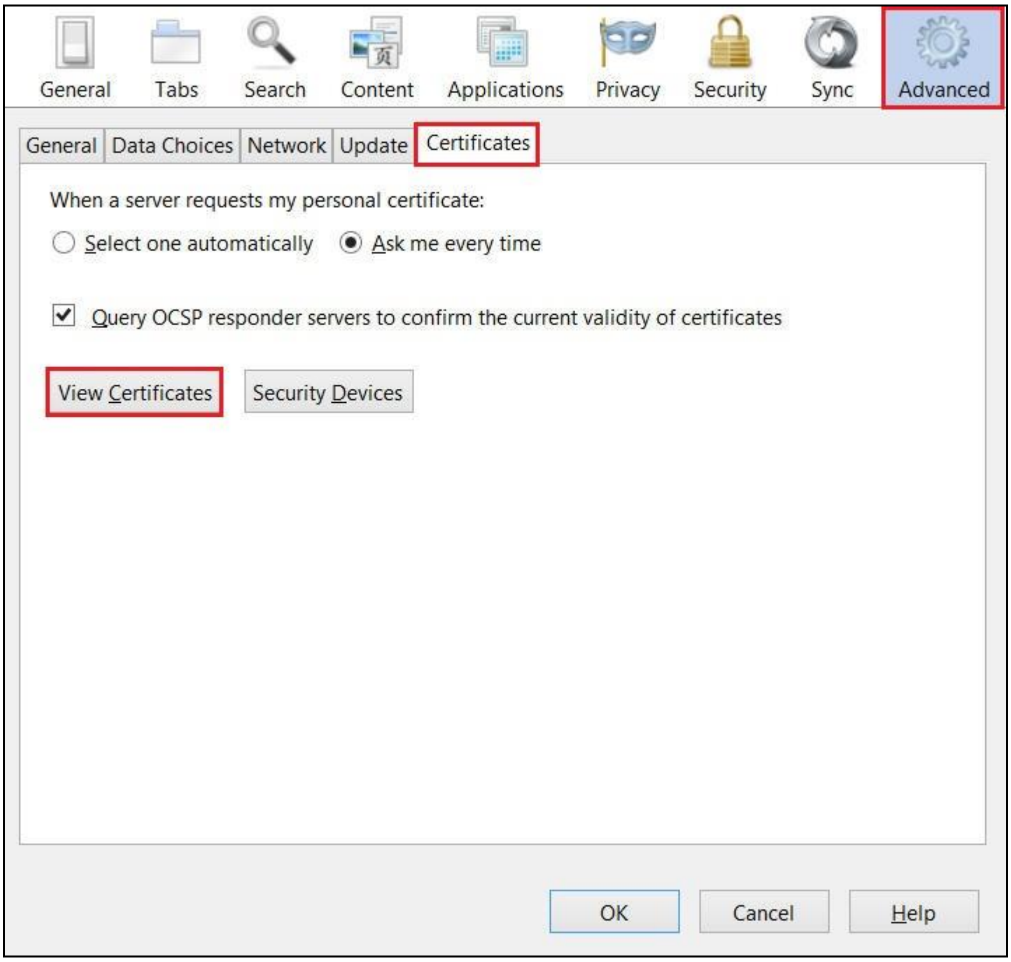
5.3.2. Private Key: Export for Mozilla Firefox users

Mozilla Firefox uses its own Certificate Repository and a specific procedure to extract the private key. These are different steps to execute:

1. In Firefox, go to **Options**.



2. In the **Options** window, click **Advanced**, next, click the **Certificates** tab, and then, click **View Certificates**.

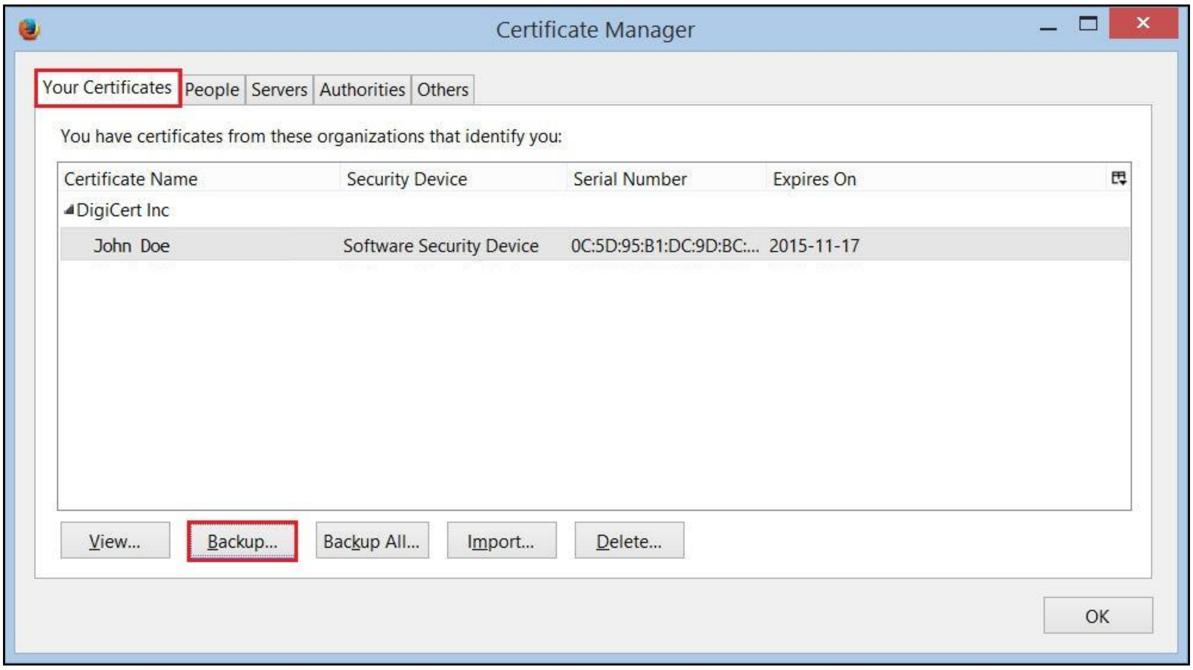


When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

☑ Query OCSP responder servers to confirm the current validity of certificates

3. In the **Certificate Manager** window, on the **Your Certificates** tab, select your code signing certificate which contains your private key you want to export and then, click **Backup**.



You have certificates from these organizations that identify you:

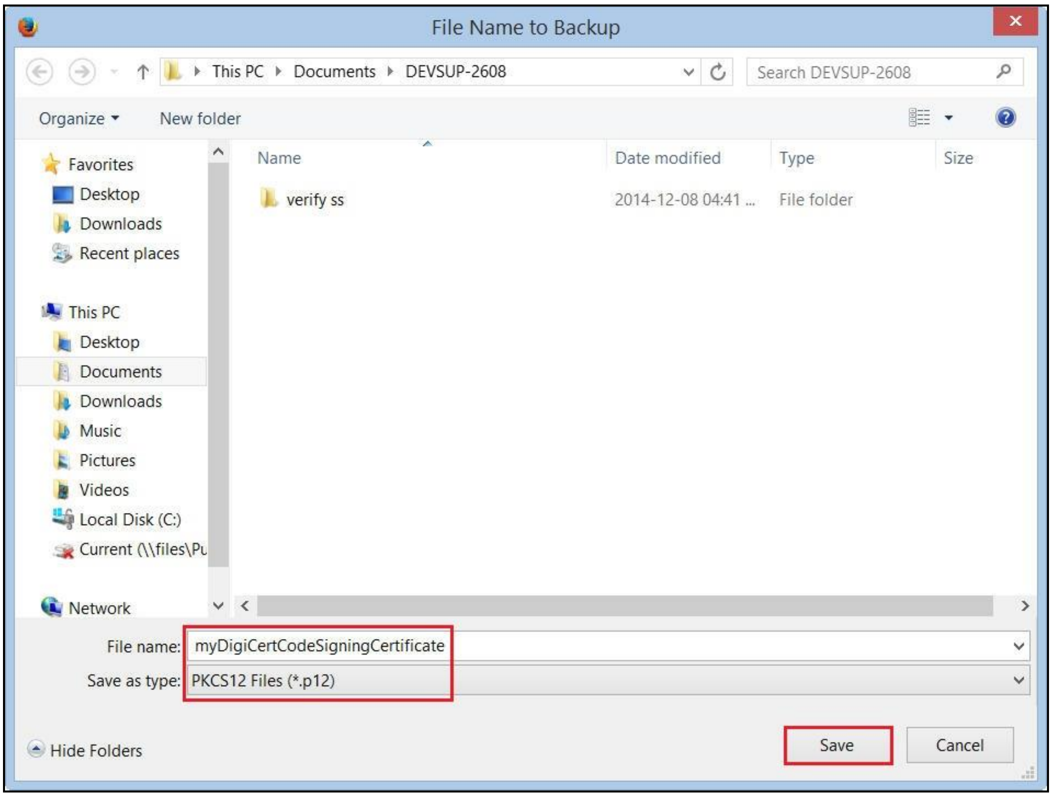
Certificate Name	Security Device	Serial Number	Expires On
◢DigiCert Inc			
John Doe	Software Security Device	0C:5D:95:B1:DC:9D:BC:...	2015-11-17

4. In the **File Name to Backup** window, go to where you want to save your private key (w/private key) .p12 file, provide a file name (i.e.*myCodeSigningCertificate*), and then click **Save**.

Make sure to save the .p12 file in a location that you will remember and to which you have permissions.

Remark:

*A **.p12** file uses the same format as a **.pfx** or a **PKCS12** file.*

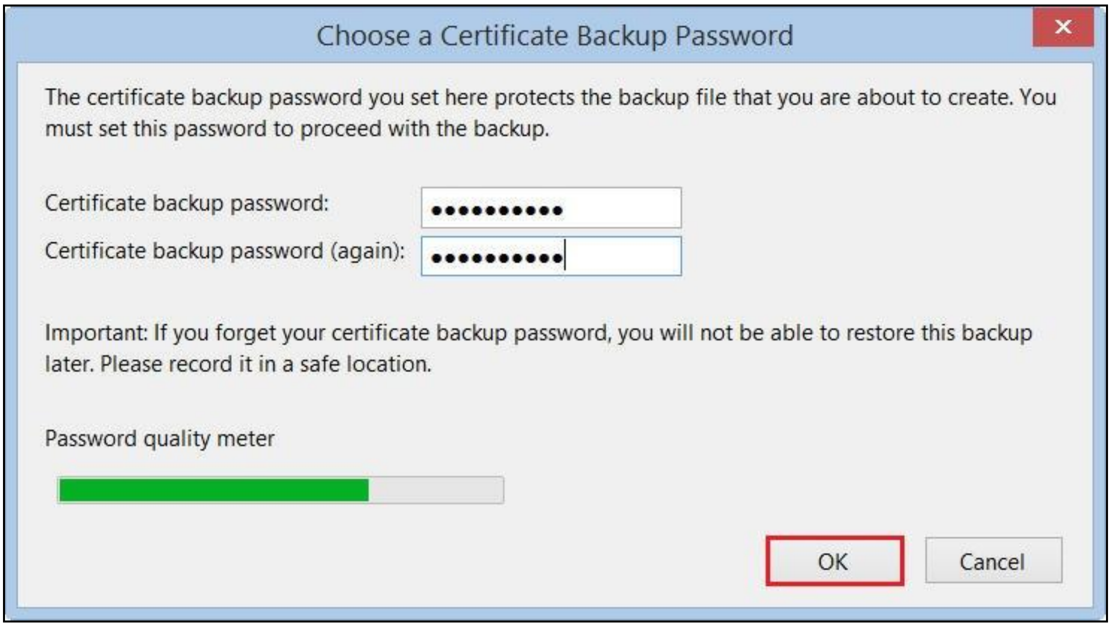


Name	Date modified	Type	Size
verify ss	2014-12-08 04:41 ...	File folder	

File name: myDigiCertCodeSigningCertificate

Save as type: PKCS12 Files (*.p12)

5. In the **Choose a Certificate Backup Password** window, create a **Certificate backup password** and then, click **OK**.



Choose a Certificate Backup Password

The certificate backup password you set here protects the backup file that you are about to create. You must set this password to proceed with the backup.

Certificate backup password: ●●●●●●●●●●●

Certificate backup password (again): ●●●●●●●●●●●

Important: If you forget your certificate backup password, you will not be able to restore this backup later. Please record it in a safe location.

Password quality meter

6. When you receive the *"Successfully backed up your security certificate(s) and private key(s)"* message, click **OK**

5.4. Public Key (certificate)

The export of the public key (certificate) depends on how your Internet Browser manages the certificates.

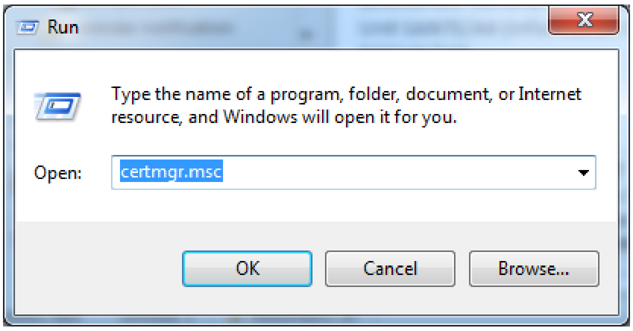
In this annex, we propose 2 procedures:

- On Microsoft Windows (Windows 10 is not yet supported) for any Internet browser which don't have own certificate repository but uses the Windows one;
- On any OS for Mozilla Firefox user.

5.4.1. Public Key (certificate): Export for Windows users

The Trust store contains the Public Keys (certificates) of the other parties (ADRs).

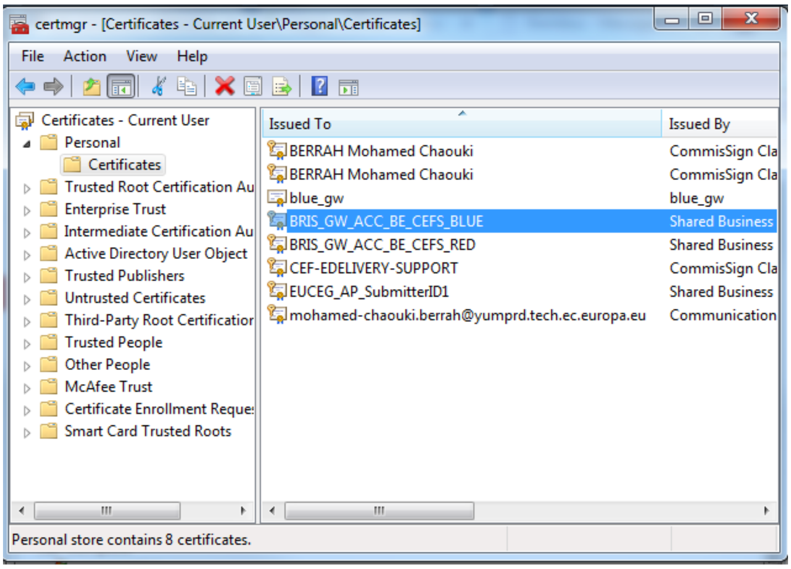
1. Run **certmgr.msc**



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: certmgr.msc

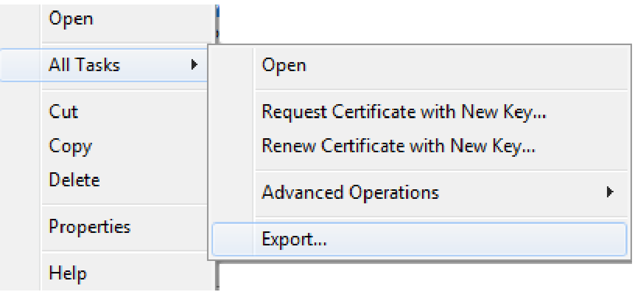
2. Open Personal certificates and choose the one that you want to export (example below):


certmgr - [Certificates - Current User\Personal\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Other People
McAfee Trust
Certificate Enrollment Reque:
Smart Card Trusted Roots

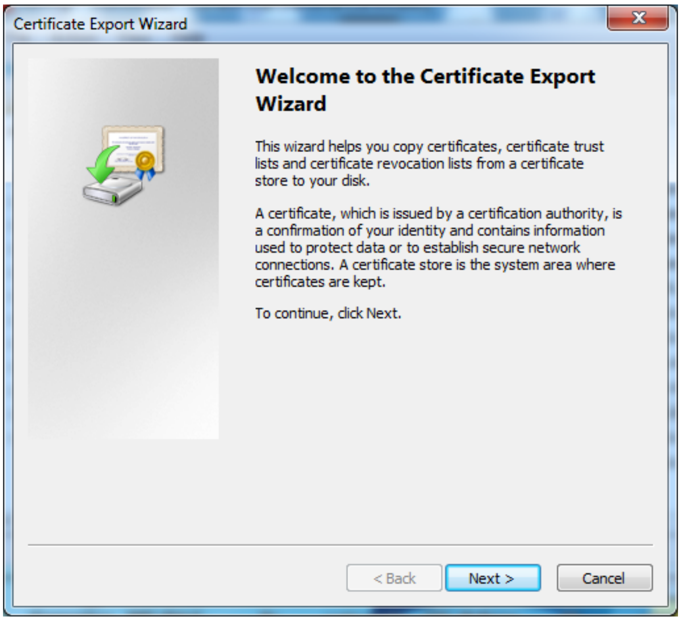
Issued To	Issued By
BERRAH Mohamed Chaouki	CommisSign Cla
BERRAH Mohamed Chaouki	CommisSign Cla
blue_gw	blue_gw
BRIS_GW_ACC_BE_CEFS_BLUE	Shared Business
BRIS_GW_ACC_BE_CEFS_RED	Shared Business
CEF-EDELIVERY-SUPPORT	CommisSign Cla
EUCEG_AP_SubmitterID1	Shared Business
mohamed-chaouki.berrah@yumprd.tech.ec.europa.eu	Communication

Personal store contains 8 certificates.

3. Right click on the "certificate > All tasks > Export"



4. Click on **Next**



Certificate Export Wizard

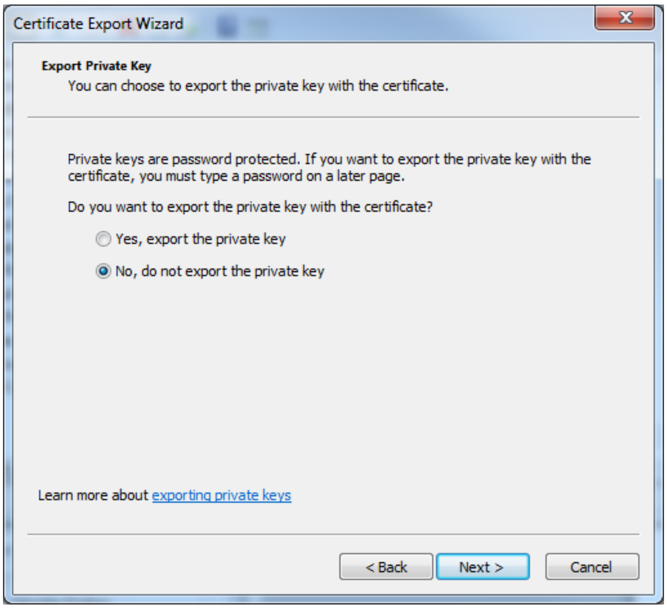
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

5. Select **No, do not export the private key** then click **Next**



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

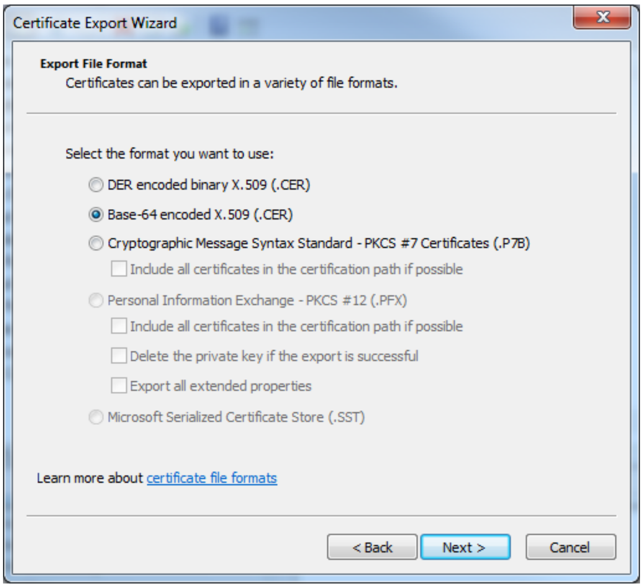
Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

Learn more about exporting private keys

6. Select **Base-64 encoded X.509 (.CER)** then click **Next**



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

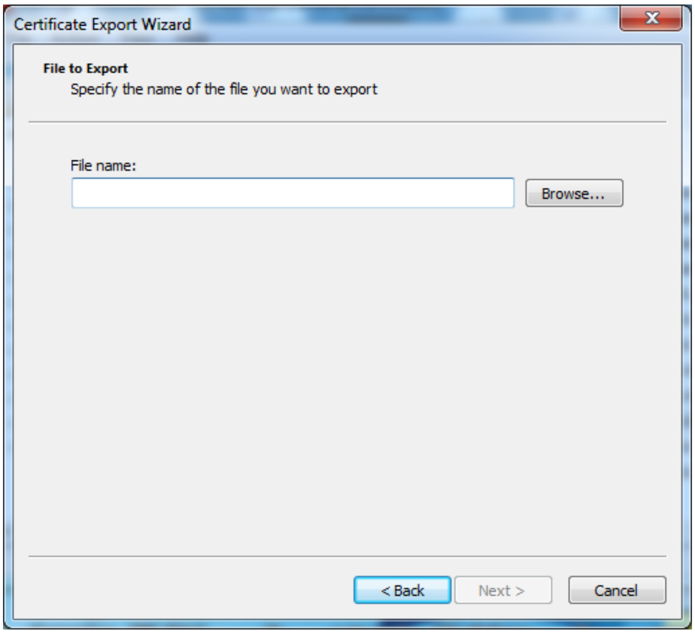
□ Delete the private key if the export is successful

□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

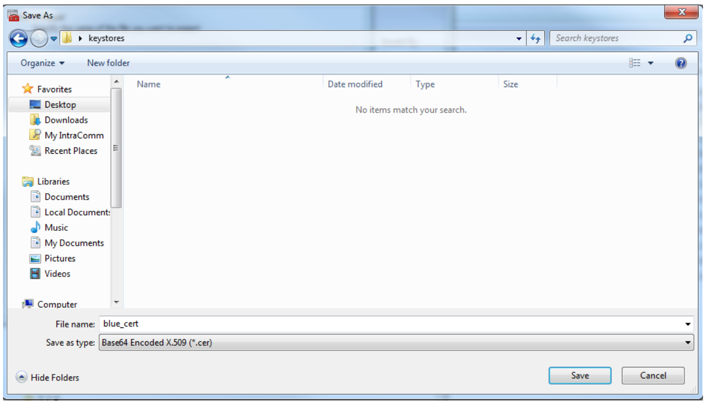
7. Choose where to export it:



Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name:



Save As

keystores

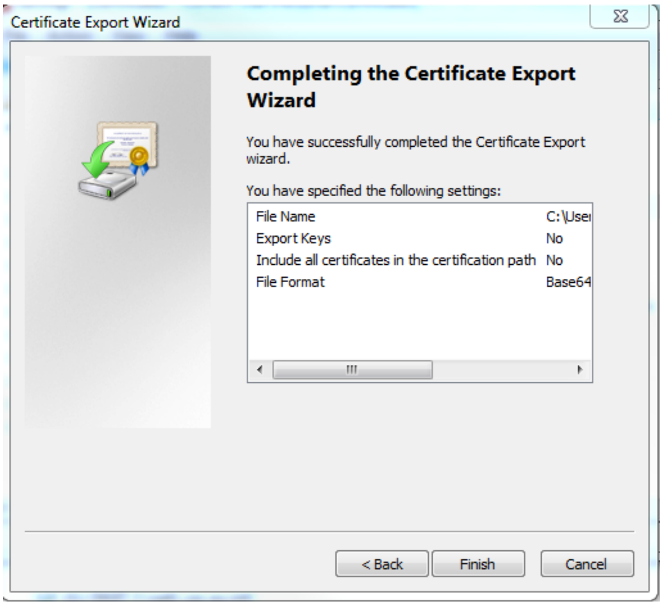
Search keystores

Name	Date modified	Type	Size

No items match your search.

File name: blue_cert

Save as type: Base64 Encoded X.509 (*.cer)



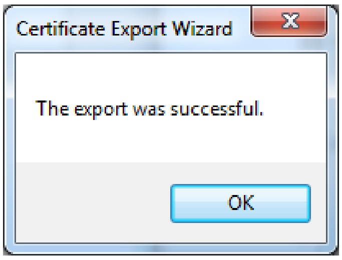
Certificate Export Wizard

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\User
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64



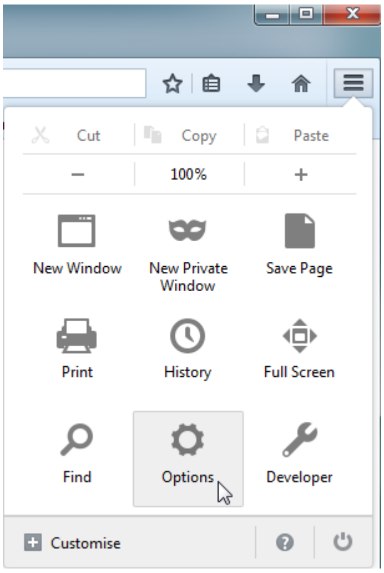
Certificate Export Wizard

The export was successful.

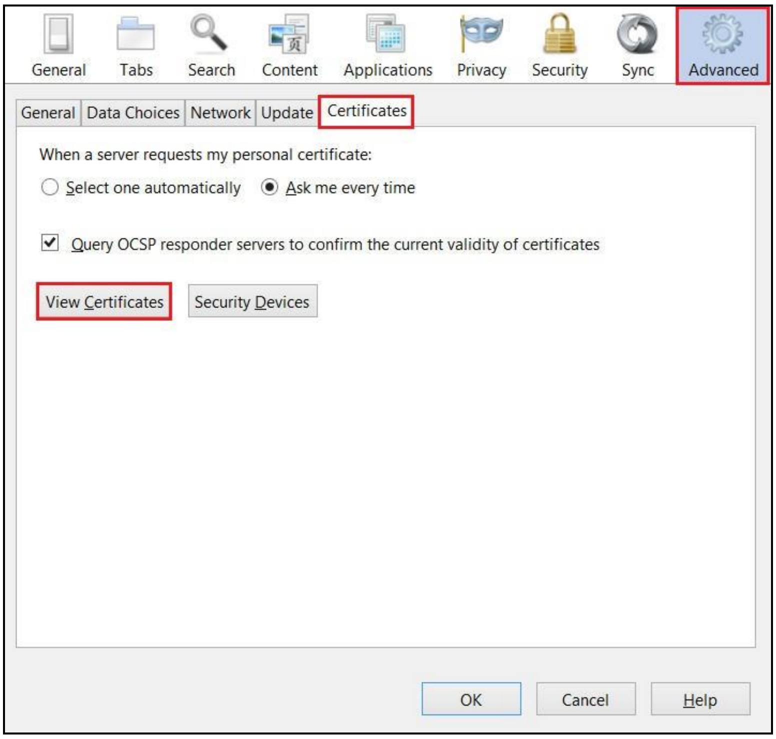
5.4.2. Public Key (certificate): Export for Mozilla Firefox users

Mozilla Firefox uses its own Certificate Repository and a specific procedure to extract the public key (certificate). These are the different steps to execute:

1. In Firefox, go to **Options**.



2. In the **Options** window, click **Advanced**, next, click the **Certificates** tab and then, click **View Certificates**.

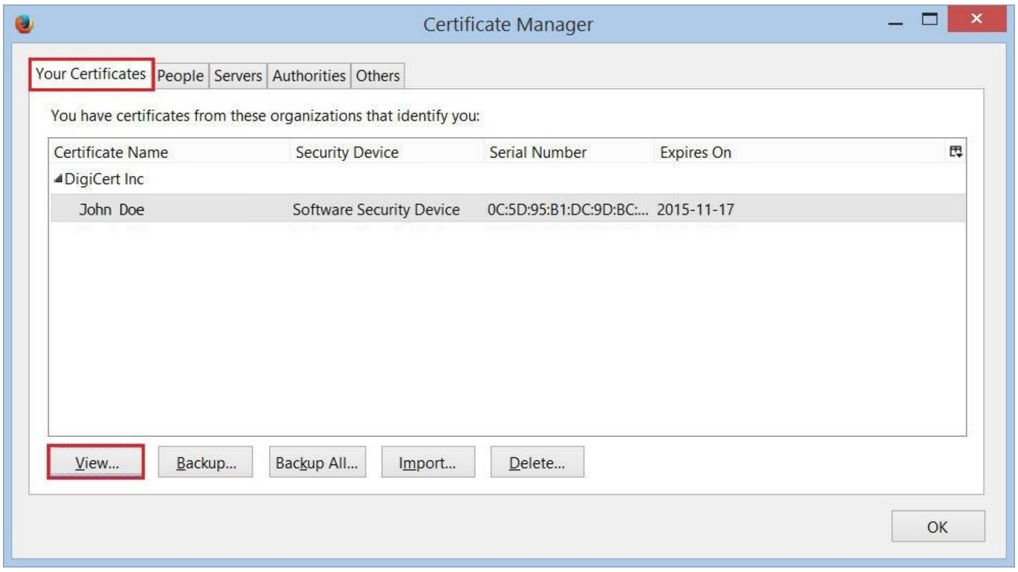


When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

☑ Query OCSP responder servers to confirm the current validity of certificates

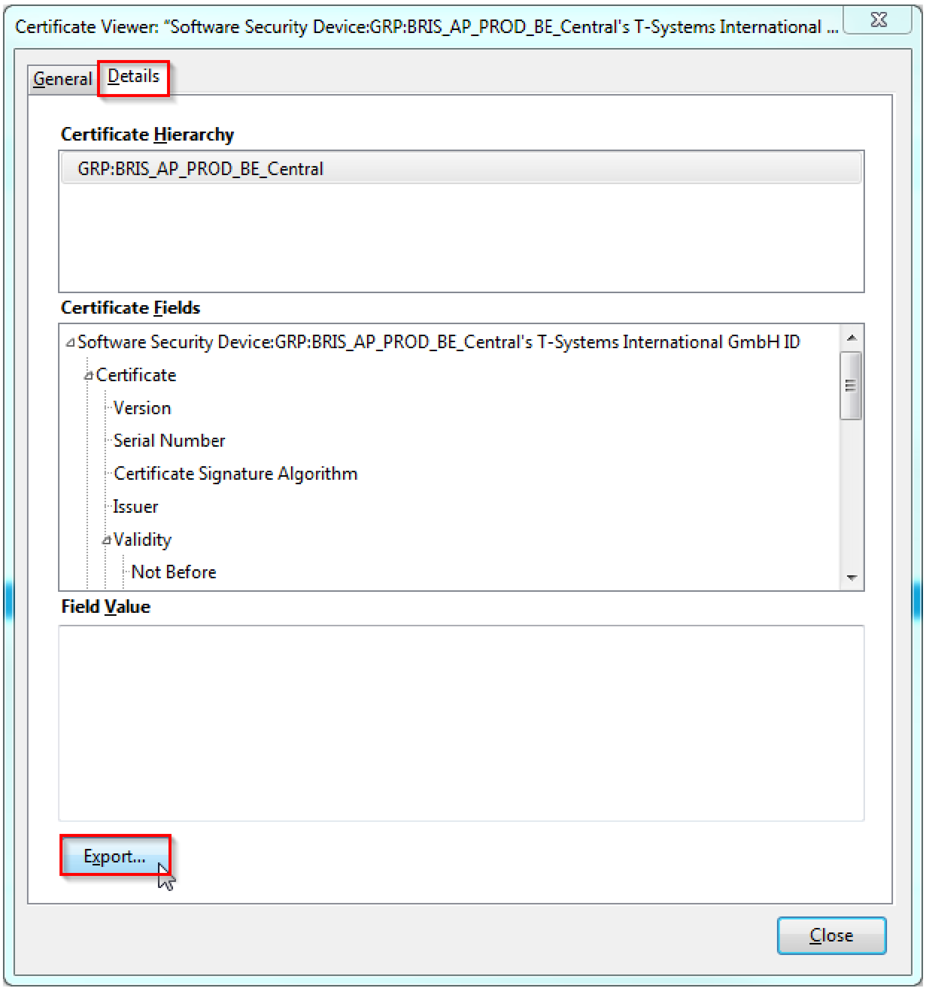
3. In the **Certificate Manager** window, on the **Your Certificates** tab, select your certificate which you want to export and then, click **View**.



You have certificates from these organizations that identify you:

Certificate Name	Security Device	Serial Number	Expires On
◢DigiCert Inc			
John Doe	Software Security Device	0C:5D:95:B1:DC:9D:BC:...	2015-11-17

4. In the **Certificate Viewer** window select the **Details** tab and click on the **Export** button.



Certificate Viewer: "Software Security Device:GRP:BRIS_AP_PROD_BE_Central's T-Systems International ...

Certificate Hierarchy

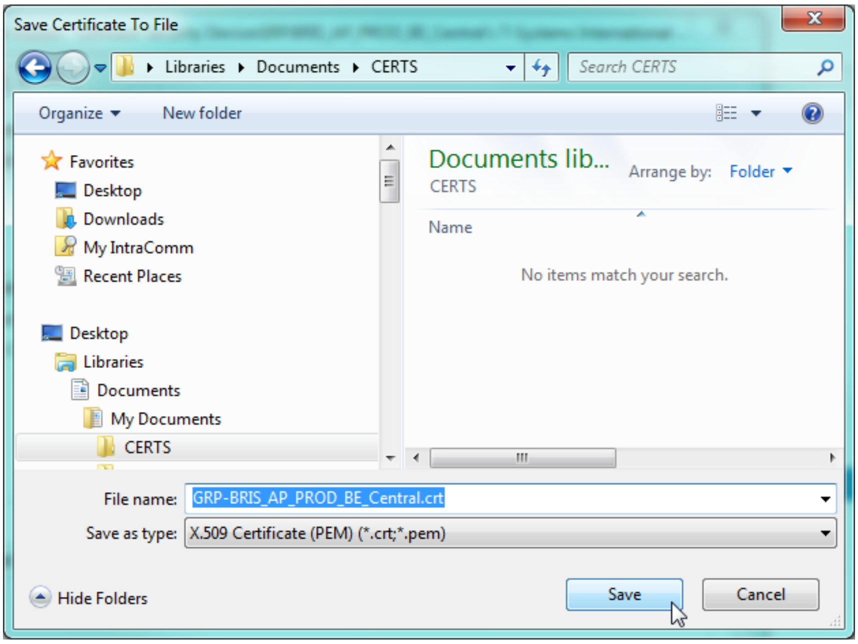
GRP:BRIS_AP_PROD_BE_Central

Certificate Fields

Software Security Device:GRP:BRIS_AP_PROD_BE_Central's T-Systems International GmbH ID
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before

Field Value

5. In the **Save Certificate To File** window, go to where you want to save your public key(certificate) in crt, pem or other format, provide a file name and then click **Save**.



File name: GRP-BRIS_AP_PROD_BE_Central.crt

Save as type: X.509 Certificate (PEM) (*.crt;*.pem)

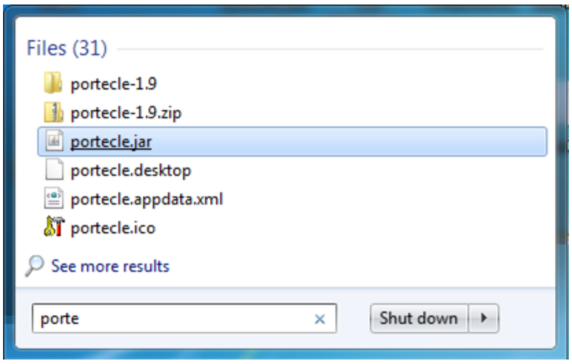
5.5. Keystore Creation

*Now that the Private key has been retrieved, we can either create a **.jks** or a **.p12** keystore file so that it can be used in the configuration of the access points, for example on Domibus (keystore section of Domibus-security.xml).*
The next 2 sections describe the procedure for both options.

5.5.1. OPTION1: JKS Keystore (preferred option)

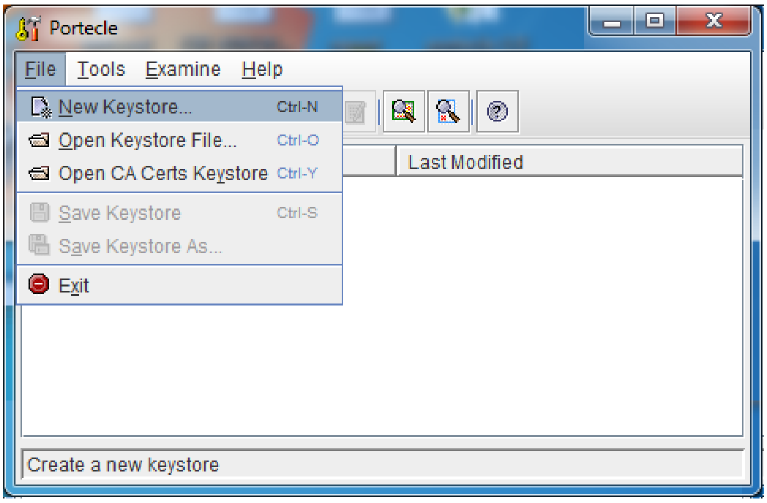
The Keystore JKS file is used to contain the Access Point's own Private and Public Keys also known as the Key Pair.

1. start **portecle.jar** (or any other suitable installed tool)



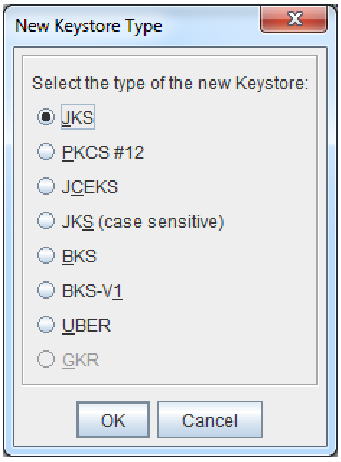
porte

2. Click on **File** then **New Keystore**



Create a new keystore

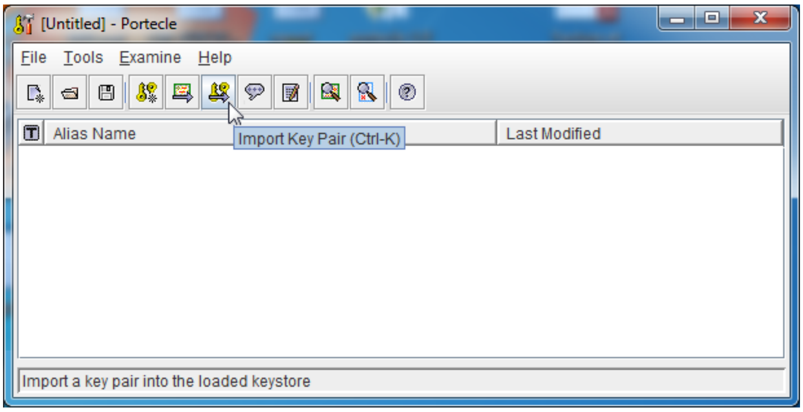
3. Select **JKS** then click on **OK**



Select the type of the new Keystore:

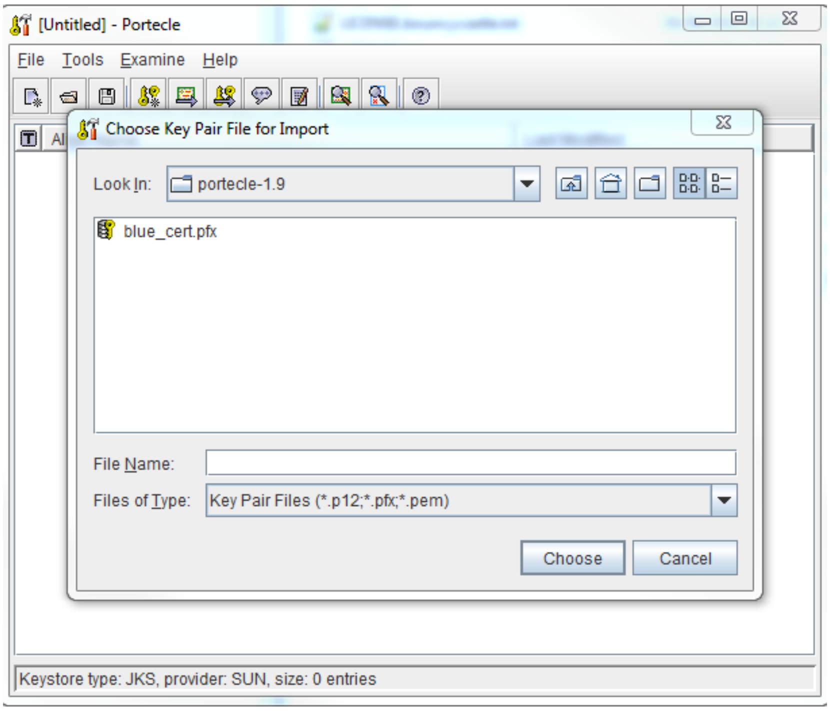
● JKS
○ PKCS #12
○ JCEKS
○ JKS (case sensitive)
○ BKS
○ BKS-V1
○ UBER
○ GKR

4. Click on the **Import Key Pair** icon



Import a key pair into the loaded keystore

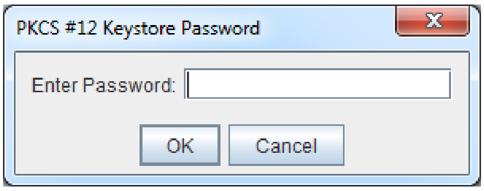
5. Locate your exported private key file (.pfx)



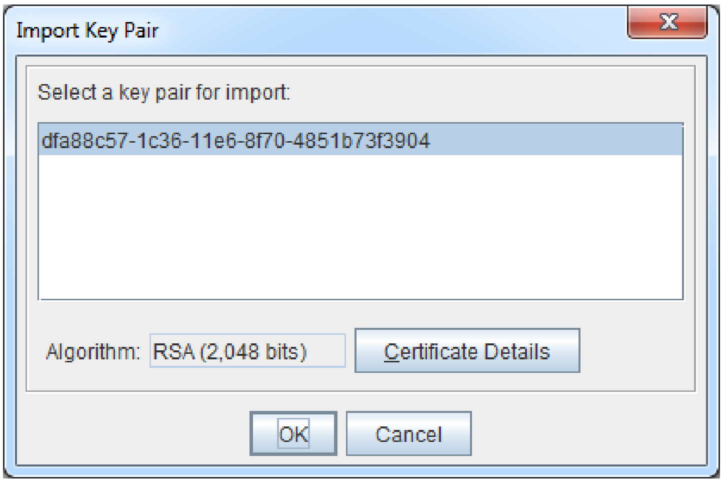
Files of Type: Key Pair Files (*.p12;*.pfx;*.pem)

Keystore type: JKS, provider: SUN, size: 0 entries

6. Enter a Password then click on **OK**



7. Click on **OK**



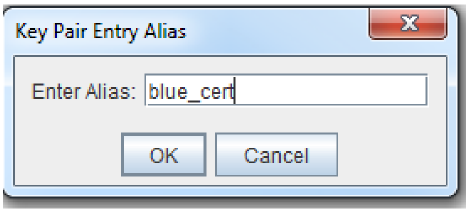
Import Key Pair

Select a key pair for import:

dfa88c57-1c36-11e6-8f70-4851b73f3904

Algorithm: RSA (2,048 bits)

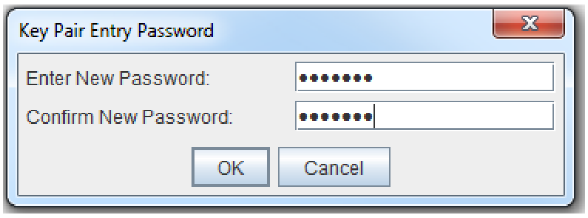
8. Enter an Alias then click on **OK**



Key Pair Entry Alias

Enter Alias: blue_cert

9. Enter Key Pair Password

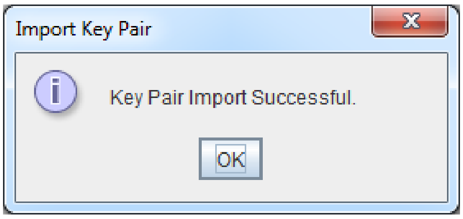


Key Pair Entry Password

Enter New Password: •••••••

Confirm New Password: •••••••

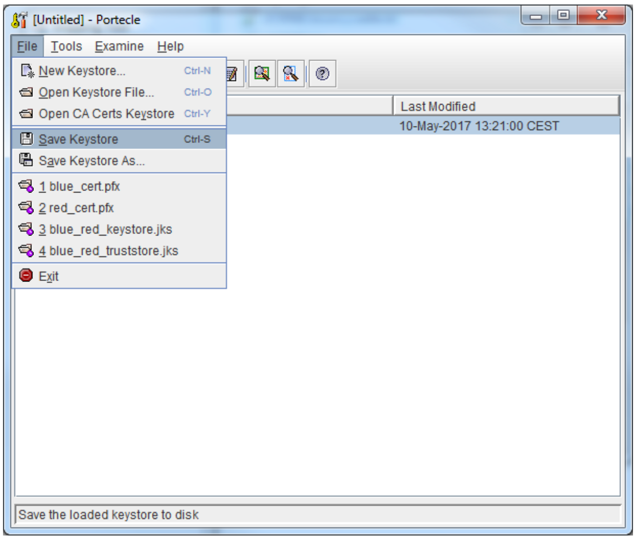
10. Click on **OK**



Import Key Pair

Key Pair Import Successful.

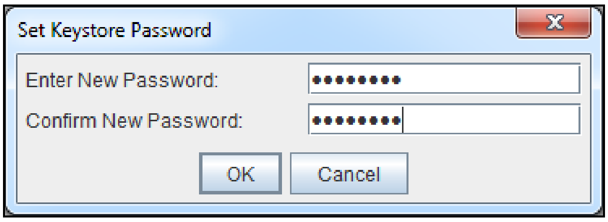
11. Save your Keystore



10-May-2017 13:21:00 CEST

Save the loaded keystore to disk

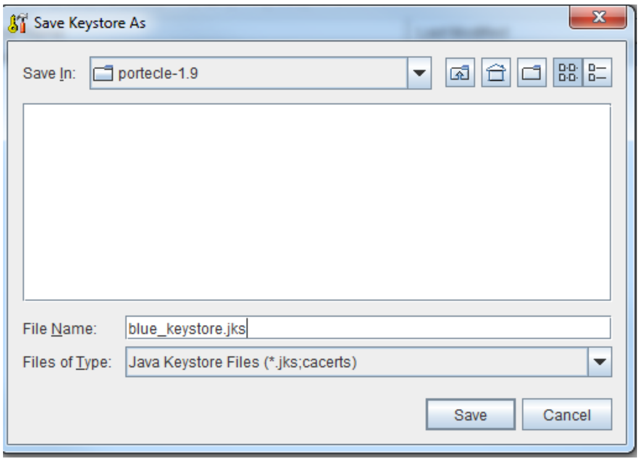
12. Set a Password for the Keystore then click on **OK**



Enter New Password: ••••••••

Confirm New Password: ••••••••

13. Choose the location and a name for the Keystore then click on OK



Save In: portecle-1.9

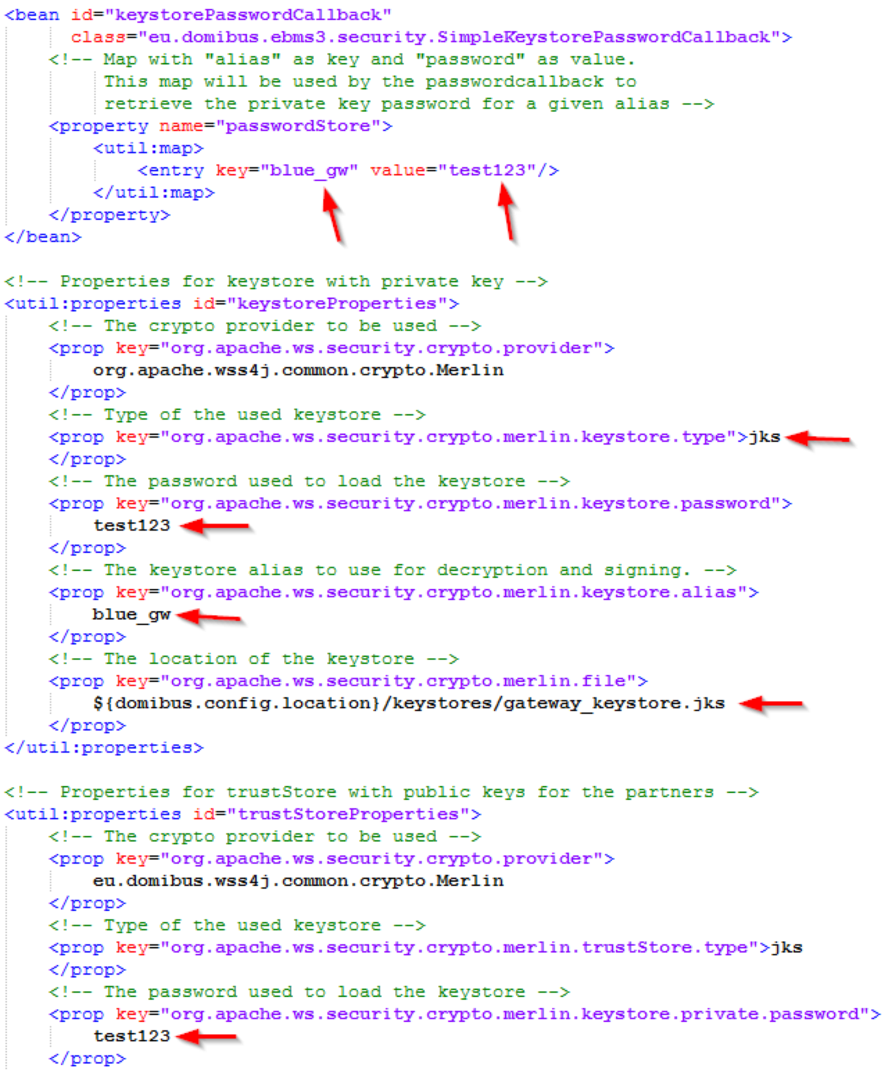
File Name: blue_keystore.jks

Files of Type: Java Keystore Files (*.jks;cacerts)

Configuration changes in domibus-security.xml / domibus.properties for the .JKS option:

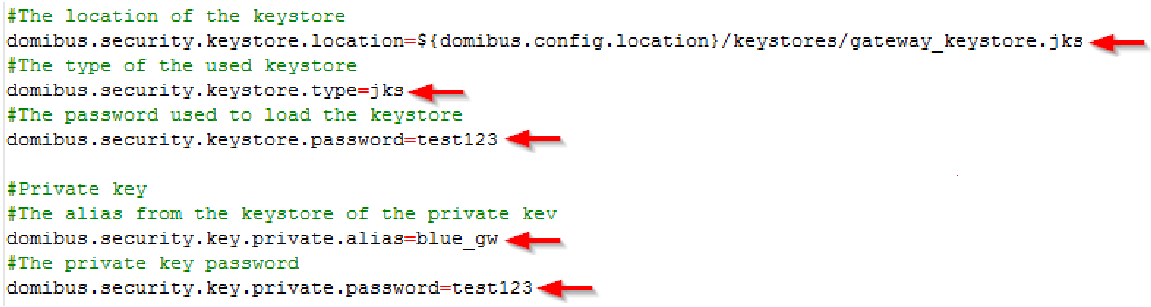
Depending on the version of Domibus that is being used, either domibus-security.xml (for version 3.2.5 and before) or domibus.properties (for version 3.3 and after) have to be updated with the keystore details included the JKS Keystore file, the chosen certificate alias and password, as shown in the examples below:

domibus-security.xml:



```
<bean id="keystorePasswordCallback"
      class="eu.domibus.ebms3.security.SimpleKeystorePasswordCallback">
    <!-- Map with "alias" as key and "password" as value.
         This map will be used by the passwordcallback to
         retrieve the private key password for a given alias -->
    <property name="passwordStore">
        <util:map>
            <entry key="blue_gw" value="test123"/>
        </util:map>
    </property>
</bean>

<!-- Properties for keystore with private key -->
<util:properties id="keystoreProperties">
    <!-- The crypto provider to be used -->
    <prop key="org.apache.ws.security.crypto.provider">
        org.apache.wss4j.common.crypto.Merlin
    </prop>
    <!-- Type of the used keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.type">jks
    </prop>
    <!-- The password used to load the keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.password">
        test123
    </prop>
    <!-- The keystore alias to use for decryption and signing. -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.alias">
        blue_gw
    </prop>
    <!-- The location of the keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.file">
        ${domibus.config.location}/keystores/gateway_keystore.jks
    </prop>
</util:properties>

<!-- Properties for trustStore with public keys for the partners -->
<util:properties id="trustStoreProperties">
    <!-- The crypto provider to be used -->
    <prop key="org.apache.ws.security.crypto.provider">
        eu.domibus.wss4j.common.crypto.Merlin
    </prop>
    <!-- Type of the used keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.trustStore.type">jks
    </prop>
    <!-- The password used to load the keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.private.password">
        test123
    </prop>
```

domibus.properties:

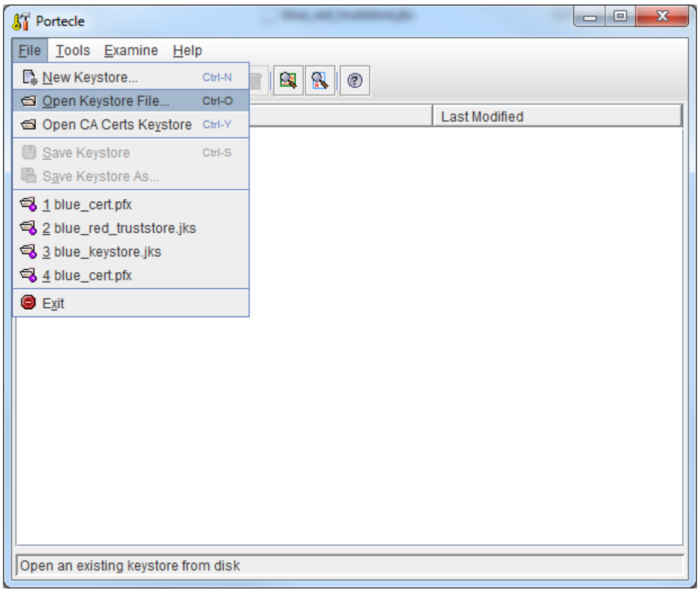


```
#The location of the keystore
domibus.security.keystore.location=${domibus.config.location}/keystores/gateway_keystore.jks
#The type of the used keystore
domibus.security.keystore.type=jks
#The password used to load the keystore
domibus.security.keystore.password=test123

#Private key
#The alias from the keystore of the private kev
domibus.security.key.private.alias=blue_gw
#The private key password
domibus.security.key.private.password=test123
```

5.5.2. OPTION2: PKCS12 Keystore (optional special request by some users)

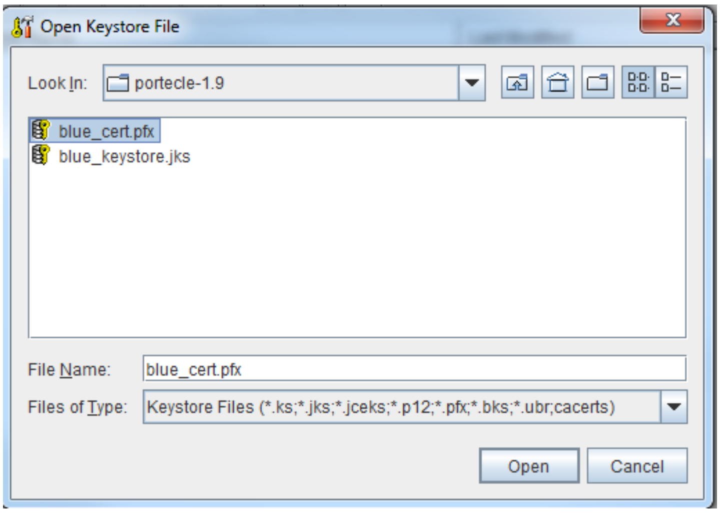
We need to make sure that the correct Alias is used in the PKCS12 Keystore, then rename it to have a .p12 extension instead of the default .pfx extension.

1. Start **portecle.jar** and choose **open Keystore file**



Open an existing keystore from disk

2. Select the .pfx private key that was exported earlier

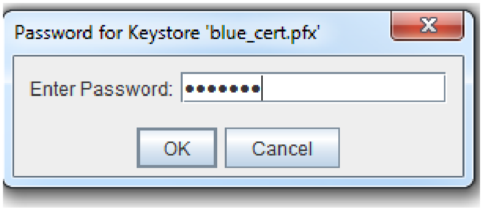


Look In: portecle-1.9

File Name: blue_cert.pfx

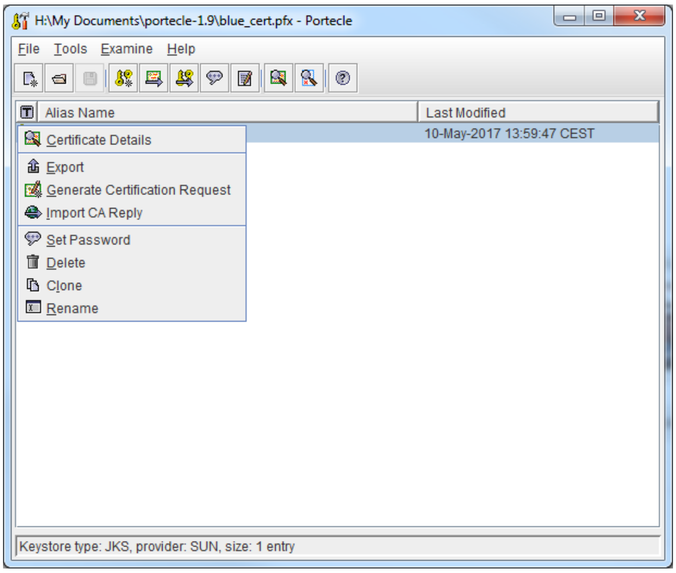
Files of Type: Keystore Files (*.ks;*.jks;*.jceks;*.p12;*.pfx;*.bks;*.ubr;cacerts)

3. Enter the password



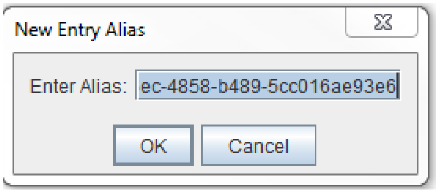
Enter Password: •••••••

4. Right click and choose rename


H:\My Documents\portecle-1.9\blue_cert.pfx - Portecle

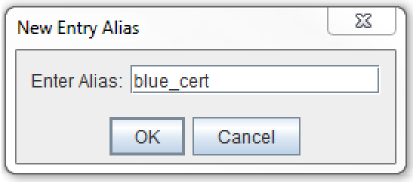
Alias Name	Last Modified
	10-May-2017 13:59:47 CEST

Keystore type: JKS, provider: SUN, size: 1 entry


New Entry Alias

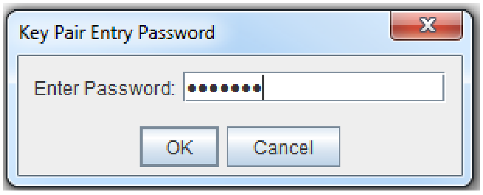
Enter Alias: ec-4858-b489-5cc016ae93e6

5. Replace the Alias with a new name


New Entry Alias

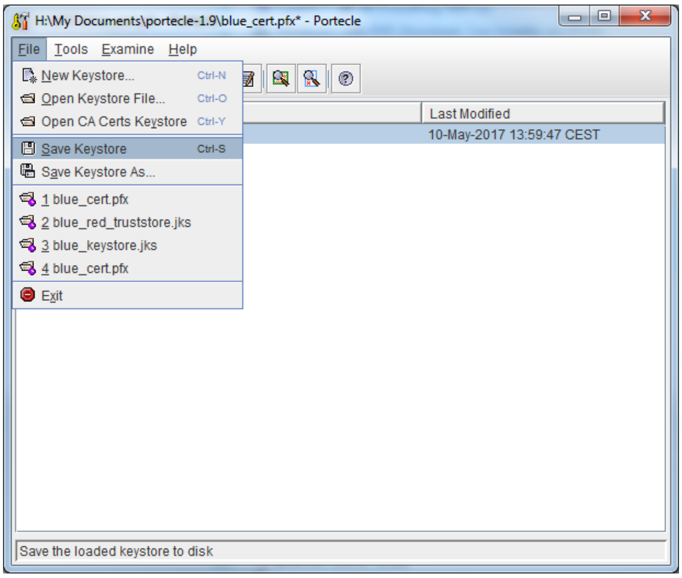
Enter Alias: blue_cert

6. Enter the password for the key pair


Key Pair Entry Password

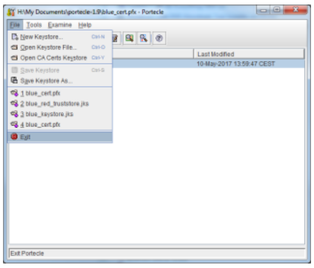
Enter Password: •••••••

7. Save the Keystore


H:\My Documents\portecle-1.9\blue_cert.pfx* - Portecle
File
Tools
Examine
Help
New Keystore... Ctrl-N
Open Keystore File... Ctrl-O
Open CA Certs Keystore Ctrl-Y
Save Keystore Ctrl-S
Save Keystore As...
1 blue_cert.pfx
2 blue_red_truststore.jks
3 blue_keystore.jks
4 blue_cert.pfx
Exit
Last Modified
10-May-2017 13:59:47 CEST

Save the loaded keystore to disk

8. Exit



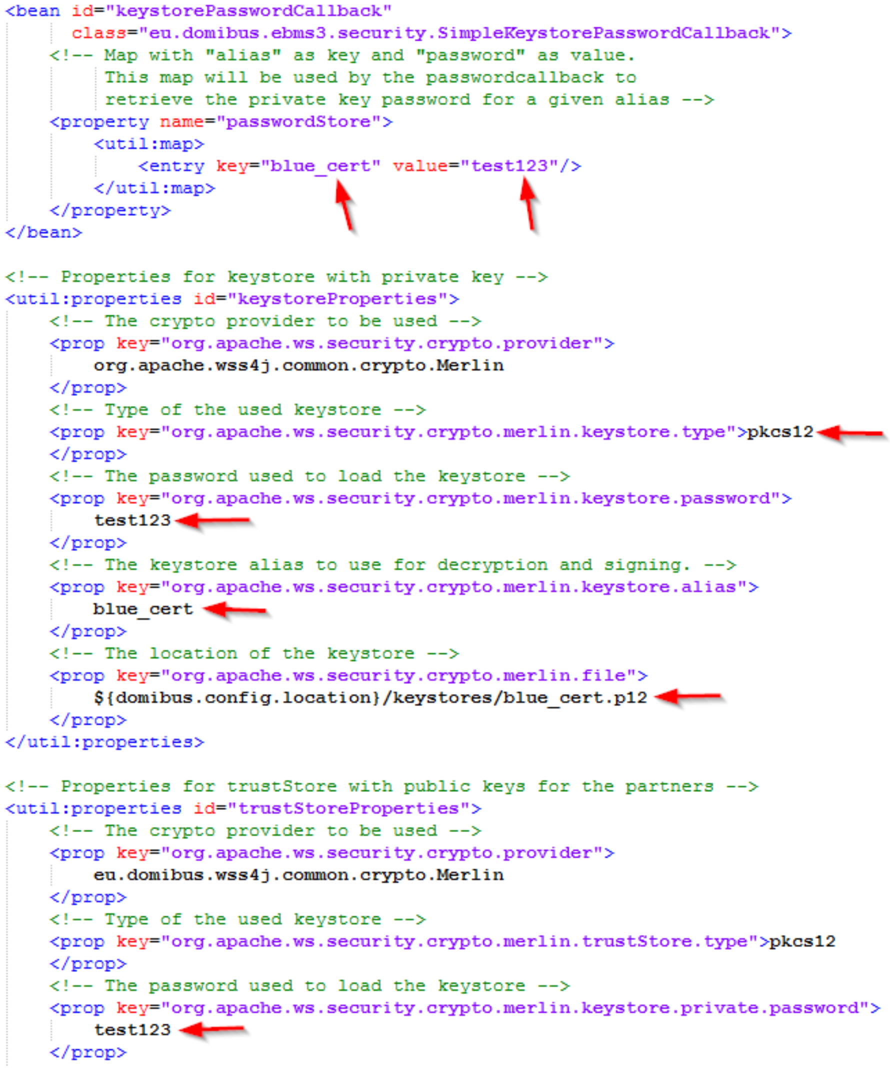
Exit Portecle

9. Change the Keystore file extension from **.pfx** to **.p12**. (e.g.: ***ren blue_cert.pfx blue_cert.p12***)

Configuration changes in domibus-security.xml / domibus.properties for the .PKCS12 option:

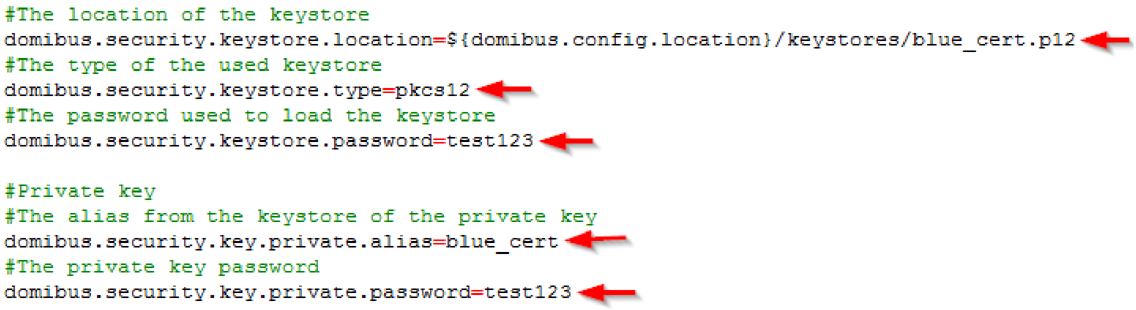
Depending on the version of Domibus that is being used, either domibus-security.xml (for version 3.2.5 and before) or domibus.properties (for version 3.3 and after) have to be updated with the keystore details included the PKCS12 keystore file, the chosen certificate alias and password, as shown in the examples below:

domibus-security.xml:



```
<bean id="keystorePasswordCallback"
      class="eu.domibus.ebms3.security.SimpleKeystorePasswordCallback">
    <!-- Map with "alias" as key and "password" as value.
         This map will be used by the passwordcallback to
         retrieve the private key password for a given alias -->
    <property name="passwordStore">
        <util:map>
            <entry key="blue_cert" value="test123"/>
        </util:map>
    </property>
</bean>

<!-- Properties for keystore with private key -->
<util:properties id="keystoreProperties">
    <!-- The crypto provider to be used -->
    <prop key="org.apache.ws.security.crypto.provider">
        org.apache.wss4j.common.crypto.Merlin
    </prop>
    <!-- Type of the used keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.type">pkcs12
    </prop>
    <!-- The password used to load the keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.password">
        test123
    </prop>
    <!-- The keystore alias to use for decryption and signing. -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.alias">
        blue_cert
    </prop>
    <!-- The location of the keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.file">
        ${domibus.config.location}/keystores/blue_cert.p12
    </prop>
</util:properties>

<!-- Properties for trustStore with public keys for the partners -->
<util:properties id="trustStoreProperties">
    <!-- The crypto provider to be used -->
    <prop key="org.apache.ws.security.crypto.provider">
        eu.domibus.wss4j.common.crypto.Merlin
    </prop>
    <!-- Type of the used keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.trustStore.type">pkcs12
    </prop>
    <!-- The password used to load the keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.private.password">
        test123
    </prop>
```

domibus.properties:

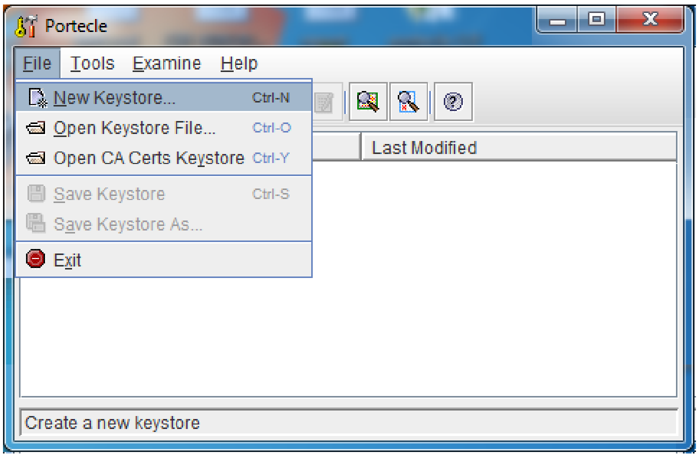


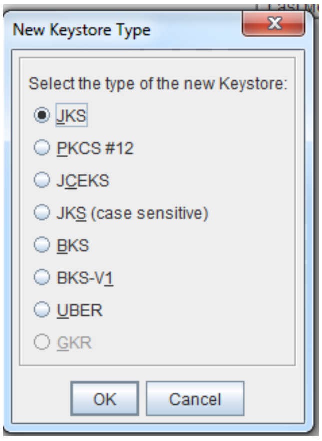
```
#The location of the keystore
domibus.security.keystore.location=${domibus.config.location}/keystores/blue_cert.p12
#The type of the used keystore
domibus.security.keystore.type=pkcs12
#The password used to load the keystore
domibus.security.keystore.password=test123

#Private key
#The alias from the keystore of the private key
domibus.security.key.private.alias=blue_cert
#The private key password
domibus.security.key.private.password=test123
```

5.6. Truststore Creation

Now that the public key has been retrieved, we can include it in a newly created (or existing) ***.jks*** *keystore file called truststore file (public keys), which will be used in the configuration of Domibus (truststore section of domibus-security.xml).*
These are the steps to follow:

1. Run Portecle, click on **File** then **New Keystore (**or **open Keystore File** if already exists**)**

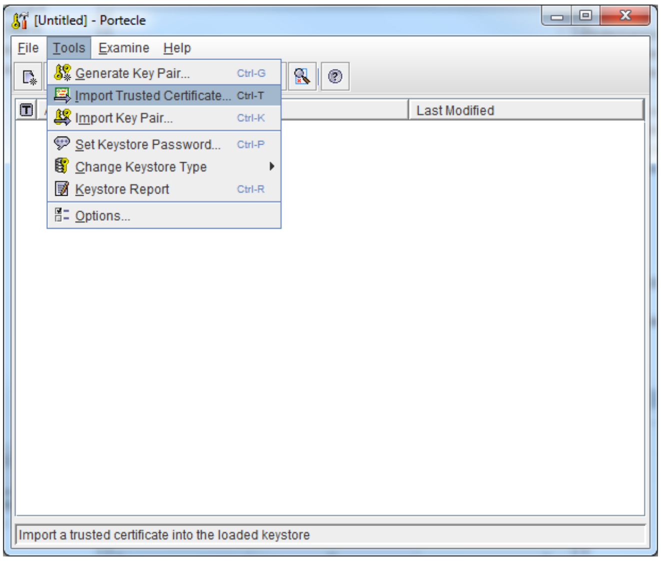



New Keystore Type

Select the type of the new Keystore:

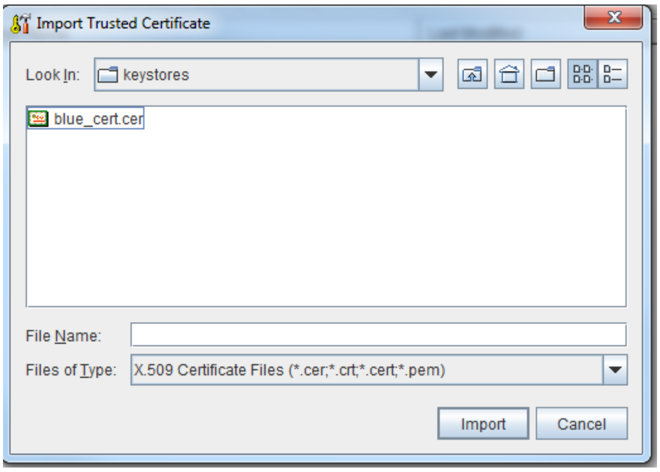
● JKS
○ PKCS #12
○ JCEKS
○ JKS (case sensitive)
○ BKS
○ BKS-V1
○ UBER
○ GKR

2. Click on the **Import Trusted Certificate** menu option.


[Untitled] - Portecle
File Tools Examine Help
Generate Key Pair... Ctrl-G
Import Trusted Certificate... Ctrl-T
Import Key Pair... Ctrl-K
Set Keystore Password... Ctrl-P
Change Keystore Type
Keystore Report Ctrl-R
Options...
Last Modified

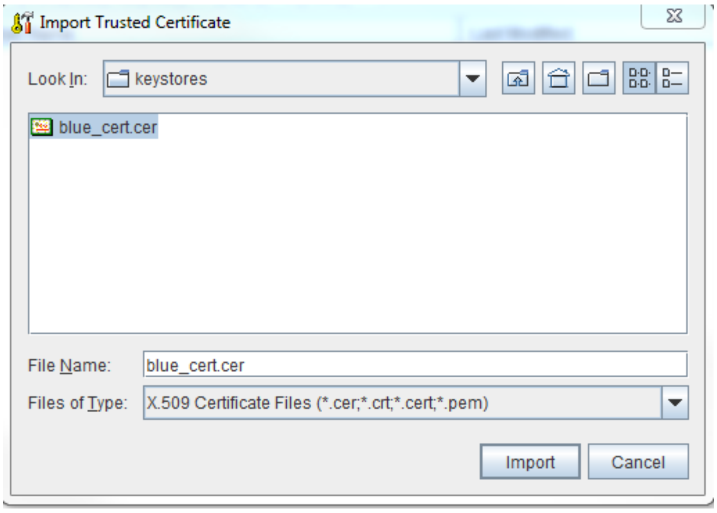
Import a trusted certificate into the loaded keystore

3. Select the public key that you exported (**.cer** extension) then click on **Import**



File Name:

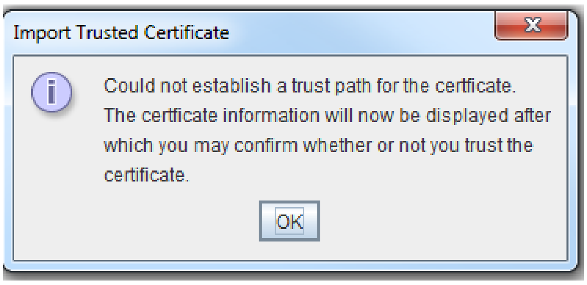
Files of Type: X.509 Certificate Files (*.cer;*.crt;*.cert;*.pem)



File Name: blue_cert.cer

Files of Type: X.509 Certificate Files (*.cer;*.crt;*.cert;*.pem)

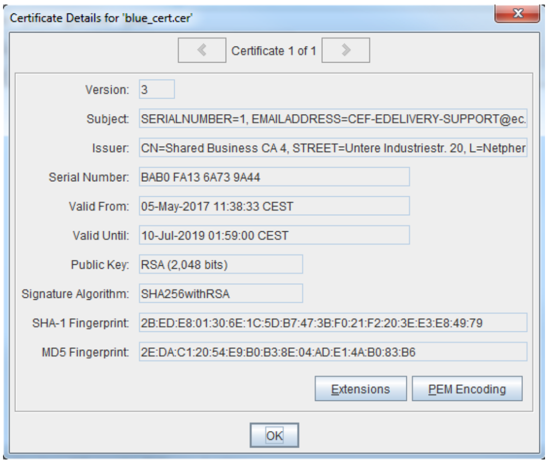
4. Click on **OK**



Import Trusted Certificate

Could not establish a trust path for the certficate. The certficate information will now be displayed after which you may confirm whether or not you trust the certificate.

5. Click on **OK**



Certificate Details for 'blue_cert.cer'

Certificate 1 of 1

Version: 3

Subject: SERIALNUMBER=1, EMAILADDRESS=CEF-EDELIVERY-SUPPORT@ec.

Issuer: CN=Shared Business CA 4, STREET=Untere Industriestr. 20, L=Netpher

Serial Number: BAB0 FA13 6A73 9A44

Valid From: 05-May-2017 11:38:33 CEST

Valid Until: 10-Jul-2019 01:59:00 CEST

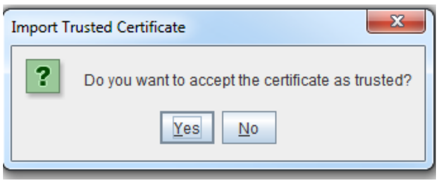
Public Key: RSA (2,048 bits)

Signature Algorithm: SHA256withRSA

SHA-1 Fingerprint: 2B:ED:E8:01:30:6E:1C:5D:B7:47:3B:F0:21:F2:20:3E:E3:E8:49:79

MD5 Fingerprint: 2E:DA:C1:20:54:E9:B0:B3:8E:04:AD:E1:4A:B0:83:B6

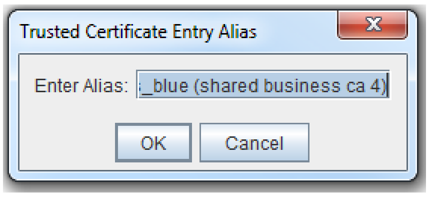
6. Click on **Yes**



Import Trusted Certificate

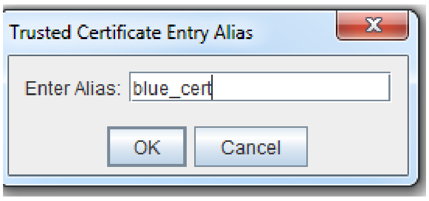
Do you want to accept the certificate as trusted?

7. Enter an Alias for the Trusted Certificate. (e.g.: blue_cert)



Trusted Certificate Entry Alias

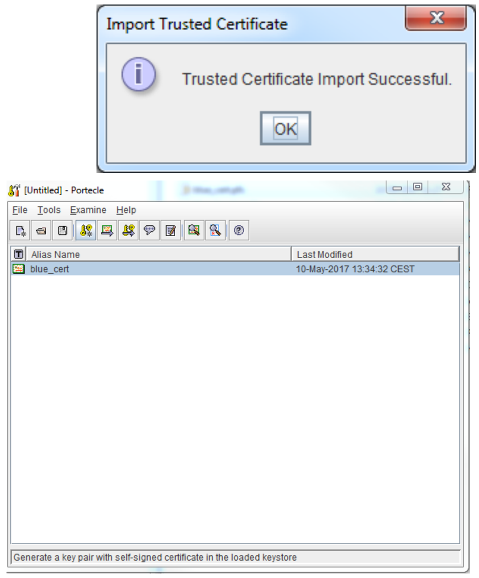
Enter Alias: :_blue (shared business ca 4)



Trusted Certificate Entry Alias

Enter Alias: blue_cert

8. Click on **OK**

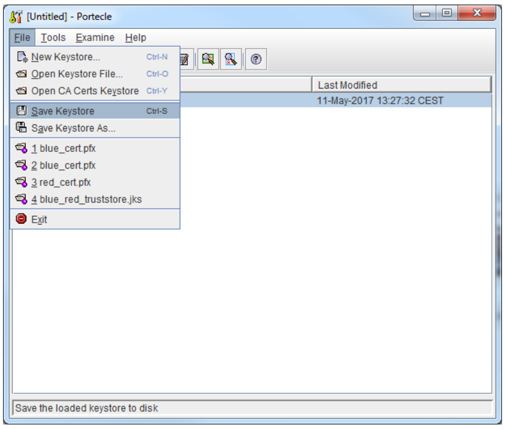


Trusted Certificate Import Successful.

Alias Name	Last Modified
blue_cert	10-May-2017 13:34:32 CEST

Generate a key pair with self-signed certificate in the loaded keystore

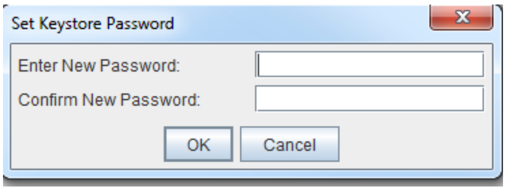
9. Save Keystore

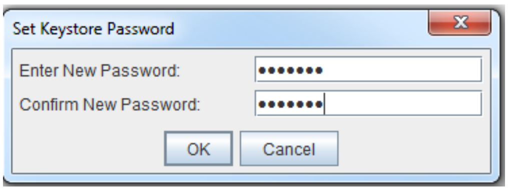


11-May-2017 13:27:32 CEST

Save the loaded keystore to disk

10. Choose a password for the keystore

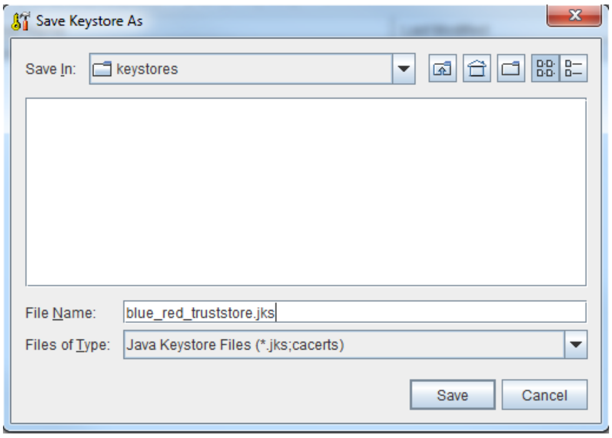




Enter New Password: •••••••

Confirm New Password: •••••••

11. Choose a name for the Keystore (e.g.:blue_red_truststore.jks)



Save In: keystores

File Name: blue_red_truststore.jks

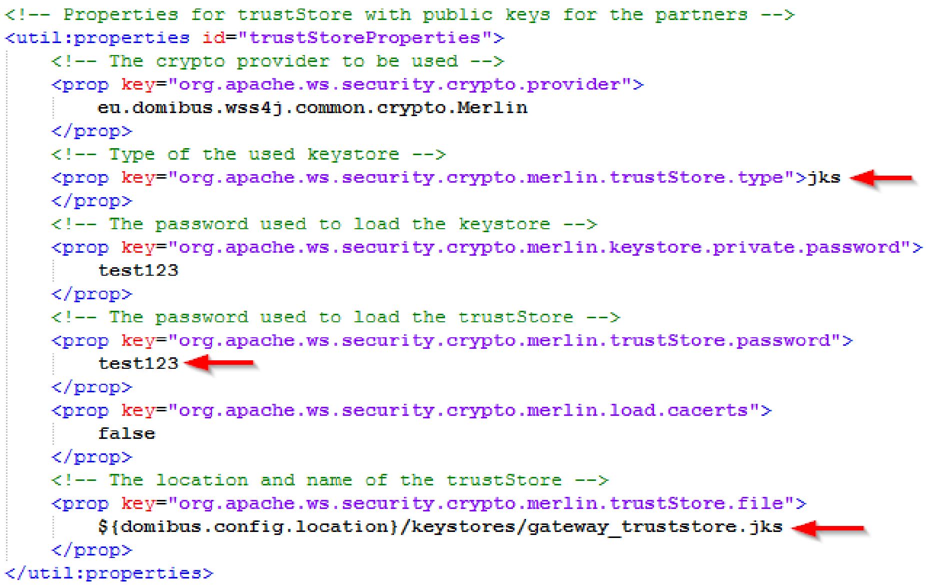
Files of Type: Java Keystore Files (*.jks;cacerts)

<u>NOTE:</u> Steps 2 to 13 can be repeated to import other public keys into the Truststore.

Configuration changes in the domibus-security.xml / domibus.properties for the JKS/PKCS12 option:

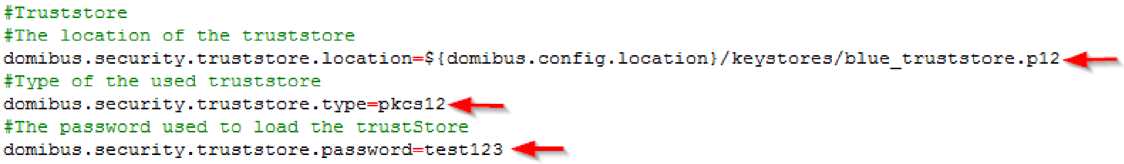
Depending on the version of Domibus that is being used, either domibus-security.xml (for version 3.2.5 and before) or domibus.properties (for version 3.3 and after) have to be updated with the truststore details included the JKS/PKCS12 truststore file and password, as shown in the examples below:

domibus-security.xml (with JKS option):



```
<!-- Properties for trustStore with public keys for the partners -->
<util:properties id="trustStoreProperties">
    <!-- The crypto provider to be used -->
    <prop key="org.apache.ws.security.crypto.provider">
        eu.domibus.wss4j.common.crypto.Merlin
    </prop>
    <!-- Type of the used keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.trustStore.type">jks
    </prop>
    <!-- The password used to load the keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.private.password">
        test123
    </prop>
    <!-- The password used to load the trustStore -->
    <prop key="org.apache.ws.security.crypto.merlin.trustStore.password">
        test123
    </prop>
    <prop key="org.apache.ws.security.crypto.merlin.load.cacerts">
        false
    </prop>
    <!-- The location and name of the trustStore -->
    <prop key="org.apache.ws.security.crypto.merlin.trustStore.file">
        ${domibus.config.location}/keystores/gateway_truststore.jks
    </prop>
</util:properties>
```

domibus.properties (with PKCS12 option):



```
#Truststore
#The location of the truststore
domibus.security.truststore.location=${domibus.config.location}/keystores/blue_truststore.p12
#Type of the used truststore
domibus.security.truststore.type=pkcs12
#The password used to load the trustStore
domibus.security.truststore.password=test123
```

5.7. General Terms and Conditions (GTC) of the CEF PKI service

Context

In its capacity as Solution Provider of the eDelivery Building Block of the Connecting Europe Facility, DIGIT makes available a PKI service[8] (referred to as "CEF PKI service") to the European Institutions, other Public Administrations and Businesses. The CEF PKI service is used by Organisations (referred to as "end-Users") participating in projects that deploy the components of CEF eDelivery.

DIGIT is a PKI tenant within the TeleSec Shared-Business-CA solution (referred to as "SBCA") operated in the Trust Center of the Group unit T-Systems International GmbH (referred to as "T-Systems"[9]). DIGIT plays the role of Master Registrar of the 'CEF_eDelivery.europa.eu' domain of the SBCA. In this role, DIGIT creates sub-domains within the 'CEF_eDelivery.europa.eu' domain for each project using the CEF PKI service.

This document provides details on the terms and conditions of the **TACHOnet project** (referred to as "the project") sub-domain. DIGIT plays the role of sub-Registrar of this sub-domain. In this capacity, it issues, revokes and renews the certificates of this project.

Disclaimer on liability

The European Commission accepts no responsibility or liability whatsoever with regard to the content of the certificate which lies exclusively with the certificate owner. It is the responsibility of the certificate owner to check the accuracy of the certificate content.

The European Commission accepts no responsibility or liability whatsoever with regard to the use of the certificate by its owner being a third legal entity outside the European Commission.

This disclaimer is not intended to limit the liability of the European Commission in contravention of any requirements laid down in applicable national law or to exclude its liability for matters which may not be excluded under that law.

Authorised /prohibited uses of certificates

Permitted usage of certificates

Once the certificate is issued, the end-User, referred to as the "certificate owner"[10], shall use the certificate only in the context of the aforementioned project. Within this context, the certificate can be used to:

- authenticate the origin of data;
- encrypt data;

[8] A PKI (Public Key Infrastructure) is a set of roles, policies, procedures and systems needed to create, manage, distribute, and revoke digital certificates.

[9] The trusted role of the Trust Center operator, located in the T-Systems Trust Center, also performs the task of internal registration authority.

[10] Identified by the "O=" attribute value in the Subject Distinguished Name of the issued certificate

- ensure detection of integrity breaches of data.

Prohibited usage of certificates

Any usage not explicitly authorised as part of the permitted usages of the certificate is prohibited.

Additional obligations of the certificate owner

The detailed terms and conditions of the SBCA are defined by T-Systems in the Certificate Policy (CP)/Certification Practice Statement (CPS) of the SBCA service11. This document includes security specifications and guidelines regarding technical and organizational aspects and describes the activities of the Trust Centre operator in the roles of Certification Authority (CA) and Registration Authority (RA) as well as the Registration Authority's (RA) delegated third party.

It should be highlighted that:

- Only entities authorised to participate in the aforementioned project can request a certificate, as described in the Service Offering Description document of the CEF PKI service for the aforementioned project.
- Regarding certificate acceptance, clause 4.4.1 of the SBCA CP/CPS applies, furthermore the terms of use and provisions described in the present document are deemed accepted by the organization to which the certificate is issued ("O=") when first used.
- Regarding publication of the certificate, clause 2.2 of the SBCA CP/CPS applies.
- All certificate owners and certified end-entities shall comply with the following requirements:
    - Protect their private key against unauthorized use.
    - Refrain from transferring or revealing their private key to third parties, even as representatives.
    - Refrain from continued use of the private key following expiry of the validity period or revocation of the certificate, other than to view encrypted data (e.g., decrypting e-mails).
    - The certificate owner is responsible for copying or forwarding the key to the end entity or entities.
    - The certificate owner must obligate the end entity/all end entities to comply with the present terms and conditions, including the SBCA CP/CPS, when dealing with the private key.
    - Certificate owner must provide the identification of those authorised representatives who are authorized to request revocation of certificates issued to the organisation with the details of events that lead to revocation and the revocation password.
    - For certificates associated to groups of persons and functions and/or legal persons, after a person leaves the group of end entities (e.g. termination of

[11] The latest version of the T-Systems SBCA CP/CPS is available from https://www.telesec.de/en/sbca-en/support/download-area/.

  - the employment relationship), the certificate owner must prevent misuse of the private key by revoking the certificate.
  - Certificate owner is responsible and has obligation to request revocation of certificate under circumstances identified in clause 4.9.1 of the SBCA CP/CPS.
- Regarding renewal or rekey of certificates, clause 4.6 or 4.7 of the SBCA CP/CPS applies.
- Regarding amendment of certificate, clause 4.8 of the SBCA CP/CPS applies.
- Regarding certificate revocation, clause 4.9 of the SBCA CP/CPS applies.

5.8. Contact persons and trusted couriers identification form (sample)

Please print the text of this document on your letterhead, add your organisation stamp and have it signed by an authorised representative of your organisation.

TACHOnet contact persons and trusted couriers identification form

I, *[name and address of the organisation representative]*, **certifies that the following information are to be used in the context of the request, generation and retrieval of public key digital certificates for TACHOnet access points supporting the confidentiality, integrity and non-repudiation of the TACHOnet messages:**

Contact person information**:**

Contact person #1	**Contact person #2**
Name:	Name:
First names:	First names:
Mobile phone:	Mobile phone:
Telephone:	Telephone:
Email:	Email:
Specimen handwritten signature:	Specimen handwritten signature:

Please duplicate the above table when more than two contact persons are required.

Trusted courier information**:**

Trusted courier #1	**Trusted courier #2**
Name:	Name:
First names:	First names:
Mobile phone:	Mobile phone:
Email:	Email:
Passport issuing country:	Passport issuing country:
Passport number:	Passport number:
Passport validity end date:	Passport validity end date:

Please duplicate the above table when more than two contact persons are required.

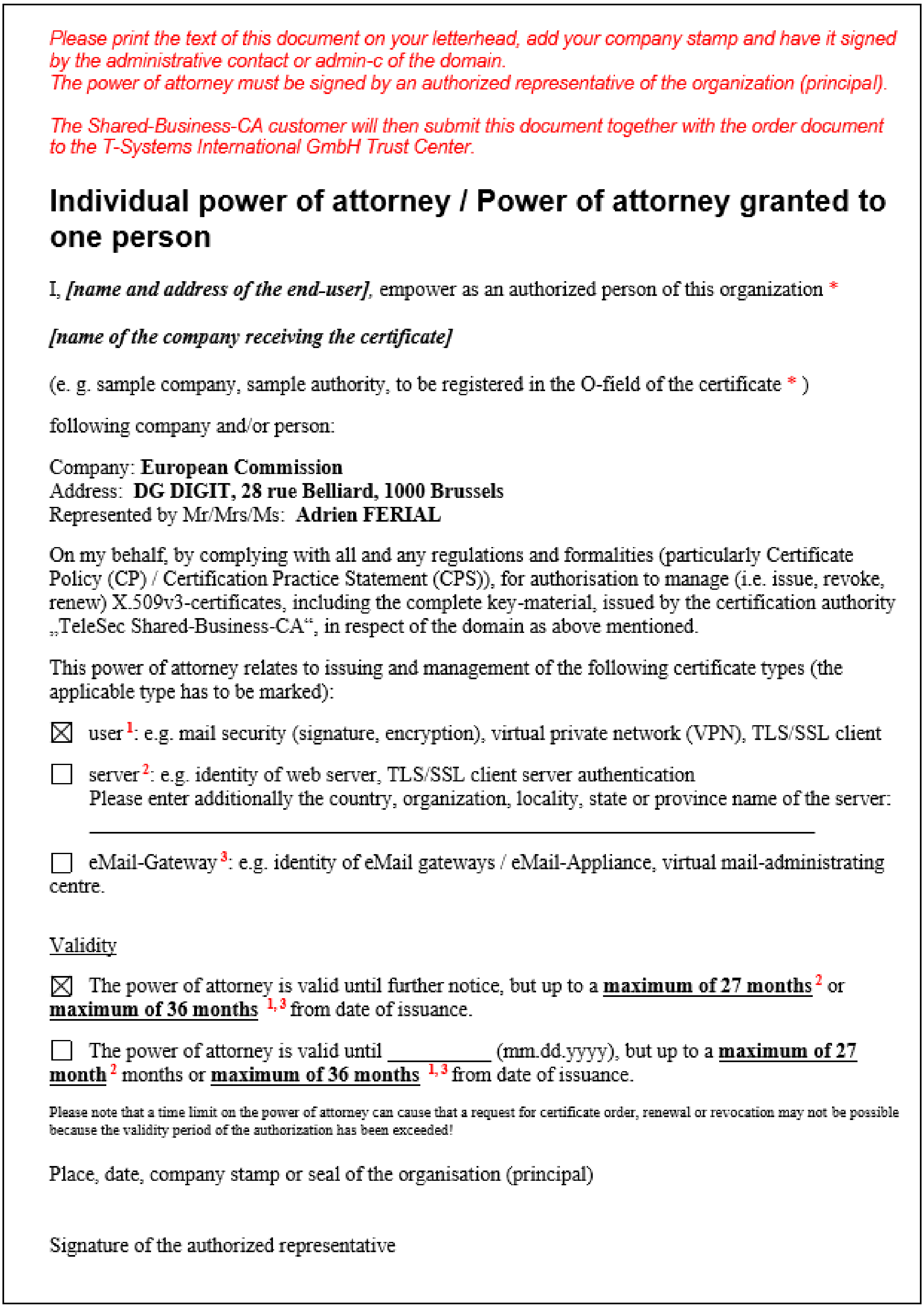
Please attach a high resolution copy of page 2 of the passport for all trusted couriers.

Place, date, company stamp or seal of the Organisation:

Signature of the authorised representative:

5.9. Individual Power of Attorney (sample)

A sample of the individual Power of Attorney that must be signed and presented by the trusted courier during face-to-face registration at RAO can be found here:



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

5.10. Certificate request paper form (sample)

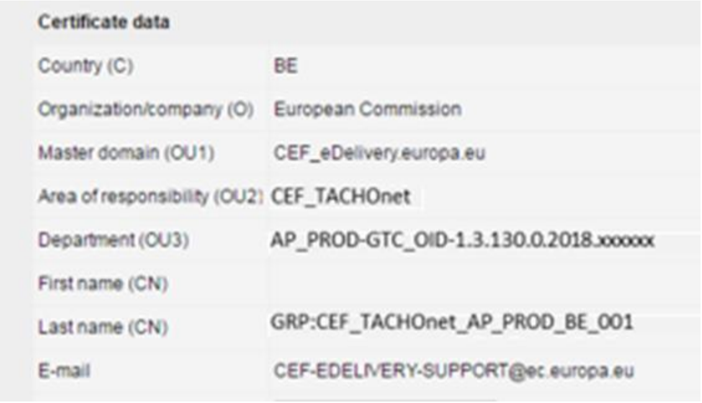
A sample of the certificate request paper form that must be signed and presented by the trusted courier during face-to-face registration at RAO can be found here:

Please print the text of this document on your letterhead, add your organisation stamp and have it signed by an authorised representative of your organisation.

TACHOnet certificate request paper form

I, *[name and address of the organisation representative]***, certifies that the following information are to be used in the context of the request, generation and retrieval of public key digital certificates for TACHOnet access points supporting the confidentiality, integrity and non-repudiation of the TACHOnet messages:**

Please reproduce the certificate data information provided by CEF Support Team acknowledging the completeness of the electronic certificate request, e.g.:



Certificate data	
Country (C)	BE
Organization/company (O)	European Commission
Master domain (OU1)	CEF_eDelivery.europa.eu
Area of responsibility (OU2)	CEF_TACHOnet
Department (OU3)	AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First name (CN)	
Last name (CN)	GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail	CEF-EDELIVERY-SUPPORT@ec.europa.eu

Certificate request reference number: ***insert reference number (e.g. 776002)***

Identification of the trusted courier proceeding to the face-to-face registration of the request: ***please fill in***

Trusted courier #1
Name:
First names:
Mobile phone:
Email:
Passport issuing country:
Passport number:
Passport validity end date:

Place, date, company stamp or seal of the Organisation:

Signature of the authorised representative:

6. List of Figures

7. List of tables

8. Contact Information

CEF Support Team

By email: CEF-EDELIVERY-SUPPORT@ec.europa.eu

By phone: +32 2 299 09 09

- **Standard Service: 8am to 6pm (Normal EC working Days)**
- **Standby Service*: 6pm to 8am (Commission and Public Holidays, Weekends)**

**** Only for critical and urgent incidents and only by phone***

Note: this draft has been submitted to the UNECE Secretariat as informal document. It has not been approved by the European Commission, and it is therefore only intended for discussion

Rules for the connection of AETR Contracting Parties to TACHOnet (the rules are provisional and subject to discussion with the competent services from the European Commission and with EU Member States)

Article 1

Scope and purpose

1. The present document sets out the terms and conditions regarding the connection of the parties to TACHOnet.

2. The parties connecting to TACHOnet which are not Member States to the EU shall abide by the provisions laid down in [this document].

3 Parties connecting to TACHOnet which are Member States to the EU may connect to TACHOnet under the terms and conditions specified in [this document], in which case they shall abide by the provisions laid down in it.

Article 2

Definitions

a) ‘Contracting party’ means any Contracting party to the AETR;

b) ‘TACHOnet’ means the system for the electronic exchange of information on driver cards between contracting parties.

c) ‘Requesting party’ means the contracting party emitting a TACHOnet request or a notification, which is then routed to the appropriate responding party by the central hub;

d) ‘Responding party’ means the contracting party to whom the TACHOnet request or notification is addressed;

e) ‘Card issuing authority’ or ‘CIA’ means the entity empowered by a contracting party for the issuing and management of tachograph cards;

Article 3

Legal and technical requirements

The contracting parties connecting to TACHOnet shall fulfil the legal and technical requirements set out in [this document], including its Annexes.

Article 4

General responsibilities

1. Neither contracting party may conclude agreements for the access to TACHOnet on behalf of other party or in any other way represent the other contracting party on the basis of [this document]. Neither contracting party acts as the other contracting party's subcontractor in the operations referred to in [this document].

2. The contracting parties shall provide access to their national register on driver cards through TACHOnet, in the way and with the level of service as defined in Annex VI.

3. The parties shall notify each other without delay if they observe disturbances or errors within their domain of responsibility, which may endanger the fulfilling of the normal operation of TACHOnet.

4. Each party shall designate contact persons for TACHOnet. Any change in contact points must be provided to the AETR Secretariat in writing.

Article 5

Tests for connection to TACHOnet

1. The connection of a contracting party to TACHOnet shall be established after the successful completion of the connection, integration and performance tests in accordance with the instructions and under the supervision of the European Commission.

2. In case of failure of the preliminary tests, the European Commission may temporarily put on hold the testing phase. The tests shall resume once the contracting party has communicated to the European Commission the adoption of the necessary technical improvements at national level, allowing the successful performance of the preliminary tests.

3. The maximum duration of the preliminary tests shall be six months.

Article 6

Trust architecture

1. Confidentiality, integrity and non-repudiation of the TACHOnet messages shall be ensured by the TACHOnet trust architecture.

2 The TACHOnet trust architecture shall be based on a public key infrastructure (PKI) service set up by the European Commission, which requirements are laid down in Annex VIII.

3. The following entities shall intervene in the TACHOnet trust architecture:

a) Certification Authority, responsible for the generation of the digital certificates to be delivered by the Registration Authority to the national authorities of the contracting parties (via trusted couriers appointed by them), as well as for setting up the technical infrastructure regarding the issuance, revocation and renewal of digital certificates.

b) Domain Owner, responsible for the operation of the central hub and for the general validation and coordination of the TACHOnet trust architecture.

c) Registration Authority, responsible for registering and approving the requests of issuance, revocation and renewal of digital certificates, and for verifying the identity of the trusted couriers.

d) Trusted Courier, is the person appointed by the national authorities, responsible for handing the public key to the Registration Authority and for getting the corresponding certificate being generated by the Certification Authority.

e) National authority from the contracting party, which shall:

- generate the private keys and the corresponding public keys to be included in the certificates to be generated by the Certification Authority;

- request the digital certificates to the Registration Authority;

- appoint the Trusted Courier.

4. The Certification Authority and the Registration Authority shall be appointed by the European Commission.

5. Any contracting party connecting to TACHOnet must request the issuance of a digital certificate in accordance with Annex VIII, in order to sign and encrypt a TACHOnet message.

6. A certificate may be revoked in accordance with Annex VIII.

Article 7

Data protection and confidentiality

1. The parties, in compliance with data protection laws at international and national level, and in particular with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, shall adopt all necessary technical and organisational measures to guarantee the security of the TACHOnet data and prevent the alteration or loss of, or unauthorised processing of or access to such data (in particular the authenticity, data confidentiality, traceability, integrity, availability and non-repudiation and security of the messages).

2. Each party shall protect its own national systems against illicit use, malicious code, viruses, computer intrusions, infringements and illegal tampering of data and other comparable actions by third parties. The parties agrees to use commercially reasonable efforts to avoid the transmission of any viruses, time bombs, worms or

similar items or any computer programming routines that may interfere with other Party's computer systems.

Article 8

Costs

1. The parties shall bear their own development and operation costs in conjunction to their own data systems and procedures as required to fulfil the obligations according to [this document].

2. The services specified in Annex I, provided by the central hub, are free of charge.

Article 9

Subcontracting

1. The parties may subcontract any of the services for which they are responsible under [this document].

2. Such subcontracting does not relieve the party from the responsibility pursuant to [this document], including the responsibility for the appropriate level of service in accordance with Annex VI.

ANNEX I

General aspects of TACHOnet

1. General description

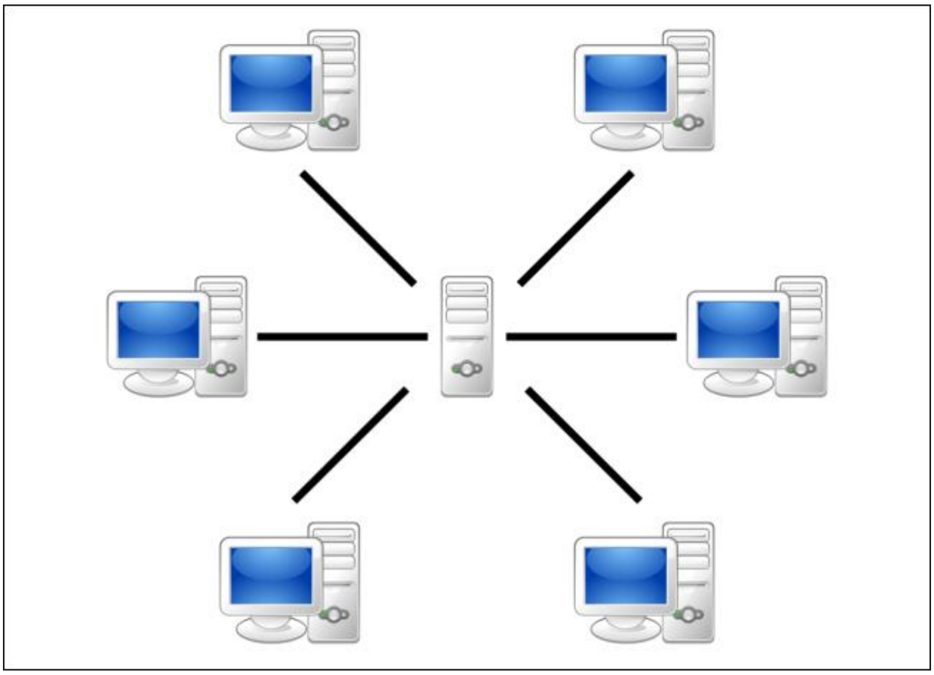
TACHOnet is an electronic system for the exchange of information on driver cards between AETR contracting parties. TACHOnet network routes the requests for information from the requesting parties to the responding parties, as well as the replies from the latter to the former. Contracting parties being part of TACHOnet must connect their national registers on driver cards to the system.

2. Architecture

TACHOnet messaging system shall be composed of the following parts:

1.1. A central hub, which shall be able to receive a request from the requesting party, validate it and process it by forwarding it to the responding parties. The central hub shall wait for each responding party to answer, consolidate all the answers and forward the consolidated response to the requesting Party.

1.2. National systems of the parties, which shall be fitted with an interface capable of both sending requests to the central hub and receiving the corresponding replies. National systems may use propriety or commercial software to transmit and receive messages from the central hub.



3. Management

3.1. The central hub shall be managed by the European Commission, which shall be responsible for the technical operation and maintenance of the central hub.

2.2. The central hub shall not store data for a period exceeding six months, other than the logging and statistical data set out in Annex VII.

2.3. The central hub shall not provide access to personal data, except for authorized European Commission personnel, when necessary for the purpose of monitoring, maintenance and troubleshooting.

2.4. Each contracting party shall be responsible for:

2.4.1. The setup and management of their national systems, including the interface with the central hub.

2.4.2. The installation and maintenance of their national system, both hardware and software, whether proprietary or commercial.

2.4.3. The correct interoperability of their national system with the central hub, including the management of error messages received from the central hub.

2.4.4. Taking all the measures to ensure the confidentiality, integrity and availability of the information.

2.4.5. The operation of the national systems in accordance with the service levels set out in Annex VI.

ANNEX II

Functionalities of TACHOnet

1. The following functionalities shall be provided through TACHOnet messaging system:

1.1. Check Issued Cards (CIC): allows the requesting party to send a Check Issued Cards Request to one or all responding parties, to determine if a card applicant already possesses a driver card issued by the responding parties. The responding parties shall reply to the request by sending a Check Issued Cards Response.

1.2. Check Card Status (CCS): allows the requesting party to ask the responding Party about the details of a card issued by the latter by sending a Check Card Status Request. The responding party shall reply to the request by sending a Check Card Status Response.

1.3. Modify Card Status (MCS): allows the requesting party to notify the responding Party, through a Modify Card Status Request, that the status of a card issued by the latter has changed. The responding party shall reply with a Modify Card Status Acknowledgement.

1.4. Issued Card Driving License (ICDL): allows the requesting party to notify the responding party, through an Issued Card Driving Licence Request, that a card has been issued by the former against a driving licence issued by the latter. The responding party shall reply with an Issued Card Driving Licence Response.

2. Other message types deemed suitable for the efficient functioning of TACHOnet shall be included, for instance error notifications.

3. National systems shall recognize the card statuses listed in the Appendix to this Annex, when using any of the functionalities described in point 1. However, parties are not required to implement an administrative procedure that makes use of all of the listed statuses.

4. When a party receives a response or notification giving a status that is not used in its administrative procedures, the national system shall translate the status on the received message to the appropriate value in that procedure. The message shall not be rejected by the responding party, as long as the status in the message is listed in the Appendix of this Annex.

5. The card status listed in the Appendix to this Annex shall not be used to determine if a driver card is valid for driving. When a party queries the register of the card issuing national authority via the CCS functionality, the response shall contain the dedicated field ‘valid for driving’. The national administrative procedures shall be such that CCS responses always contain the appropriate ‘valid for driving’ value.

Appendix

Card statuses

Card Status	Definition
Application	The CIA has received an application to issue a driver card. This information has been registered and stored in the database with the generated search keys.
Approved	The CIA has approved the application for the tachograph card.
Rejected	The CIA did not approve the application.
Personalised	The tachograph card has been personalised.
Dispatched	The National Authority has dispatched the driver card to the relevant driver or delivering agency.
Handed Over	The National Authority has handed over the driver card to the relevant driver.
Confiscated	The driver card has been taken from the driver by the competent authority.
Suspended	The driver card has been taken temporarily from the driver.
Withdrawn	The CIA has decided to withdraw the driver card. The card has been permanently invalidated.
Surrendered	The tachograph card has been returned to the CIA, and declared no longer needed.
Lost	The tachograph card has been declared lost to the CIA.
Stolen	The tachograph card has been reported stolen to the CIA. A stolen card is considered lost.
Malfunctioning	The tachograph card has been reported as malfunctioning to the CIA.
Expired	The period of validity of the tachograph card has expired.
Replaced	The tachograph card, which has been reported lost, stolen or malfunctioning, has been replaced by a new card. The data on the new card is the same, with the exception of the card number replacement index, which has been increased by one.
Renewed	The tachograph card has been renewed because of a change of administrative data or the validity period coming to an end. The card number of the new card is the same, with the exception of the card number renewal index, which has been increased by one.
In Exchange	The CIA that issued a driver card has received a notification that the procedure to exchange that card for a driver card issued by the CIA of another Party has started.

Card Status	**Definition**
Exchanged	The CIA that issued a driver card has received a notification that the procedure to exchange that card for a driver card issued by the CIA of another Party has completed.

ANNEX III

Message provisions of TACHOnet

1. General technical requirements

1.1. The central hub shall provide both synchronous and asynchronous interfaces for the exchange of messages. Parties may choose the most suitable technology to interface with their own applications.

1.2. All messages exchanged between the central hub and the national systems must be UTF-8 encoded.

1.3. National systems shall be capable of receiving and processing messages containing Greek or Cyrillic characters.

2. XML messages structure and Schema definition (XSD)

2.1. The general structure of XML messages shall follow the format defined by the XSD schemas installed in the central hub.

2.2. The central hub and the national systems shall transmit and receive messages that conform to the message XSD schema.

2.3. National systems shall be capable of sending, receiving and processing all messages corresponding to any of the functionalities set out in Annex I.

2.4. The XML messages shall include at least the minimum requirements laid down in the Appendix to this Annex.

Appendix

Minimum requirements for the content of the XML messages

Common Header		Mandatory
Version	The official version of the XML specifications will be specified through the namespace defined in the message XSD and in the *version* attribute of the Header element of any XML message. The version number ('n.m') will be defined as fixed value in every release of the XML Schema Definition file (xsd).	Yes
Test Identifier	Optional id for testing. The originator of the test will populate the id and all participants in the workflow will forward / return the same id. In production it should be ignored and will not be used if it is supplied.	No
Technical Identifier	A UUID uniquely identifying each individual message. The sender generates a UUID and populates this attribute. This data is not used in any business capacity.	Yes
Workflow Identifier	The workflowId is a UUID and should be generated by the requesting Party. This id is then used in all messages to correlate the workflow.	Yes
Sent At	The date and time (UTC) that the message was sent.	Yes
Timeout	This is an optional date and time (in UTC format) attribute. This value will be set only by the Hub for forwarded requests. This will inform the responding party of the time when the request will be timed out. This value is not required in MS2TCN_<x>_Req and all response messages. It is optional so that the same header definition can be used for all message types regardless of whether or not the timeoutValue attribute is required.	No
From	The ISO 3166-1 Alpha 2 code of the party sending the message or 'EU'.	Yes
To	The ISO 3166-1 Alpha 2 code of the party to which the message is being sent or 'EU'.	Yes

ANNEX IV

Transliteration and NYSIIS (New York State Identification and Intelligence System) Services

1. The NYSIIS algorithm implemented in the central hub shall be used to encode the names of all the drivers in the national register.

2. When searching for a card via the CIC functionality the NYSIIS keys shall be used as the primary search mechanism.

3. Additionally, parties may employ a custom algorithm to return additional results.

4. The search results shall indicate the search mechanism which was used to find a record, either NYSIIS or custom.

5. If a party chooses to record ICDL notifications then the NYSIIS keys contained in the notification shall be recorded as part of the ICDL data.

5.1 When searching the ICDL data the party shall use the NYSIIS keys of the applicant’s name.

ANNEX V

Security requirements

1. HTTPS shall be used for the exchange of messages between the central hub and the national systems.

2. National systems shall use the PKI certificates provided by the European Commission for the purposes of securing the transmission of messages between the national system and the central hub.

3. National systems shall implement, as a minimum, certificates using the SHA-2 (SHA-256) signature hash algorithm and a 2048 bit public key length.

ANNEX VI

Service levels

1. National systems shall fulfil the following minimum level of service:

1.1. They shall be available 24 hours a day, 7 days a week.

1.2. Their availability shall be monitored by a heartbeat message issued from the central hub.

1.3. Their availability rate shall be 98%, according to the following table (the figures have been rounded to the nearest convenient unit):

An availability of	means an unavailability of		
	Daily	Monthly	Yearly
98%	0.5 hours	15 hours	7.5 days

Parties are encouraged to respect the daily availability rate, however it is recognised that certain necessary activities, such as system maintenance, require a down time of more than 30 minutes. However, the monthly and yearly availability rates remain mandatory.

1.4. They shall respond to a minimum of 98% of the requests forwarded to them in one calendar month.

1.5. They shall respond to requests within 10 seconds.

1.6 The global request timeout (time within which the requestor may wait for a response) shall not exceed 20 seconds.

1.7. They shall be able to service a request rate of 6 messages per second.

1.8. National systems may not send requests to the TACHOnet hub at a rate exceeding 2 requests per second.

1.9. Every national system shall be able to cope with potential technical problems of the central hub or national systems in other parties. These include, but are not limited to:

(a) loss of connection to the central hub;

(b) no response to a request;

(c) receipt of responses after message timeout;

(d) receipt of unsolicited messages;

(e) receipt of invalid messages.

2. The central hub shall:

2.1. feature an availability rate of 98%;

2.2. provide to national systems notification of any errors, either via the response message or via a dedicated error message. The national systems, in turn, shall receive these dedicated error messages and have an escalation workflow in place to take any appropriate action to rectify the notified error.

3. Maintenance

Parties shall notify other parties and the European Commission of any routine maintenance activities via the web application, at least one week before the beginning of those activities if technically possible.

ANNEX VII

Logging and Statistics of the data collected at the central hub

1. In order to ensure privacy, the data for statistical purposes shall be anonymous. Data identifying a specific card, driver or driver licence shall not be available for statistical purposes.

2. Logging information shall keep track of all transactions for monitoring and debugging purposes, and allow the generation of statistics about these transactions.

3. Personal data shall not be retained in the logs for more than 6 months. Statistical information shall be retained indefinitely.

4. The statistical data used for reporting shall include:

(a) the requesting party;

(b) the responding party;

(c) the type of message;

(d) the status code of the response;

(e) the date and time of the messages;

(f) the response time.

ANNEX VIII

PKI service for TACHOnet

1. The Directorate General for Informatics of the European Commission (DIGIT) shall make available a PKI service[1] (referred to as “CEF PKI service”) to the AETR Contracting Parties connecting to TACHOnet (henceforth the national authorities).

2. The procedure for request and revocation of TACHOnet certificates, as well as the detailed terms and conditions for its usage, are defined in the Appendix

3. Usage of certificates:

3.1. Once the certificate is issued, the national authority[2], shall use the certificate only in the context of TACHOnet. The certificate can be used to:

a) authenticate the origin of data;

b) encrypt data;

c) ensure detection of integrity breaches of data.

3.2. Any usage not explicitly authorised as part of the permitted usages of the certificate is prohibited.

4. Contracting parties shall:

a) Protect their private key against unauthorized use.

b) Refrain from transferring or revealing their private key to third parties, even as representatives.

c) Ensure confidentiality, integrity, and availability of the private keys generated, stored and used for TACHOnet.

d) Refrain from continued use of the private key following expiry of the validity period or revocation of the certificate, other than to view encrypted data (e.g., decrypting e-mails). Expired keys shall be either destroyed or retained in a manner preventing its use.

e) Provide the Registration Authority with the identification of those authorised representatives who are authorized to request revocation of certificates issued to the organisation (revocation requests shall include a revocation request password and details about the events that lead to revocation).

f) Prevent misuse of the private key by requesting the revocation of the associated public key certificate in case of compromise of the private key or of the private key activation data.

[1] A PKI (Public Key Infrastructure) is a set of roles, policies, procedures and systems needed to create, manage, distribute, and revoke digital certificates.

[2] Identified by the “O=” attribute value in the Subject Distinguished Name of the issued certificate

g) Be responsible and hold the obligation of requesting revocation of certificate under circumstances identified in the certification policies (CP) and certification practices statement (CPS) of the Certification Authority.

h) Notify the Registration Authority without delay of loss, theft, or potential compromise of any AETR keys used in the context of TACHOnet.

5. Liabilities

Without prejudice of the liability of the European Commission in contravention of any requirements laid down in applicable national law or with respect to liability for matters which may not be excluded under that law, the European Commission shall not be responsible or liable with regard to:

a) the content of the certificate which lies exclusively with the certificate owner. It shall be the responsibility of the certificate owner to check the accuracy of the certificate content.

b) the use of the certificate by its owner.

Appendix

Public Key Infrastructure

Service Offering Description

PKI for TACHOnet

Table of Contents

1. Introduction

A PKI (Public Key Infrastructure) is a set of roles, policies, procedures and systems needed to create, manage, distribute, and revoke digital certificates[3]. The PKI service of CEF eDelivery enables issuance and management of digital certificates used to ensure confidentiality, integrity and non-repudiation of the information exchanged between the eDelivery components i.e. between Access Points (AP).

The PKI service of CEF eDelivery is based on the Trust Center Services TeleSec Shared Business CA (Certification Authority) for which the Certificate Policy (CP) / Certification Practices Statement (CPS) of TeleSec Shared-Business-CA of T-Systems International GmbH[4] apply.

The CEF PKI service issues certificates that are suitable for securing various business processes within and outside of companies, organisations, public authorities and institutions that require a medium security level to prove the authenticity, integrity and trustworthiness of the end-entity.

In the annex at the end of this document, you will find the procedures to create the Keystores, Truststores and their corresponding configuration in Domibus.

This document provides details on the issuance of the certificates for the Organisations participating to the TACHOnet project.

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

[4] The latest version of the CP and CPS can be downloaded on https://www.telesec.de/en/sbca-en/support/download-area/

2. CERTIFICATE REQUEST PROCESS

This section describes the complete certificate issuance workflow and associated processes that lead to the publication of certificates for use in the TACHOnet project as they are generated by the CEF eDelivery PKI Service.

Remarks:

- *The PKI service Shared Business CA does not support Windows 10. Please only use Windows 7.*
- *Please use Mozilla Firefox whenever possible which works well with the T-Systems Portal.*
- *Google Chrome cannot be used as it has disabled key generation.*

2.1. Roles and Responsibilities

2.1.1. The "Organisation" or the "national authority" requesting the certificate

Entity: National Authority.

Role: Organisation which is requesting the certificates in the context of the TACHOnet project.

Responsibilities:

- Requests the services of the CEF PKI service to get the valid certificates.
- Generate the private keys and the corresponding public keys to be included in the certificates issued by the Certification Authority (CA).
- Download the certificate when approved.
- Sign and send back to the RA
  - The contact persons and trusted couriers identification form;
  - The signed individual Power of Attorney[5].

[5] A power of attorney is a legal document by which the Organisation empowers and authorises the European Commission represented by the identified official responsible for the CEF PKI service the power to request the generation of a certificate on its behalf from the T-Systems International GmbH TeleSec Shared Business CA. See also §5.9 - Contact persons and trusted couriers identification form (sample)

Please print the text of this document on your letterhead, add your organisation stamp and have it signed by an authorised representative of your organisation.

TACHOnet contact persons and trusted couriers identification form

I, *[name and address of the organisation representative]***, certifies that the following information are to be used in the context of the request, generation and retrieval of public key digital certificates for TACHOnet access points supporting the confidentiality, integrity and non-repudiation of the TACHOnet messages:**

Contact person information**:**

Contact person #12	**Contact person #2F**
Name:	Name: t
First names::	First names:n
Mobile phone::	Mobile phone:T
Telephone::	Telephone:m
Email::	Email:
Specimen handwritten signature:	Specimen handwritten signature:

Please duplicate the above table when more than two contact persons are required.

Trusted courier information**:**

Trusted courier #12	**Trusted courier #2i**
Name:	Name: t
First names:	First names:b obile phone:onbbile phone:: mail:aiaail:as assport issuing country:trsssport g country:assport assport number:besssport :umber:sp assport validity end date:atsssport validity end cate th *Please duplicate the above table when more than two contact persons are required.*
Mobile phone::	Mobile phone:l
Email::	Email:p
Passport issuing country::	Passport issuing country:r
Passport number::	Passport number:i
Passport validity end date::	Passport validity end date:e

Please duplicate the above table when more than two contact persons are required.

Please attach a high resolution copy of page 2 of the passport for all trusted couriers.

Place, date, company stamp or seal of the Organisation:

Signature of the authorised representative:

2.1.2. The Trusted Courier

Entity: A Trusted Courier is a natural person appointed by the responsible for handing the public key to the Registration Authority and for getting the corresponding certificate from the Registration Authority.

Role: Execute the face-to-face presentation against the Registration Authority, representing the Organisation that is requesting the certificates.

Responsibilities:

- Hands over the public key to the Registration Authority during a face-to-face identification and registration process,
- Gets the corresponding certificate from the Registration Authority.

2.1.3. The Domain Owner

Entity: DG MOVE, acting as the TACHOnet project owner.

Role: Entity responsible for the project and project domain, namely the TACHOnet project, in which the certificates will be used. Also referred to as the "Domain owner" or "Sub-domain owner".

Responsibilities:

- General validation and coordination of the TACHOnet trust architecture, including validation of the procedures for the issuance of the certificates;
- Operate the TACHOnet central hub;
- Perform, along with national authorities, the test of connection to TACHOnet.

2.1.4. The Registration Authority

Entity: DG JRC.

Role: The registration authority is the entity responsible for verifying the identity of the trusted courier, for registering and approving the requests of issuance, revocation and renewal of digital certificates.

Responsibilities: Acting as registration authority (RA)

- Assign the unique identifier to the requesting organisation.
- Authenticate the identity of the requesting organisation, its contact points and trusted couriers.

Individual Power of Attorney (sample).

- Communicate with the CEF Support regarding the authenticity of requesting organisation, its contact points and trusted couriers.
- Inform the requesting organisation about the approval or rejection of certificate.

2.1.5. CEF Support

Role: CEF PKI Service owner.

Responsibilities:

- Provide for the technical infrastructure for certificate requests by national authorities.
- Validate or reject certificate request.
- Communicate with the registration authority for the identity verification of the requesting organisation, when required.
- Act as the technical single point of contact to the requesting organisation, domain owner, registration authority and provide support for queries related to CEF PKI Services.

2.2. Certificate Issuance Workflow

Purpose: Organisation to obtain PKI certificates for the TACHOnet access points.

Actors:

- Organisation operating the access point (AP);
- Domain Owner;
- CEF Support Team.

Process: This process consists of the following sequential steps:

- **Step 1:** Trusted courier identification
- **Step 2:** Certificate request creation;
- **Step 3**: Registration at RA;
- **Step 4:** Certificate generation;
- **Step 5:** Certificate publication;
- **Step 6:** Certificate acceptance.

The overview of the certificate issuance workflow is shown in the diagram below.

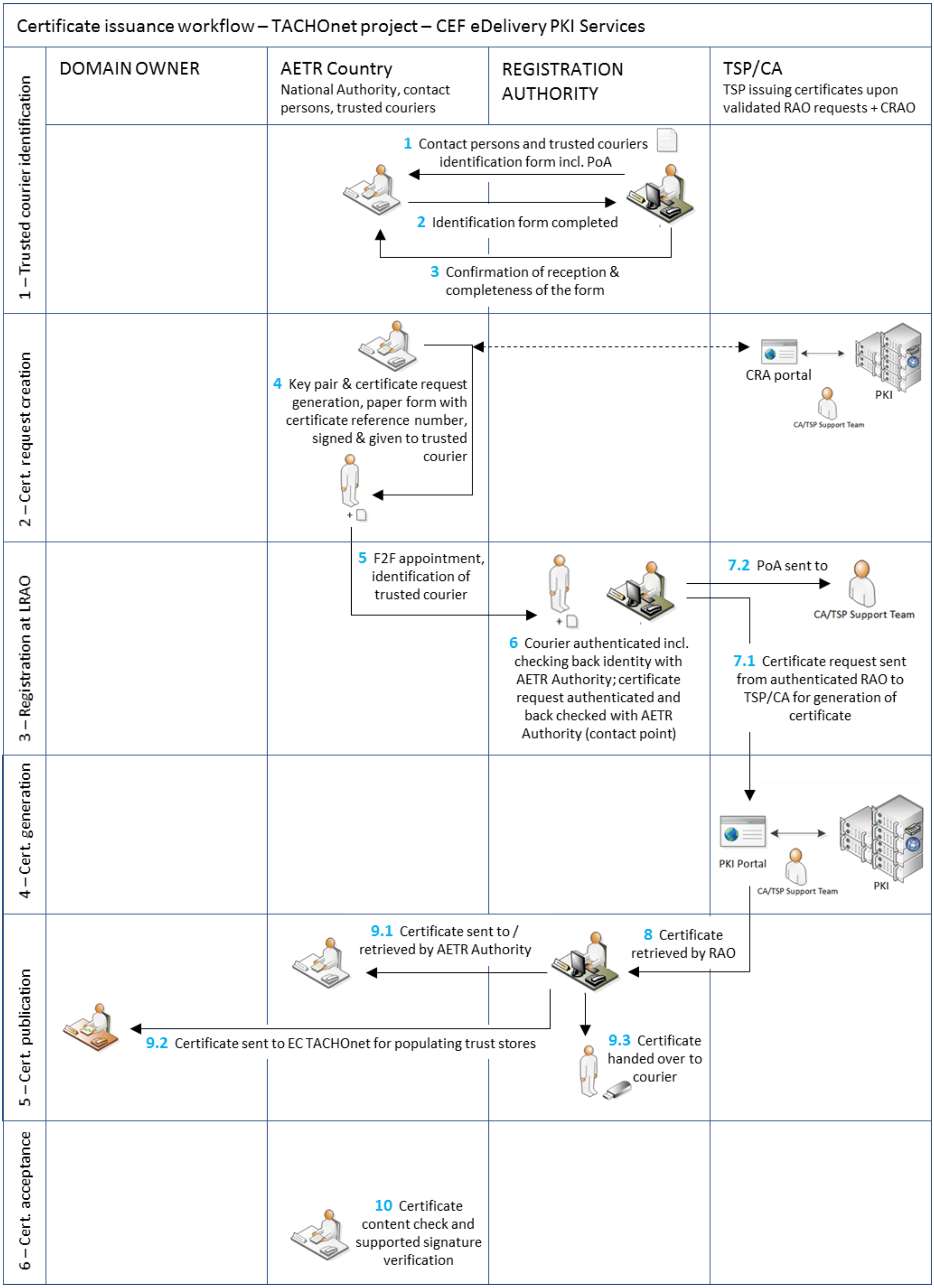

Certificate issuance workflow – TACHOnet project – CEF eDelivery PKI Services
DOMAIN OWNER
AETR Country
National Authority, contact persons, trusted couriers
REGISTRATION AUTHORITY
TSP/CA
TSP issuing certificates upon validated RAO requests + CRAO
1 – Trusted courier identification
1 Contact persons and trusted couriers identification form incl. PoA
2 Identification form completed
3 Confirmation of reception & completeness of the form
2 – Cert. request creation
4 Key pair & certificate request generation, paper form with certificate reference number, signed & given to trusted courier
CRA portal
PKI
CA/TSP Support Team
3 – Registration at LRAO
5 F2F appointment, identification of trusted courier
6 Courier authenticated incl. checking back identity with AETR Authority; certificate request authenticated and back checked with AETR Authority (contact point)
7.2 PoA sent to
CA/TSP Support Team
7.1 Certificate request sent from authenticated RAO to TSP/CA for generation of certificate
4 – Cert. generation
PKI Portal
CA/TSP Support Team
PKI
5 – Cert. publication
9.1 Certificate sent to / retrieved by AETR Authority
8 Certificate retrieved by RAO
9.2 Certificate sent to EC TACHOnet for populating trust stores
9.3 Certificate handed over to courier
6 – Cert. acceptance
10 Certificate content check and supported signature verification

Figure 1 - Certificate issuance workflow

2.2.1. Step 1: Trusted courier identification

Purpose: To enable service providers to submit a request for PKI certificates for APs.

Actors:

- Organisation;
- Domain owner.

Process:

1. RA sends to the national authority the contact persons and trusted couriers' identification form[6]. This form also include a power of attorney (PoA) the organisation (AETR Authority) needs to sign.
2. The national authority sends back the completed form and signed PoA to the RA.
3. The RA acknowledges the good reception and completeness of the form.
4. The RA provides a copy/update of the list of contact persons and trusted couriers to the domain owner.

2.2.2. Step 2: Certificate request creation

> ***Remark**: The request and the retrieval of the certificate have to be done on the same computer and the same browser.*

Purpose: To enable organisations to create a request for PKI certificates for APs and prepare the face-to-face registration file.

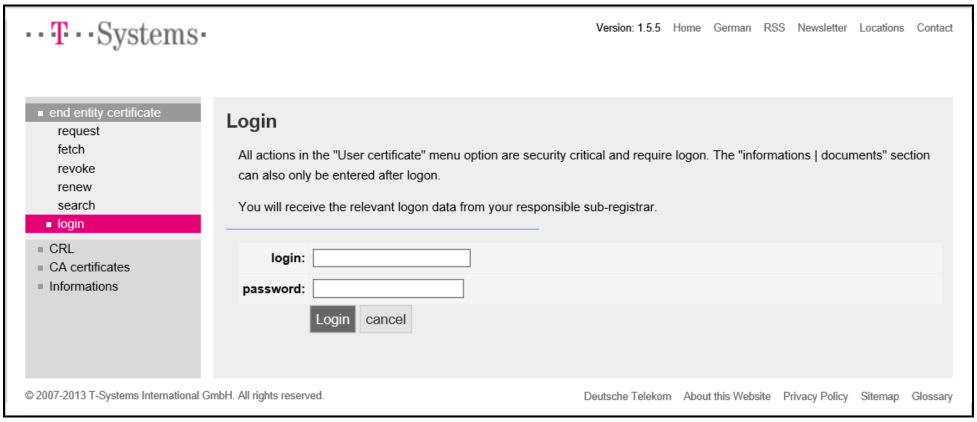
Actors:

- Organisation;
- CEF support team.

Process:

1. An Organisation navigates to the user web interface to request the certificate. The URL is https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en:

[6] See §5.8.



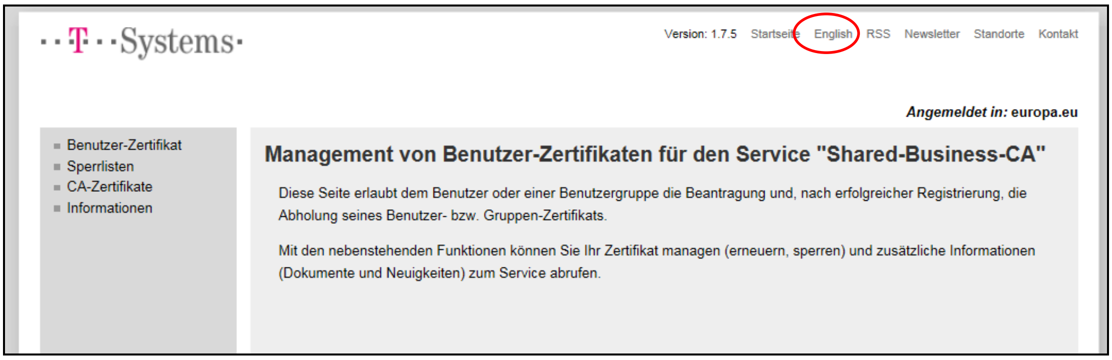
Login

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

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

© 2007-2013 T-Systems International GmbH. All rights reserved.

The username is "**sbca/CEF_eDelivery.europa.eu**" and the password is "**digit.333**"
In case that the language changes to German, click on English to change the page's language.



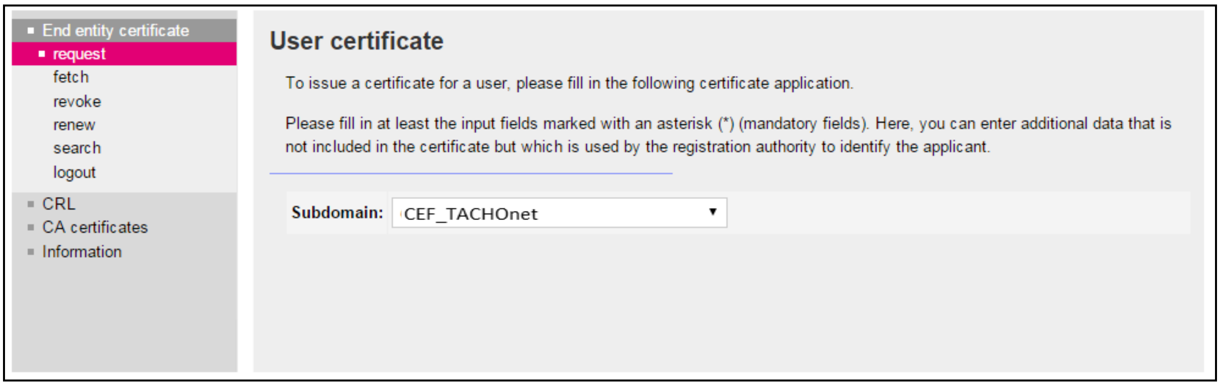
Angemeldet in: europa.eu

Management von Benutzer-Zertifikaten für den Service "Shared-Business-CA"

Diese Seite erlaubt dem Benutzer oder einer Benutzergruppe die Beantragung und, nach erfolgreicher Registrierung, die Abholung seines Benutzer- bzw. Gruppen-Zertifikats.

Mit den nebenstehenden Funktionen können Sie Ihr Zertifikat managen (erneuern, sperren) und zusätzliche Informationen (Dokumente und Neuigkeiten) zum Service abrufen.

2. The Organisation clicks on "request" on the left side of the panel and selects "CEF_TACHOnet” in the dropdown list;



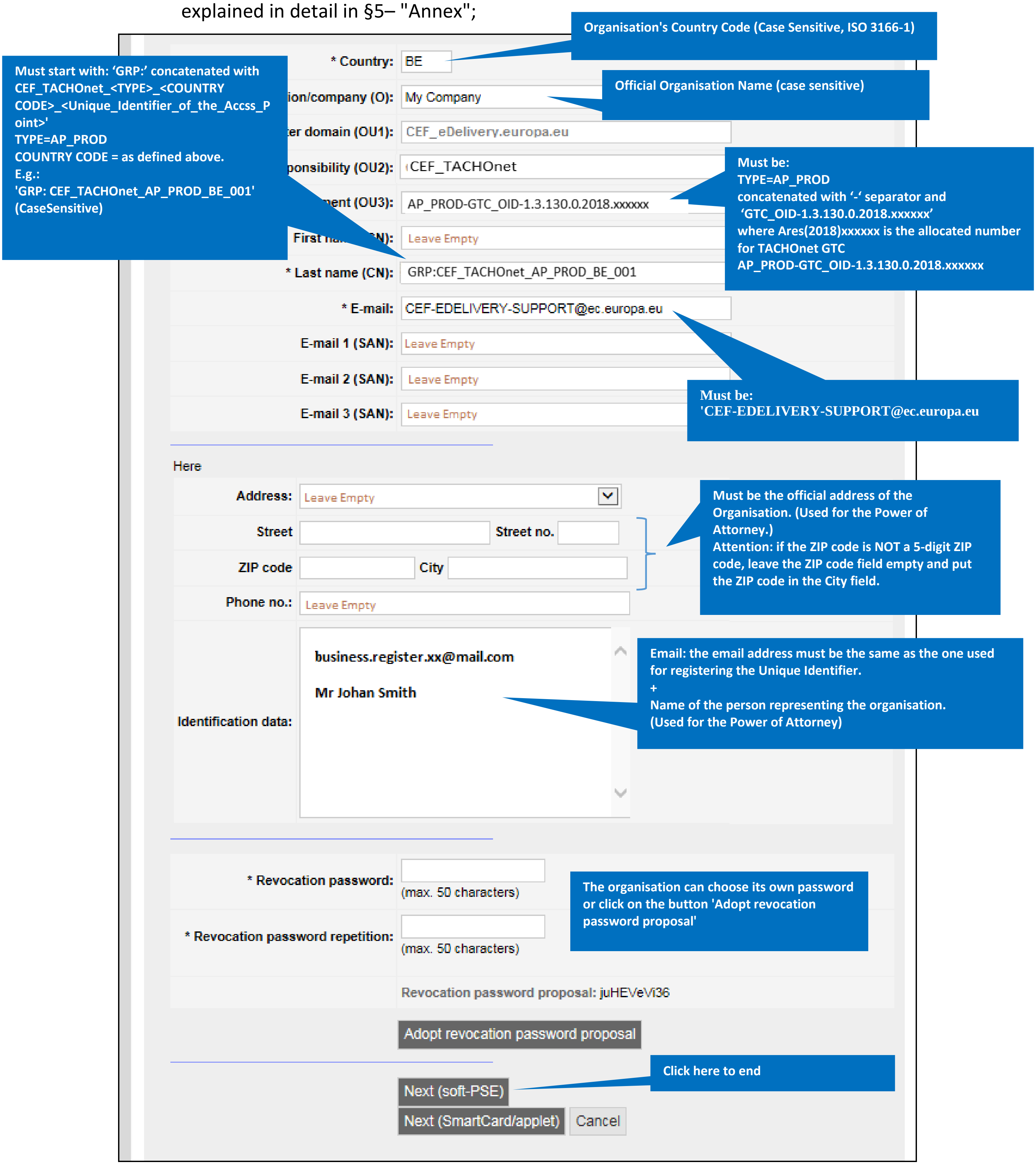
User certificate

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

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

Subdomain: CEF_TACHOnet

3. The Organisation populates the certificate request form as illustrated below and as explained in detail in §5– "Annex";



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

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'
(CaseSensitive)

Official Organisation Name (case sensitive)

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

* Country:	BE
ion/company (O):	My Company
er domain (OU1):	CEF_eDelivery.europa.eu
ponsibility (OU2):	CEF_TACHOnet
ment (OU3):	AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First na (N):	Leave Empty
* Last name (CN):	GRP:CEF_TACHOnet_AP_PROD_BE_001
* E-mail:	CEF-EDELIVERY-SUPPORT@ec.europa.eu
E-mail 1 (SAN):	Leave Empty
E-mail 2 (SAN):	Leave Empty
E-mail 3 (SAN):	Leave Empty

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

Here

Address:	Leave Empty		
Street		Street no.	
ZIP code		City	
Phone no.:	Leave Empty		
Identification data:	business.register.xx@mail.com Mr Johan Smith		

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)

* Revocation password:	(max. 50 characters)
* Revocation password repetition:	(max. 50 characters)
	Revocation password proposal: juHEVeVi36

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

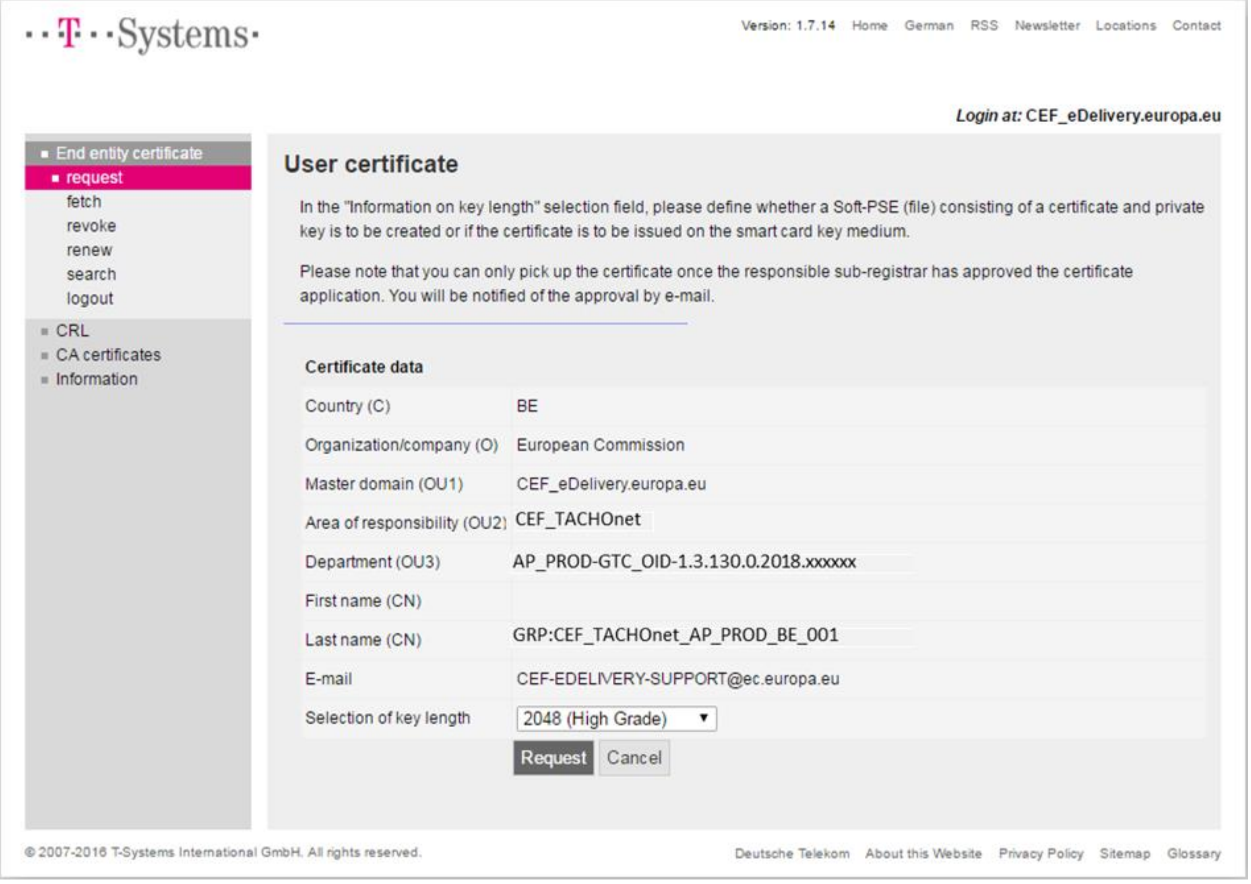
Click here to end

The Organisation must click on 'Next (soft-PSE)'

The complete details of each requested field is shown in the following table:

Requested Fields	Description
Country	**C=Country Code**, location of certificate owner, verified using a public directory; Constraints: 2 characters, in accordance to ISO 3166-1, alpha-2, Case Sensitive; Examples: DE, BE, NL, Specific cases: UK (for Great-Britain), EL (for Greece)
Organisation/Company (O)	**O=Organization name of the certificate owner**
Master domain (OU1)	**OU=CEF_eDelivery.europa.eu**
Area of responsibility (OU2)	**OU=CEF_TACHOnet**
Department (OU3)	Mandatory value per "AREA OF RESPONSIBILITY" The content must be checked using a positive list (white list) when the certificate is requested. If the information does not correspond to the list, the request is prevented. Format: **OU=<TYPE>-<GTC_NUMBER>** Where "<TYPE>" is replaced by AP_PROD: Access Point in Production environment. And where <GTC_NUMBER> is **GTC_OID-1.3.130.0.2018.xxxxxx**, where Ares(2018)xxxxxx is the GTC number for the TACHOnet project. e.g.: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First name (CN)	Must be Empty
Last name (CN)	Must start with "GRP:", followed by a common name. Format: **CN=GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** e.g.: GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail	**E=CEF-EDELIVERY-SUPPORT@ec.europa.eu**
E-mail 1 (SAN)	Must be Empty
E-mail 2 (SAN)	Must be Empty
E-mail 3 (SAN)	Must be Empty
Address	Must be Empty
Street	Must be the official address of the Organisation of the Certificate Owner. (Used for the Power of Attorney.)
Street no.	Must be the official address of the Organisation of the Certificate Owner. (Used for the Power of Attorney.)
Zip Code	Must be the official address of the Organisation of the Certificate Owner. (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.
City	Must be the official address of the Organisation of the Certificate Owner. (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.
Phone no	Must be Empty
Identification data	The email address must be the same as the one used for registering the Unique Identifier. + Must be the name of the person representing the organisation. (Used for the Power of Attorney) + **Commercial Register No** (only mandatory for private organisations) **Entered at the Local Court of** (only required for German and Austrian private organisations)
Revocation password	Mandatory field chosen by the requestor
Revocation password repetition	Mandatory field chosen by the requestor repeated

Selection of key length 2048(High Grade) must be chosen.



· · T · · Systems·
Version: 1.7.14 Home German RSS Newsletter Locations Contact
End entity certificate
request
fetch
revoke
renew
search
logout
CRL
CA certificates
Information
Request
Cancel
Deutsche Telekom About this Website Privacy Policy Sitemap Glossary

Login at: CEF_eDelivery.europa.eu

User certificate

In the "Information on key length" selection field, please define whether a Soft-PSE (file) consisting of a certificate and private key is to be created or if the certificate is to be issued on the smart card key medium.

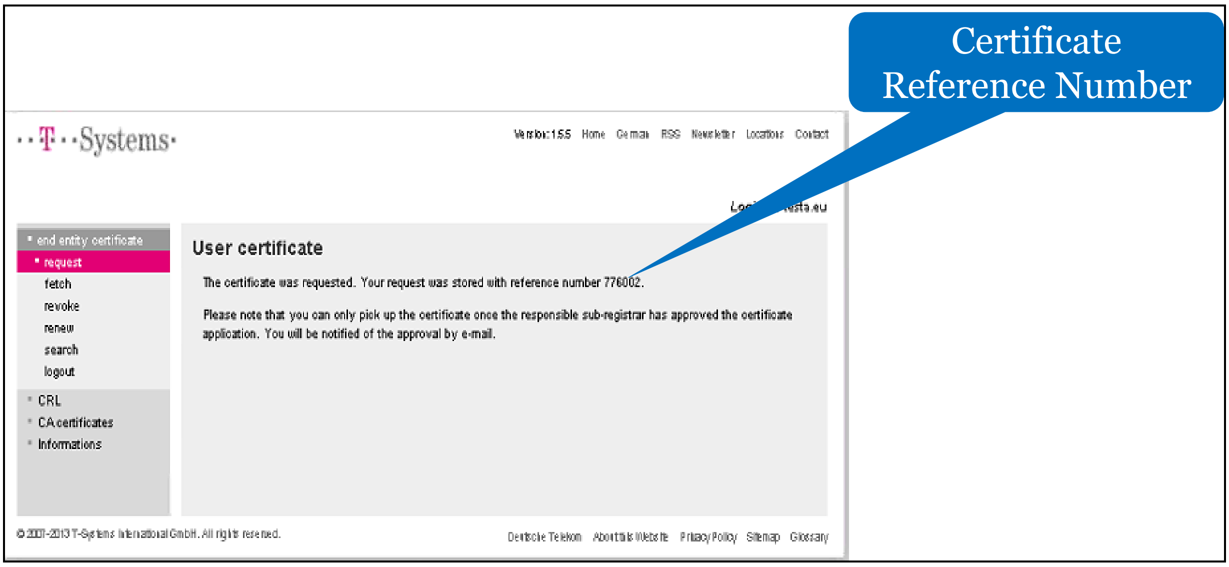
Please note that you can only pick up the certificate once the responsible sub-registrar has approved the certificate application. You will be notified of the approval by e-mail.

Certificate data

Country (C)	BE
Organization/company (O)	European Commission
Master domain (OU1)	CEF_eDelivery.europa.eu
Area of responsibility (OU2)	CEF_TACHOnet
Department (OU3)	AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First name (CN)	
Last name (CN)	GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail	CEF-EDELIVERY-SUPPORT@ec.europa.eu
Selection of key length	2048 (High Grade) ▼

© 2007-2016 T-Systems International GmbH. All rights reserved.

4. **Important**: the Organisation **needs to record** the reference number to retrieve the certificate;



Certificate Reference Number
· · T · · Systems·
Version: 1.5.5 Home German RSS Newsletter Locations Contact
end entity certificate
request
fetch
revoke
renew
search
logout
CRL
CA certificates
Informations
Deutsche Telekom About this Website Privacy Policy Sitemap Glossary

User certificate

The certificate was requested. Your request was stored with reference number 776002.

Please note that you can only pick up the certificate once the responsible sub-registrar has approved the certificate application. You will be notified of the approval by e-mail.

© 2007-2013 T-Systems International GmbH. All rights reserved.

5. CEF Support Team, who operates the sub-RA, checks for new requests of certificates and verifies if the information in the certificate request is valid, i.e. that it conforms to the naming convention specified in the §5.1 - Certificate Naming Convention.

6. CEF Support Team verifies that the information entered in the request is in a valid format.
7. When either check from points (5.) or (6.) above fails, CEF Support Team sends an email to the email address provided in the "Identification data" of the request form, with the Domain Owner in cc, in which the Organisation is requested to start the process again. The failed certificate request is cancelled.
8. CEF Support Team sends an email to <lrao-cert-edelivery@tachonet.eu> to inform the Registration Authority Officer (RAO) about the validity of the request. The email shall include:
    - The name of the requestor (organisation), available in the field "Organisation (O)" of the certificate request;
    - The certificate data (see last screenshot figure in point (3) above) including the name of the AP for which the certificate is to be issued, available in the field "Last Name (CN)" of the certificate request;
    - The certificate reference number;
    - The address of the requestor (organisation), its email and the name of the person representing the organisation.
9. End of the process.

The overview of the Certificate Request process is shown in the diagram below.

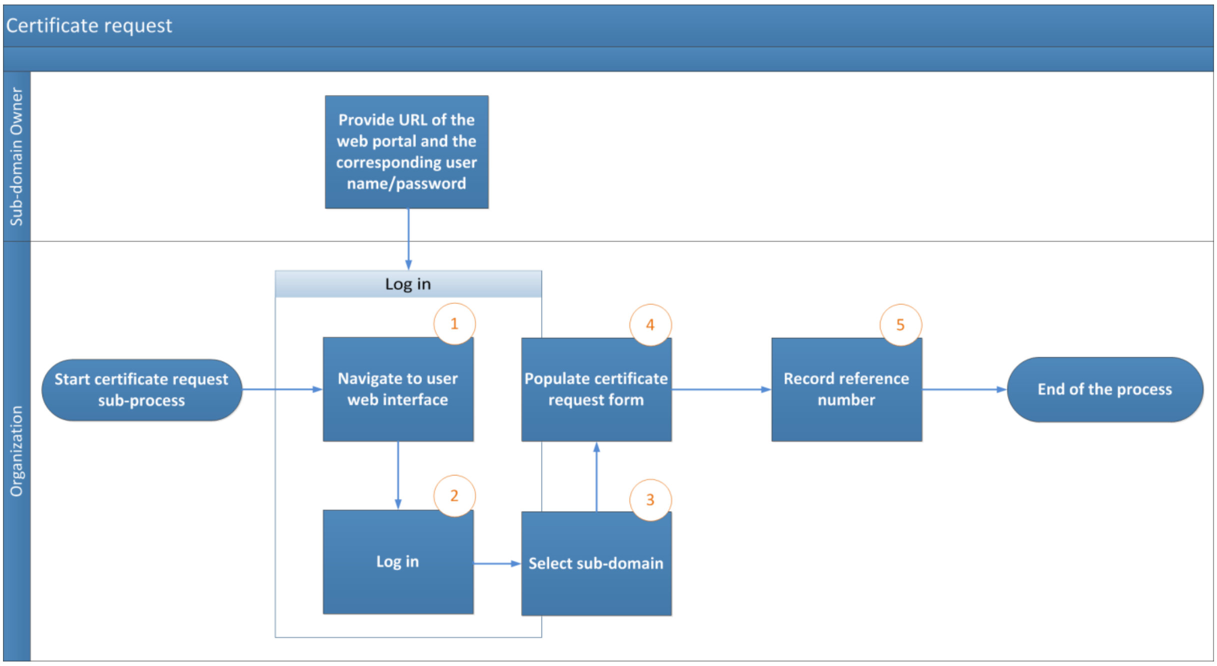

Certificate request
Sub-domain Owner
Organization
Provide URL of the web portal and the corresponding user name/password
Log in
Start certificate request sub-process
1
Navigate to user web interface
2
Log in
3
Select sub-domain
4
Populate certificate request form
5
Record reference number
End of the process

Figure 2 – Certificate request

2.2.3. Step 3: Registration at RAO (Certificate approval)

Purpose: Ensure that the certificate requestor is authorized to get the certificates in a given sub-domain.

Actors:

- CEF Support Team;
- Registration Authority Officers - RAO;
- Organisation (AETR Authority, trusted courier, contact point)

Process:

1. The trusted courier or contact point makes an appointment with the RAO via email exchange identifying the trusted courier who will proceed to the face-to-face (Organisation email: as per trusted courier identification form – step 1; Domain RAO email: <lrao-cert-edelivery@tachonet.eu>).

2. The Organisation prepares the face-to-face documentary package consisting in:

    a. The filled-in and signed power of attorney (see §5.9);

    b. A copy of the valid passport of the trusted courier who will perform the face-to-face. This copy must be signed by one of the step 1 identified Organisation points of contact;

    c. The certificate request paper form (see § 5.10) signed by one of the Organisation points of contact.

3. The RAO receptions the trusted courier after identity screening at the building reception. The RAO conduct the face-to-face registration of the certificate request by:

    a. Identifying and authenticating the trusted courier:

        i. Verifying the trusted courier physical appearance against the passport presented by the trusted courier;

        ii. Verifying the validity of the passport presented by the trusted courier;

        iii. Verifying the validated passport presented by the trusted courier against the copy of the valid passport of the trusted courier signed by one of the step 1 identified Organisation points of contact. Signature is authenticated against the original "trusted courier and contact points identification form";

    b. Verifying the filled-in and signed power of attorney;

    c. Verifying certificate request paper form and its signature against the original "trusted courier and contact points identification form";

    d. Calling the signatory contact point to double check the identity of the trusted courier and the content of the certificate request.

4. The RAO confirms to the CEF Support Team that the certificate requestor is indeed authorized to operate the components for which it is asking the certificates and that the corresponding face-to-face registration process was successful. The confirmation must be sent using a "CommiSign" certificate secure email with as attachments a scanned copy of the authenticated face-to-face documentary package and of the signed RAO process check list (see §5.11).
5. If the RAO confirms the validity of the request, the process continues; If not (5b), the certificate issuance is rejected and the Organisation informed;
6. CEF Support Team approves the certificate request.
7. CEF Support Team notifies the RAO of the approval of the certificate.
8. The RAO notifies the Organisation that the certificate can be retrieved via the user portal. The RAO hands over a copy of the certificate to the trusted courier.
9. End of the process.

The overview of the certificate approval process is shown in the diagram below.

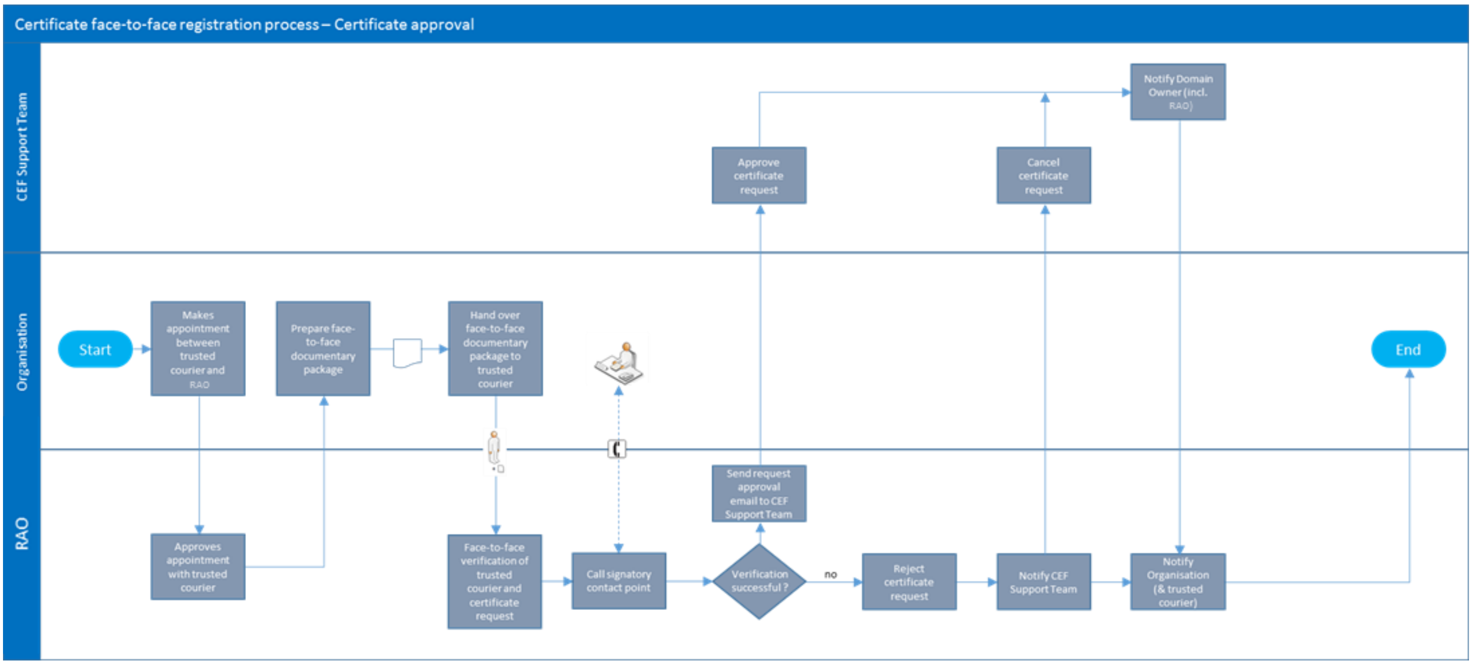

Certificate face-to-face registration process – Certificate approval
CEF Support Team
Organisation
RAO
Start
Makes appointment between trusted courier and RAO
Prepare face-to-face documentary package
Hand over face-to-face documentary package to trusted courier
Approves appointment with trusted courier
Face-to-face verification of trusted courier and certificate request
Call signatory contact point
Verification successful ?
no
Send request approval email to CEF Support Team
Approve certificate request
Reject certificate request
Notify CEF Support Team
Cancel certificate request
Notify Domain Owner (incl. RAO)
Notify Organisation (& trusted courier)
End

Figure 2 - Certificate approval

2.2.4. Step 3: Certificate generation

Purpose: Generation of the requested certificate.

Actors:

- CEF Support Team;

Process:

1. Upon approval of the certificate request, the certificate is generated.

2.2.5. Step 4: Certificate publication & retrieval

Purpose: Distribute and/or download the certificate for AP.

Actors:

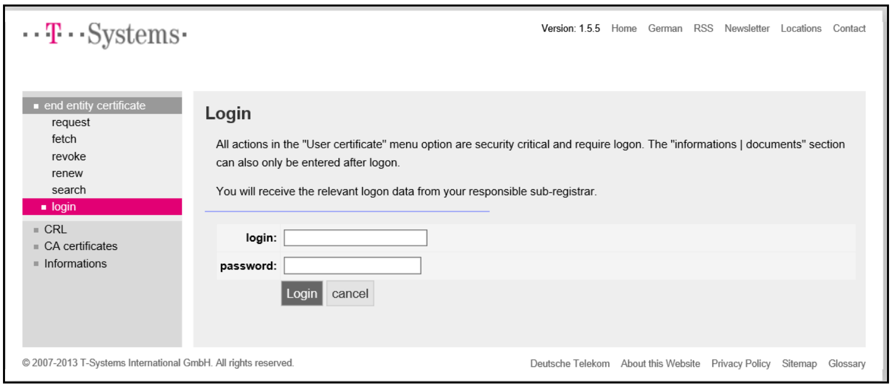
- CEF Support Team;
- Domain Owner;
- RAO;
- Organisation (AETR Authority, trusted courier, contact point)

Process:

1. Following approval of the certificate request, the RAO may retrieve the certificate and hand over a copy to the trusted courier.

2. An Organisation receives the notification from Domain Owner or from the RAO that the certificates can be retrieved;

    a. An Organisation navigates to the user portal and logs in. The URL is https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en:



Login

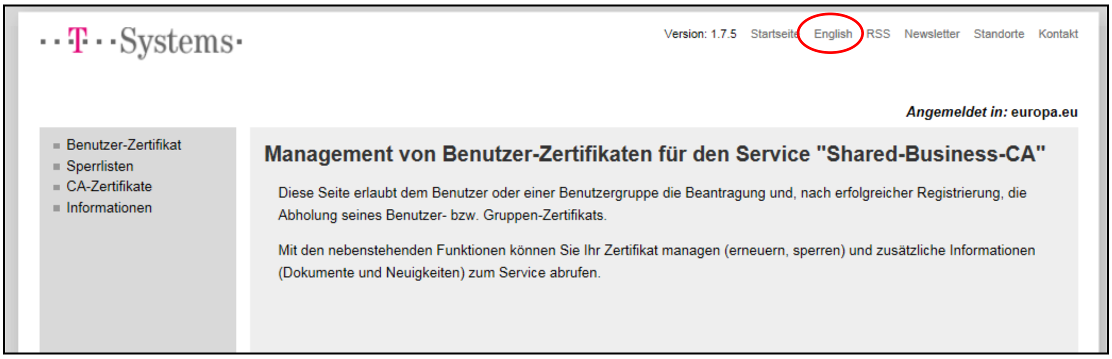
All actions in the "User certificate" menu option are security critical and require logon. The "informations | documents" section can also only be entered after logon.

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

© 2007-2013 T-Systems International GmbH. All rights reserved.

The username is "**sbca/CEF_eDelivery.europa.eu**" and the password is "**digit.333**"

In case that the language changes to German, click on English to change the page's language.



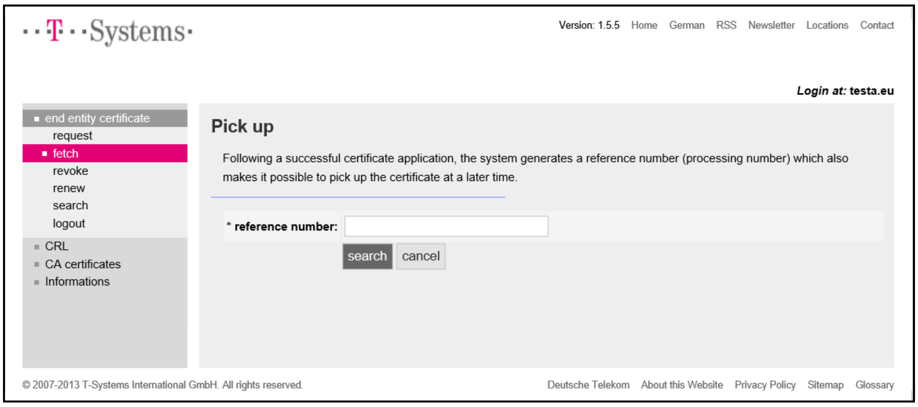
Angemeldet in: **europa.eu**

Management von Benutzer-Zertifikaten für den Service "Shared-Business-CA"

Diese Seite erlaubt dem Benutzer oder einer Benutzergruppe die Beantragung und, nach erfolgreicher Registrierung, die Abholung seines Benutzer- bzw. Gruppen-Zertifikats.

Mit den nebenstehenden Funktionen können Sie Ihr Zertifikat managen (erneuern, sperren) und zusätzliche Informationen (Dokumente und Neuigkeiten) zum Service abrufen.

b. An Organisation clicks on the "fetch" button on the left-hand side and provides the reference number recorded during the certificate request process;



Login at: **testa.eu**

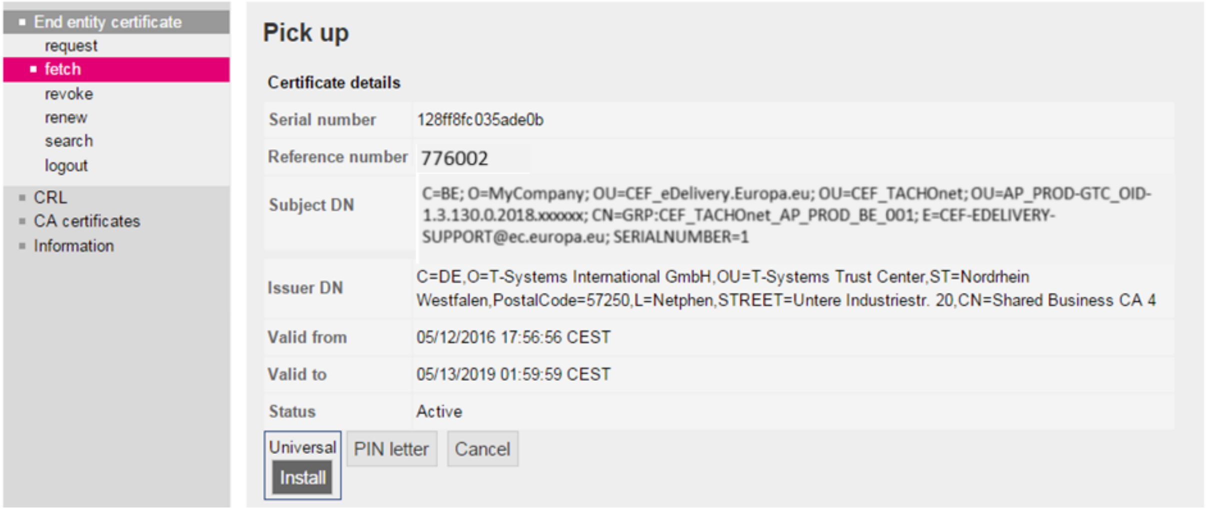
Pick up

Following a successful certificate application, the system generates a reference number (processing number) which also makes it possible to pick up the certificate at a later time.

*** reference number:**

© 2007-2013 T-Systems International GmbH. All rights reserved.

c. The requestor installs certificates by clicking on the install button;



Pick up

Certificate details

Serial number	128ff8fc035ade0b
Reference number	776002
Subject DN	C=BE; O=MyCompany; OU=CEF_eDelivery.Europa.eu; OU=CEF_TACHOnet; OU=AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx; CN=GRP:CEF_TACHOnet_AP_PROD_BE_001; E=CEF-EDELIVERY-SUPPORT@ec.europa.eu; SERIALNUMBER=1
Issuer DN	C=DE,O=T-Systems International GmbH,OU=T-Systems Trust Center,ST=Nordrhein Westfalen,PostalCode=57250,L=Netphen,STREET=Untere Industriestr. 20,CN=Shared Business CA 4
Valid from	05/12/2016 17:56:56 CEST
Valid to	05/13/2019 01:59:59 CEST
Status	Active

d. End of the process, the certificate is now installed in the repository used by your current browser.

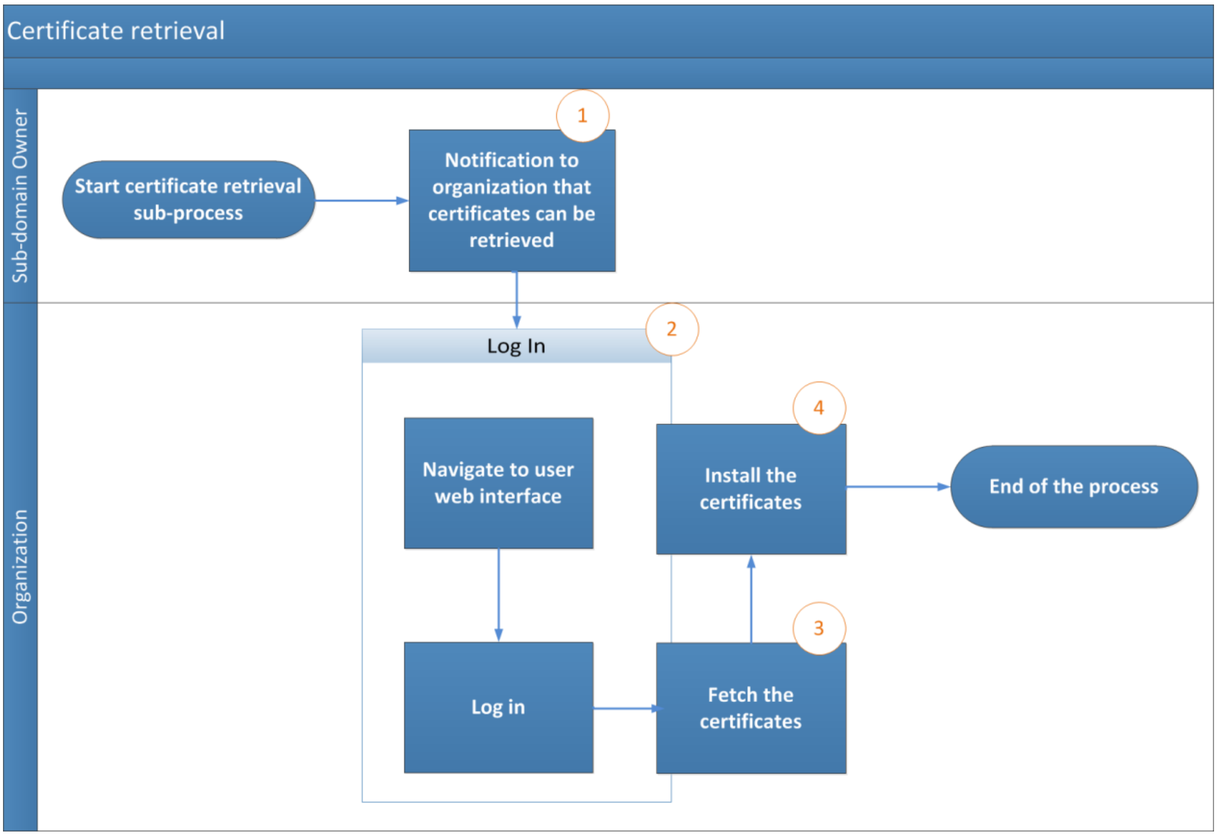
The certificate needs now to be installed on the Access Point. As this is implementation-specific, the Organisation needs to refer to its Access Point provider to obtain the description of this process.

The following steps are needed for the certificate installation on the Access Point:

1. Export the private key and the certificate,
2. Create the keystore and the truststore,
3. Install the keystore and the truststore on the access point.

More information can be found in §5 – "Annex".

The overview of the certificate retrieval process by the Organisation is shown in the diagram below.



Certificate retrieval
Sub-domain Owner
Organization
Start certificate retrieval sub-process
1
Notification to organization that certificates can be retrieved
2
Log In
Navigate to user web interface
Log in
3
Fetch the certificates
4
Install the certificates
End of the process

Figure 3 - Certificate retrieval

3. CERTIFICATE REVOCATION PROCESS

Purpose: Revoke a certificate for the AP.

Actors:

- Organization;
- CEF eDelivery Sub-domain Owner;
- RAO;
- CEF Support Team.

Process:

1. An Organization, a CEF eDelivery sub-domain owner (including an RAO of that or on behalf of that CEF eDelivery sub-domain owner), submits a revocation request through the user web portal;

2. The sub-RA operated by the CEF Support Team executes the certificate revocation.

The overview of the revocation of a service provider process is shown in the diagram below.

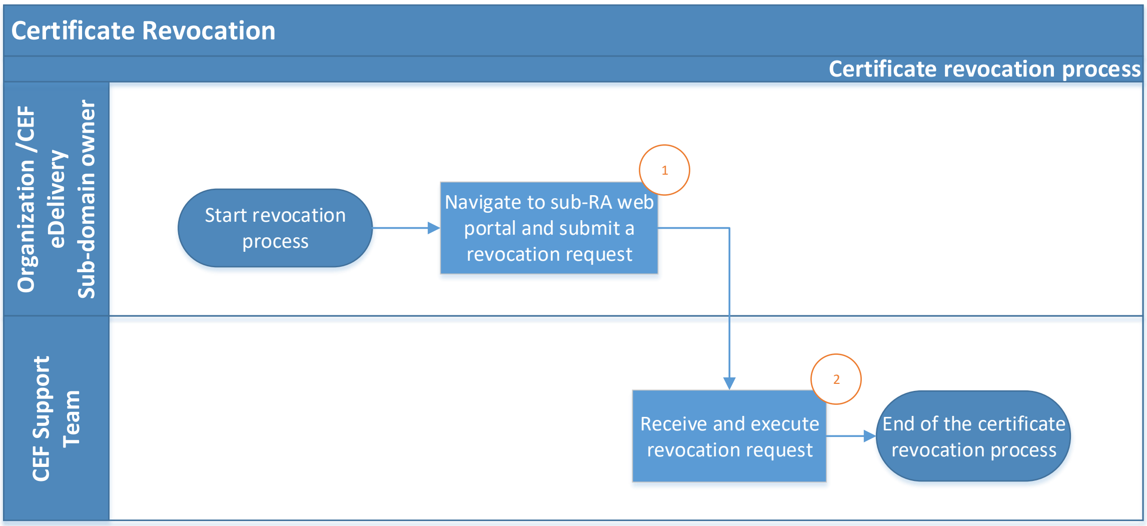

Certificate Revocation
Certificate revocation process
Organization /CEF eDelivery Sub-domain owner
CEF Support Team
Start revocation process
Navigate to sub-RA web portal and submit a revocation request
1
Receive and execute revocation request
2
End of the certificate revocation process

Figure 4 - Certificate revocation

4. GLOSSARY

The key terms used in this Component Offering Description are defined in the CEF Definitions section on the CEF Digital Single Web Portal:

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

The key acronyms used in this Component Offering Description are defined in the CEF Glossary on the CEF Digital Single Web Portal:

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

5. Annexes

5.1. Certificate Naming Convention

This annex contains the information that supports proper understanding and execution of the processes described in §2 – "CERTIFICATE REQUEST PROCESS".

In order to achieve separation per area of responsibility, the CEF eDelivery PKI service uses the naming convention in the certificate metadata.

In particular, the naming assignment listed below must be used when requesting **end-entity user certificates**. Permitted characters for the fields are **a-z A-Z 0-9, ' ( ) + , . / : = ? -**.

1. **Country Code (C)**
   - *Description*: originating country of the service provider.
   - *Constraints: 2 characters, in accordance to ISO 3166-1, alpha-2, Case Sensitive;*
   - *Examples: DE, BE, NL.*
2. **Name of the Organisation (O)**
   - *Description: contains the name of the Organisation authorized to operate APs;*
   - *It is a legal entity approved by the corresponding eDelivery sub-owner;*
   - *Constraints: must be the **name of the service provider (the requestor – see §2.1 Roles and Responsibilities) organisation as it appears in official registers** (Case sensitive).*
   - *Example: Corp_A.*
3. **Master Domain/client (OU1)**
   - *Description: name of the master domain.*
   - *Constraints: has a fixed value*: **"CEF_eDelivery.europa.eu"**
4. **Area of Responsibility (OU2)**
   - *Description: the business sub-domain in which CEF eDelivery is used.*
   - *Constraints: has a fixed value*: **"CEF_TACHOnet"**.
5. **Department (OU3)**
   - *Description: identifier of the access point and the environment (test, production, acceptance);*
     1. *Format: OU=<TYPE>-<GTC_NUMBER>*
        ➔ *where "<TYPE>" is replaced by AP_PROD, access point in production => AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx*
        ➔ *where <GTC_NUMBER> is: "GTC_OID-1.3.130.0.2018.xxxxxx", where Ares(2018)xxxxxx is the number of the GTC signed by TACHOnet.*
6. **First Name:** must be left empty;
7. **Last Name (CN):**
   - *Description:* a unique identifier of the subject to which the certificate is issued*;*

- *Constraints:*
    1. Maximum 64 characters;
    2. Must be "GRP:" concatenated with a common name with the following format: <CEF_TACHOnet>_<TYPE>_<COUNTRY CODE>_<UNIQUE ID>

       where <**TYPE>** is AP_PROD, Access Point in production and UNIQUE ID is a unique identifier.

       Examples: GRP: CEF_TACHOnet_AP_PROD_BE_001
    3. Case Sensitive.

8. **Email Address:** Must contain CEF-EDELIVERY-SUPPORT@ec.europa.eu, case sensitive;
9. **E-mail 1, e-mail 2, e-mail 3:** must be left empty.
10. **Address**: must be left empty.
11. **Street, Street no., ZIP code & City**: 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, put the ZIP code in the City field and leave the ZIP code field empty.
12. **Phone no**.: must be left empty.
13. **Identification data**:
    - **Email address:** the email address must be the same as the one used for registering the Unique Identifier
    - **Name of the person representing the organisation**
    - **Mandatory only for private organisations: Commercial Register No**
    - **Mandatory only for private organisations in Austria or Germany: Entered at the Local Court of**

Please note that the email address needs to be identical to the one used to register the SubmitterID for TACHOnet. The email will be checked and if the same email is not provided, the certificate request will be refused. By relying on the certificate naming convention described above, the certificate validation process is implemented to ensure that only inter-sub-domain certificates are trusted.

5.2. The certificate validation process

The certificate validation is implemented by each CEF eDelivery component and is part of the CEF eDelivery source code.

All the certificates trusted by the CEF eDelivery component AP are listed in its local trust store. The certificate validation process therefore verifies if the certificate is listed in the local trust store of the verifying component and if the certificate itself is valid, e.g. authentic, not revoked and not expired. The process is described in the diagram and the supporting table below.

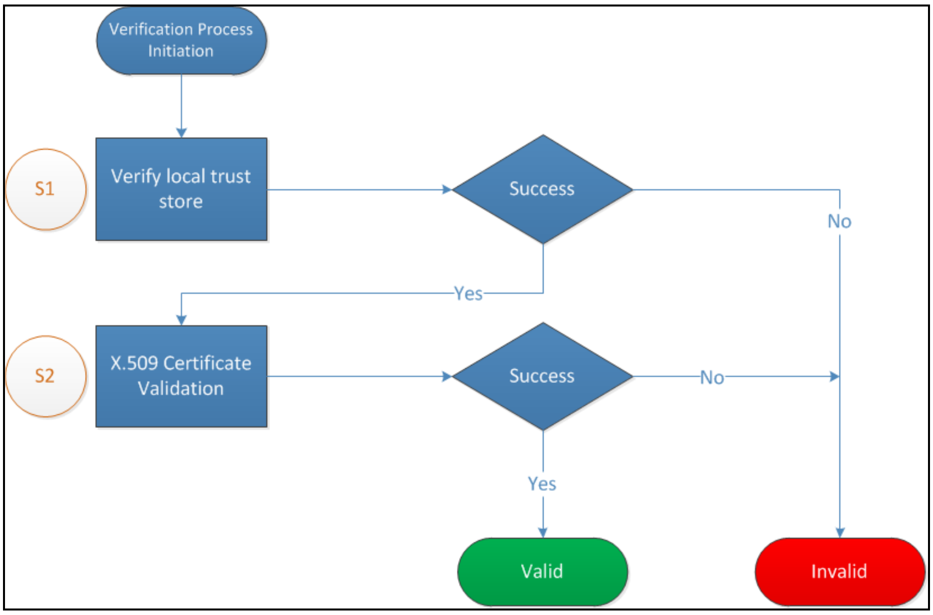


Figure 5 - Certificate validation in the CEF eDelivery PKI

The diagram in Figure 5 is further explained in the table below.

S1: Verify local trust store	The verifying component first checks if the certificate is in its local trust store.
S2: X.509 Certificate Validation	As T-Systems publishes a directory from where the issued certificates can be retrieved, it can be leveraged to keep the trust stores up-to-date. The directory services support LDAP communication protocol. The standard certificate validation in accordance to the ETSI standard[7] that includes the verification of the expiration date, revocation status, and sub-CA signature on the certificate.

Table 1 - Certificate Validation Steps

Remark:

> *As the certificates for all the domains are issued by the same sub-CA, the certificate policy is the same for all the sub-domains. This means that the algorithms and key lengths are fixed. The keys are 2048 bits long and the signature algorithm is SHA256RSA.*

[7] https://www.etsi.org/deliver/etsi_ts/102800_102899/102853/01.01.02_60/ts_102853v010102p.pdf

5.3. Private Key

The export of the private key depends on how your Internet Browser manages the certificates.

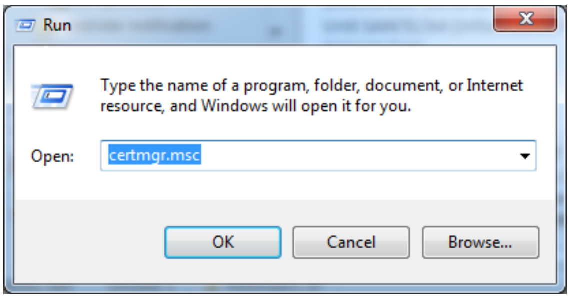
In this annex, we propose 2 procedures:

- On Microsoft Windows (Windows 10 is not yet supported) browser which don't have own certificate repository but uses the Windows one.
- On any OS for Mozilla Firefox users.

5.3.1. Private Key: Export for Windows users

After the installation of the PKI certificate, you can export your private key. Follow the steps below:

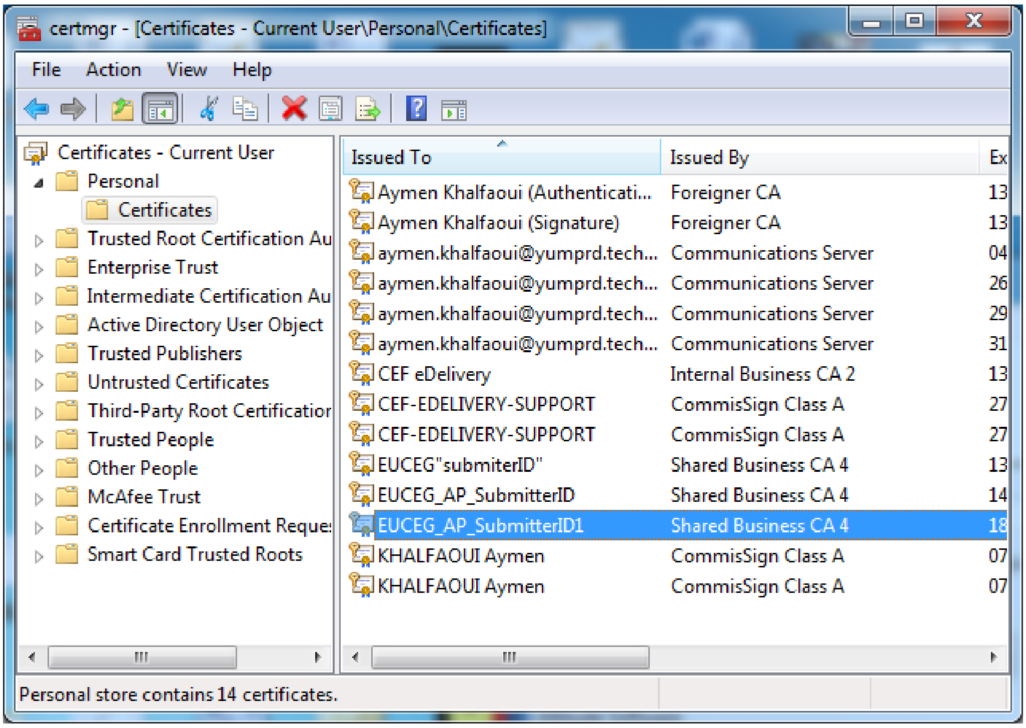
1- Run **certmgr.msc**



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: certmgr.msc

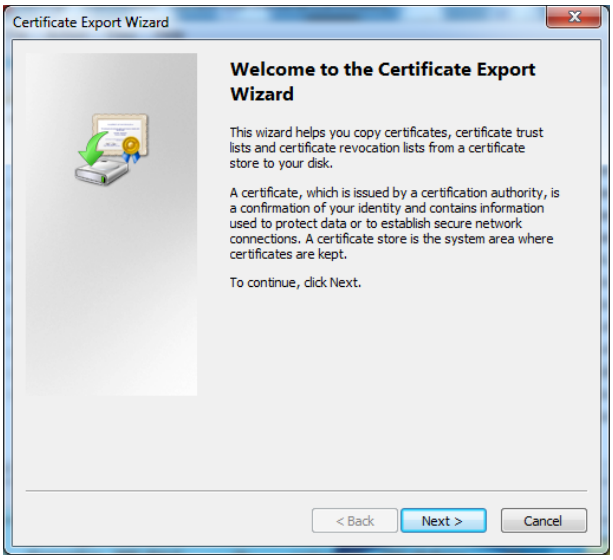
2- Open Personal certificates and choose the one that you want to export (example below):


certmgr - [Certificates - Current User\Personal\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification Au
Enterprise Trust
Intermediate Certification Au
Active Directory User Object
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificatior
Trusted People
Other People
McAfee Trust
Certificate Enrollment Reque:
Smart Card Trusted Roots

Issued To	Issued By	Ex
Aymen Khalfaoui (Authenticati...	Foreigner CA	13
Aymen Khalfaoui (Signature)	Foreigner CA	13
aymen.khalfaoui@yumprd.tech...	Communications Server	04
aymen.khalfaoui@yumprd.tech...	Communications Server	26
aymen.khalfaoui@yumprd.tech...	Communications Server	29
aymen.khalfaoui@yumprd.tech...	Communications Server	31
CEF eDelivery	Internal Business CA 2	13
CEF-EDELIVERY-SUPPORT	CommisSign Class A	27
CEF-EDELIVERY-SUPPORT	CommisSign Class A	27
EUCEG"submiterID"	Shared Business CA 4	13
EUCEG_AP_SubmitterID	Shared Business CA 4	14
EUCEG_AP_SubmitterID1	Shared Business CA 4	18
KHALFAOUI Aymen	CommisSign Class A	07
KHALFAOUI Aymen	CommisSign Class A	07

Personal store contains 14 certificates.

3- Right click on the "certificate > All tasks > Export"



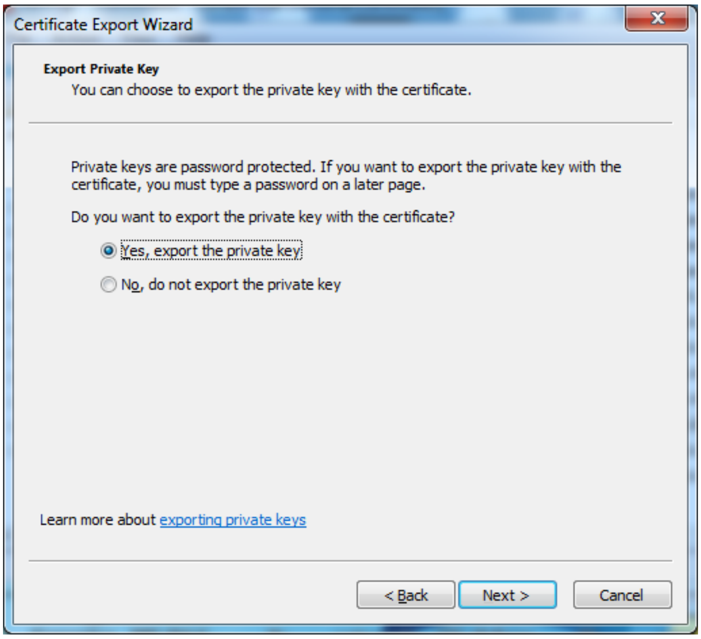
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

4- Select yes, export the private key



Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

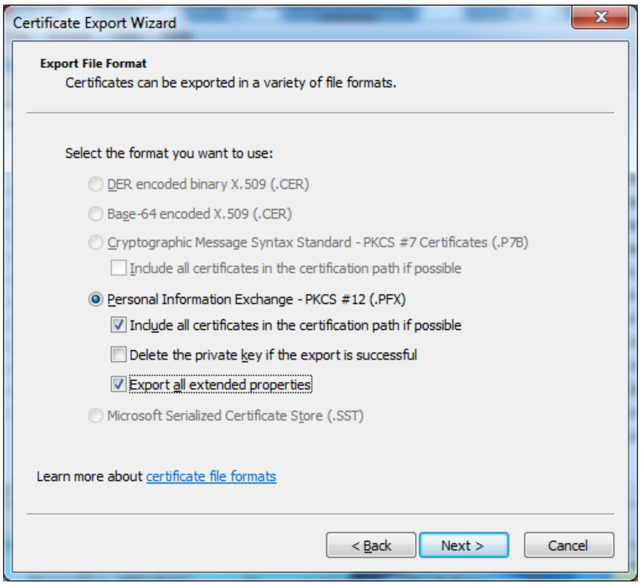
Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

Learn more about exporting private keys

5- Select both **include all certificates…** and **Export all….** As shown below



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

☑ Include all certificates in the certification path if possible

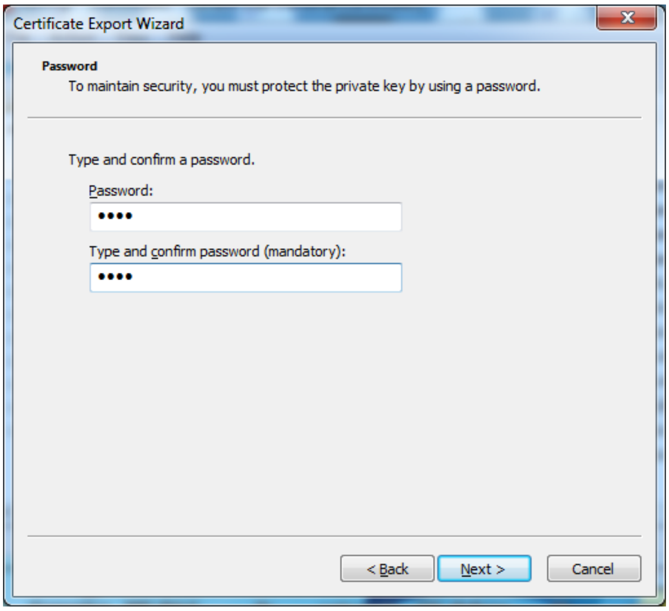
□ Delete the private key if the export is successful

☑ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

6- Set a password



Certificate Export Wizard

Password

To maintain security, you must protect the private key by using a password.

Type and confirm a password.

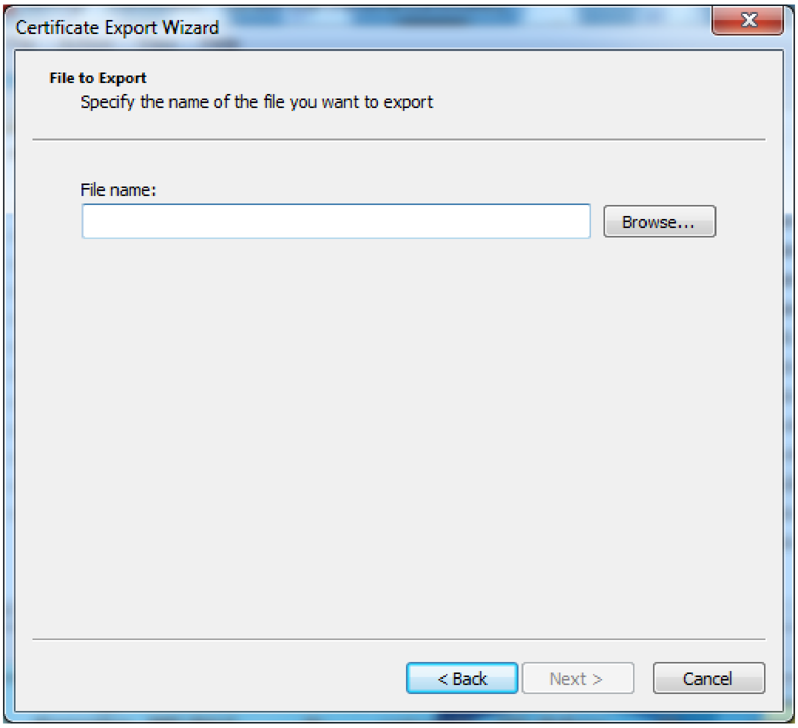
Password:

●●●●

Type and confirm password (mandatory):

●●●●

7- Choose where to export it



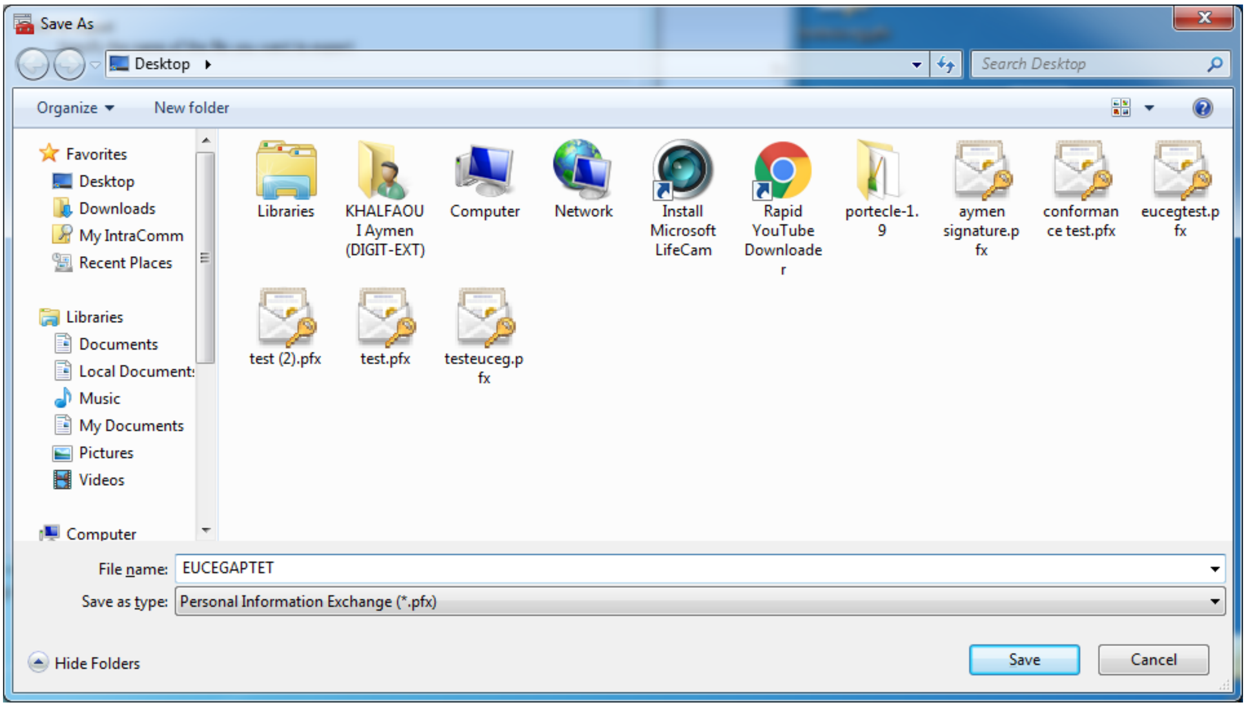
Certificate Export Wizard

File to Export

Specify the name of the file you want to export

File name:

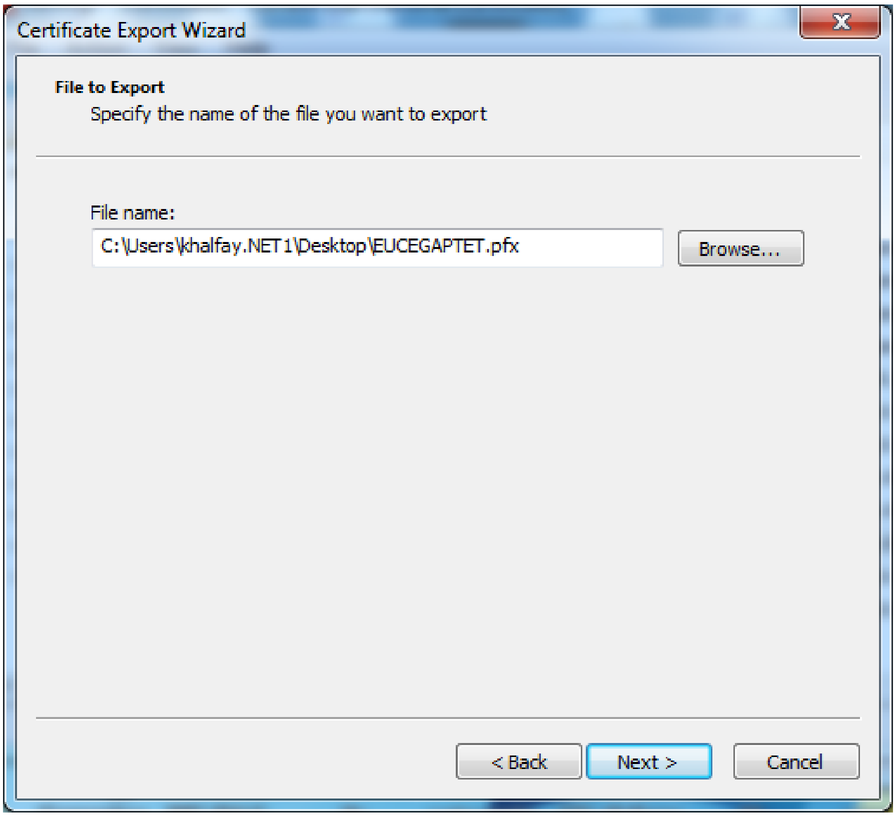
8- Choose a name:



File name: EUCEGAPTET

Save as type: Personal Information Exchange (*.pfx)

9- Click on **Next**:



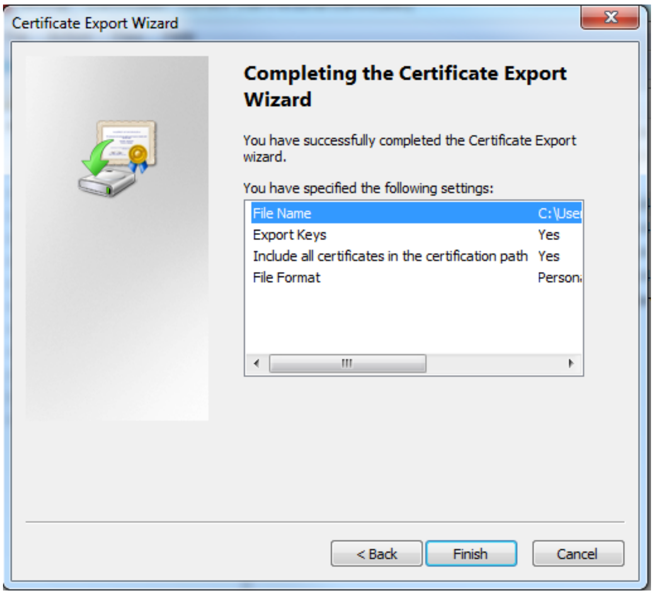
File to Export

Specify the name of the file you want to export

File name:

C:\Users\khalfay.NET1\Desktop\EUCEGAPTET.pfx

10- Click on **Finish**:

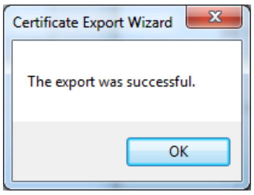


Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Use
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Person

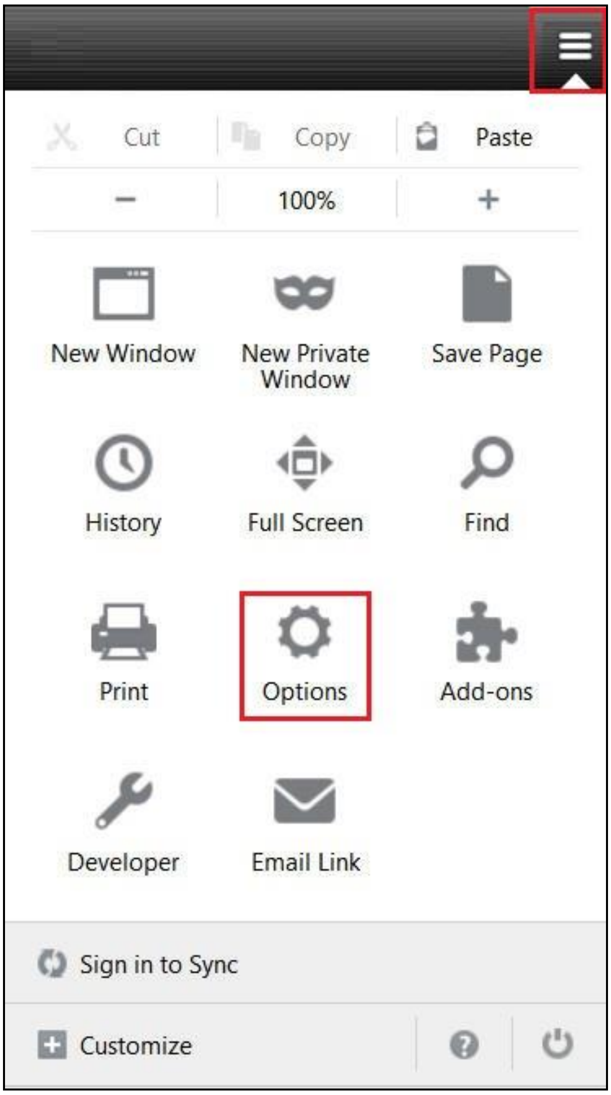


The export was successful.

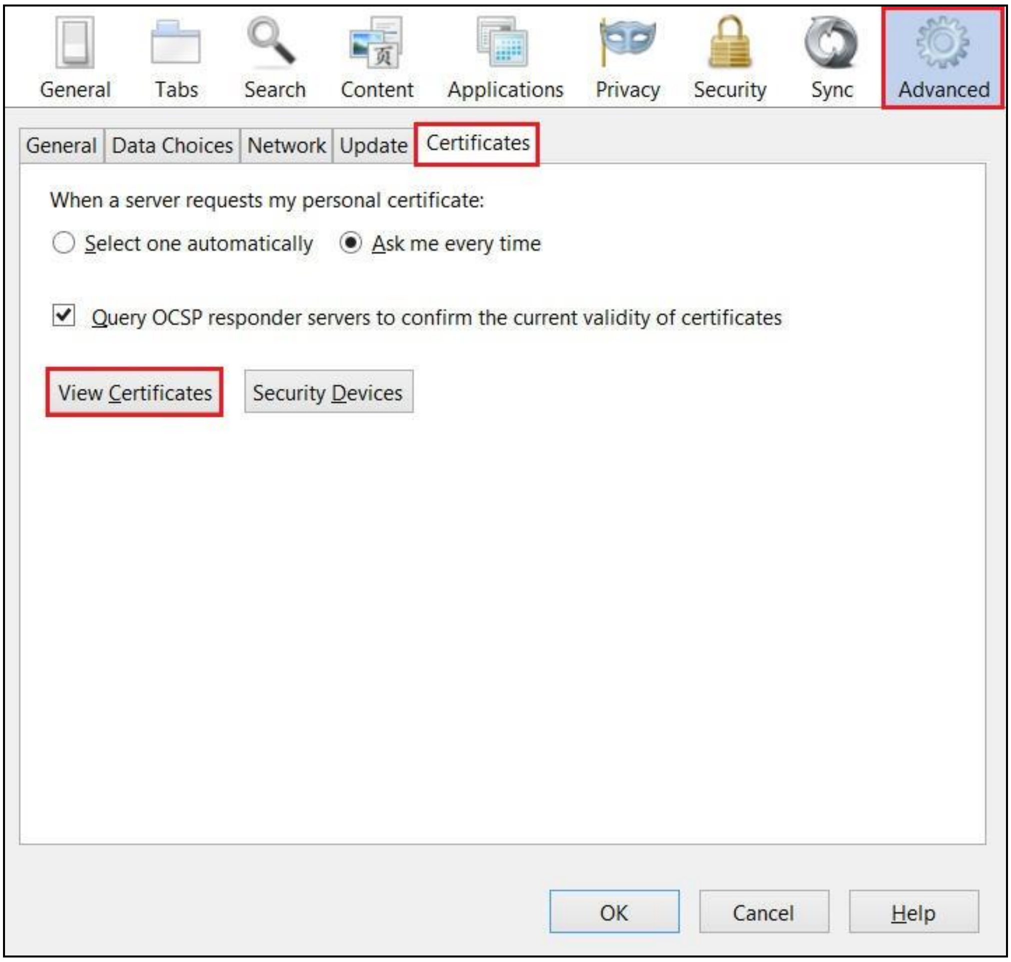
5.3.2. Private Key: Export for Mozilla Firefox users

Mozilla Firefox uses its own Certificate Repository and a specific procedure to extract the private key. These are different steps to execute:

1. In Firefox, go to **Options**.



2. In the **Options** window, click **Advanced**, next, click the **Certificates** tab, and then, click **View Certificates**.

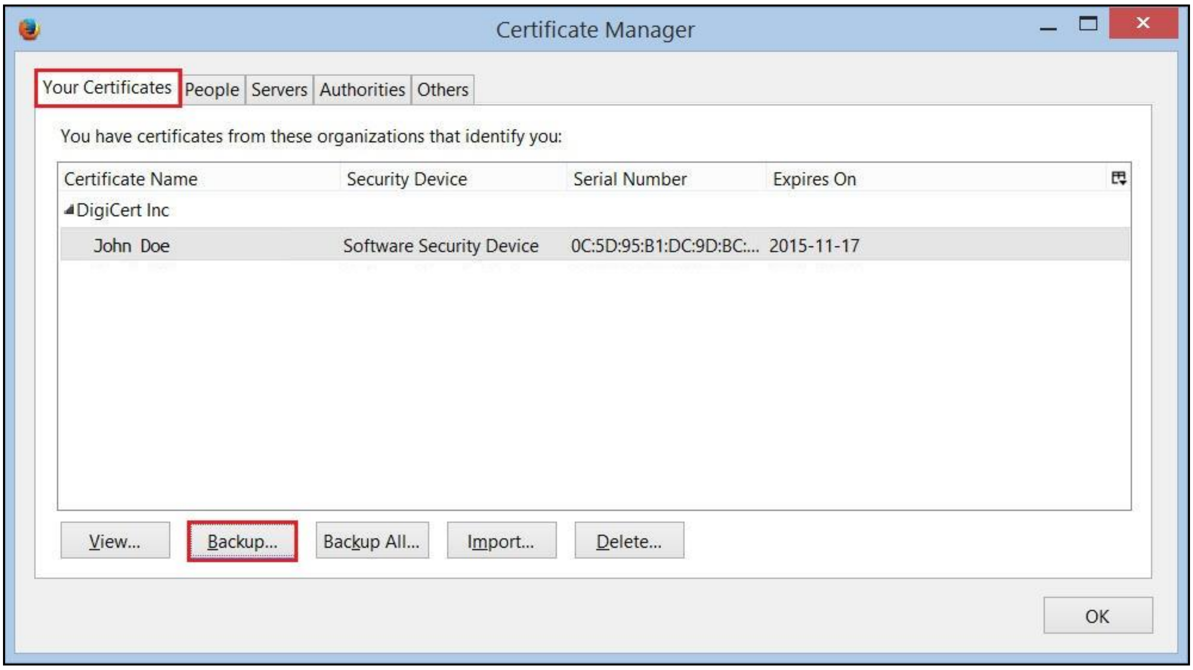


When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

☑ Query OCSP responder servers to confirm the current validity of certificates

3. In the **Certificate Manager** window, on the **Your Certificates** tab, select your code signing certificate which contains your private key you want to export and then, click **Backup**.



You have certificates from these organizations that identify you:

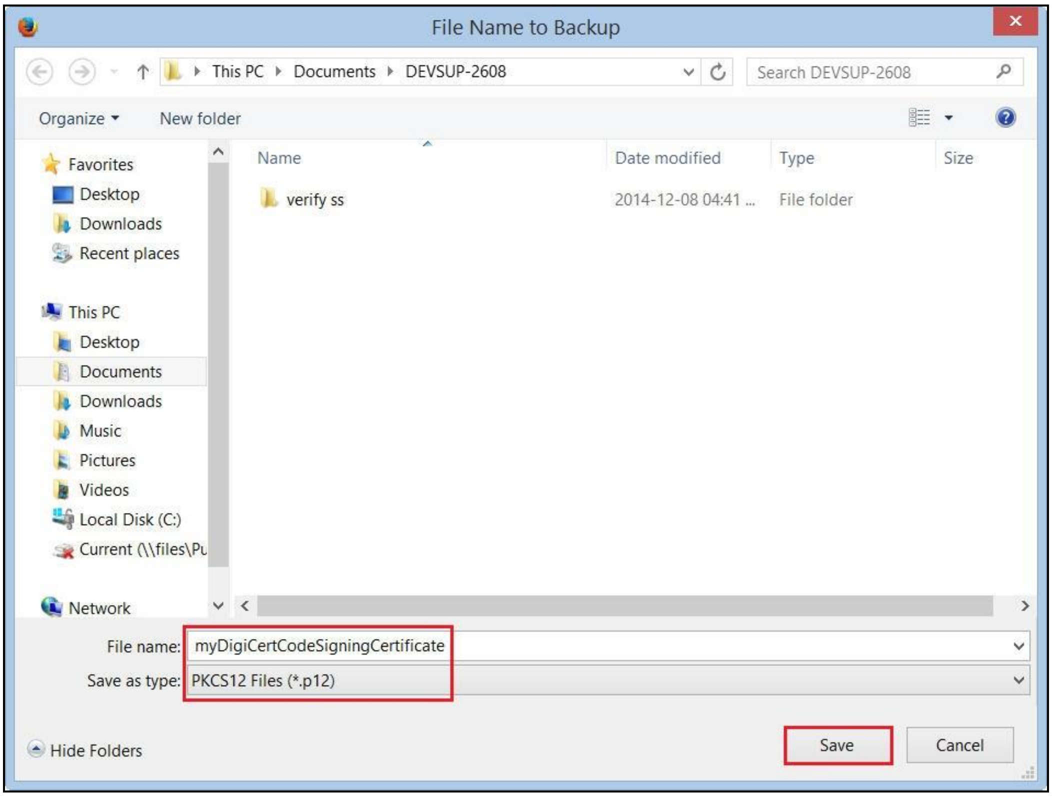
Certificate Name	Security Device	Serial Number	Expires On
◢DigiCert Inc			
John Doe	Software Security Device	0C:5D:95:B1:DC:9D:BC:...	2015-11-17

4. In the **File Name to Backup** window, go to where you want to save your private key (w/private key) .p12 file, provide a file name (i.e.*myCodeSigningCertificate*), and then click **Save**.

Make sure to save the .p12 file in a location that you will remember and to which you have permissions.

Remark:

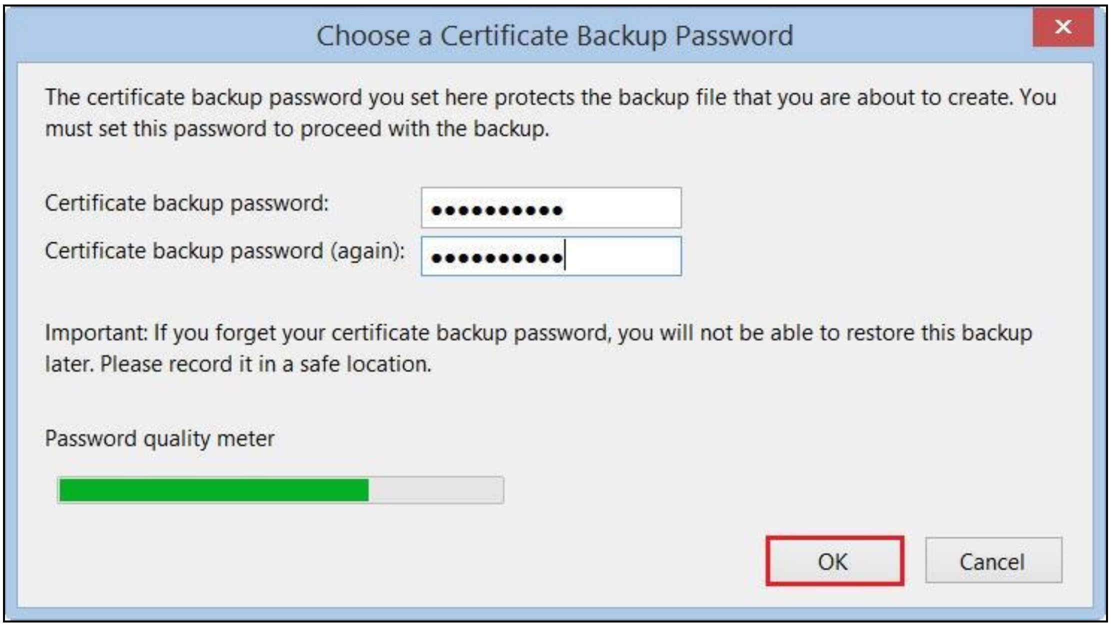
*A **.p12** file uses the same format as a **.pfx** or a **PKCS12** file.*



File name: myDigiCertCodeSigningCertificate

Save as type: PKCS12 Files (*.p12)

5. In the **Choose a Certificate Backup Password** window, create a **Certificate backup password** and then, click **OK**.



Choose a Certificate Backup Password

The certificate backup password you set here protects the backup file that you are about to create. You must set this password to proceed with the backup.

Certificate backup password: ●●●●●●●●●●●

Certificate backup password (again): ●●●●●●●●●●●

Important: If you forget your certificate backup password, you will not be able to restore this backup later. Please record it in a safe location.

Password quality meter

6. When you receive the *"Successfully backed up your security certificate(s) and private key(s)"* message, click **OK**

5.4. Public Key (certificate)

The export of the public key (certificate) depends on how your Internet Browser manages the certificates.

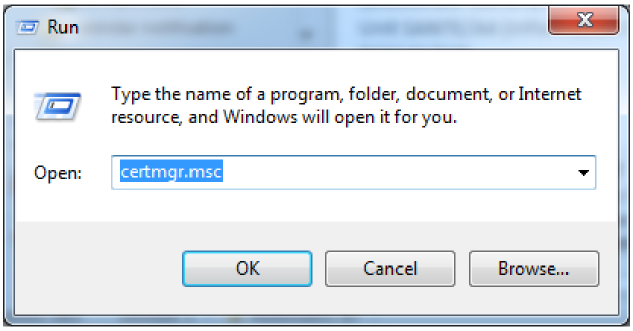
In this annex, we propose 2 procedures:

- On Microsoft Windows (Windows 10 is not yet supported) for any Internet browser which don't have own certificate repository but uses the Windows one;
- On any OS for Mozilla Firefox user.

5.4.1. Public Key (certificate): Export for Windows users

The Trust store contains the Public Keys (certificates) of the other parties (ADRs).

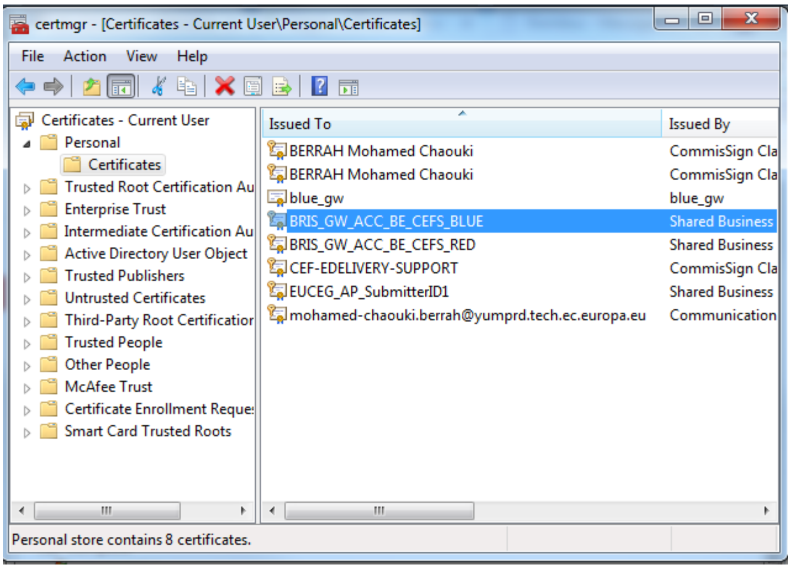
1. Run **certmgr.msc**



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: certmgr.msc

2. Open Personal certificates and choose the one that you want to export (example below):

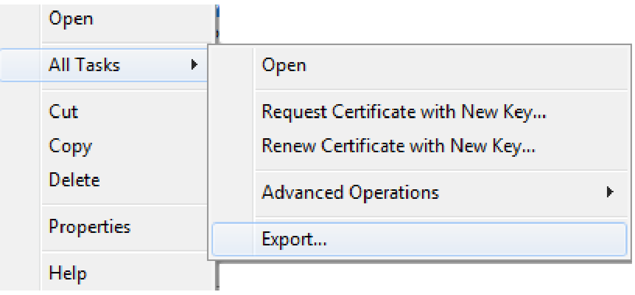

certmgr - [Certificates - Current User\Personal\Certificates]
File
Action
View
Help

Certificates - Current User
- Personal
  - Certificates
- Trusted Root Certification Au
- Enterprise Trust
- Intermediate Certification Au
- Active Directory User Object
- Trusted Publishers
- Untrusted Certificates
- Third-Party Root Certificatior
- Trusted People
- Other People
- McAfee Trust
- Certificate Enrollment Reque:
- Smart Card Trusted Roots

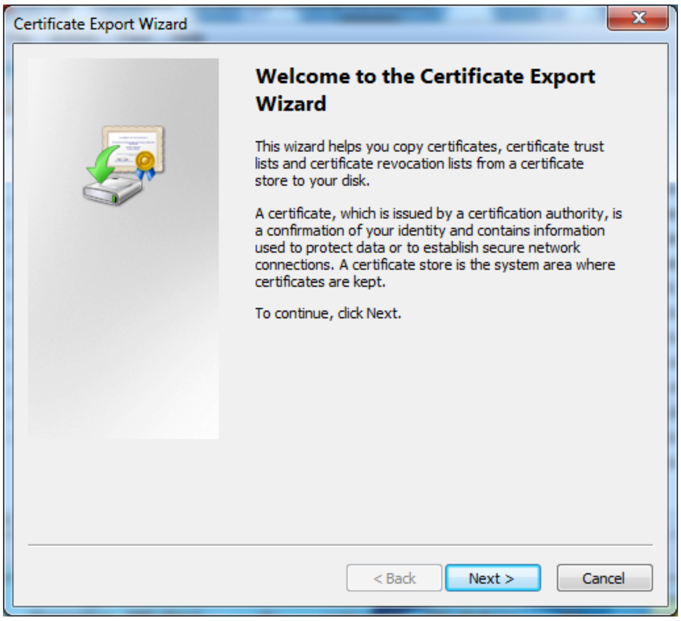
Issued To	Issued By
BERRAH Mohamed Chaouki	CommisSign Cla
BERRAH Mohamed Chaouki	CommisSign Cla
blue_gw	blue_gw
BRIS_GW_ACC_BE_CEFS_BLUE	Shared Business
BRIS_GW_ACC_BE_CEFS_RED	Shared Business
CEF-EDELIVERY-SUPPORT	CommisSign Cla
EUCEG_AP_SubmitterID1	Shared Business
mohamed-chaouki.berrah@yumprd.tech.ec.europa.eu	Communication

Personal store contains 8 certificates.

3. Right click on the "certificate > All tasks > Export"



4. Click on **Next**



Certificate Export Wizard

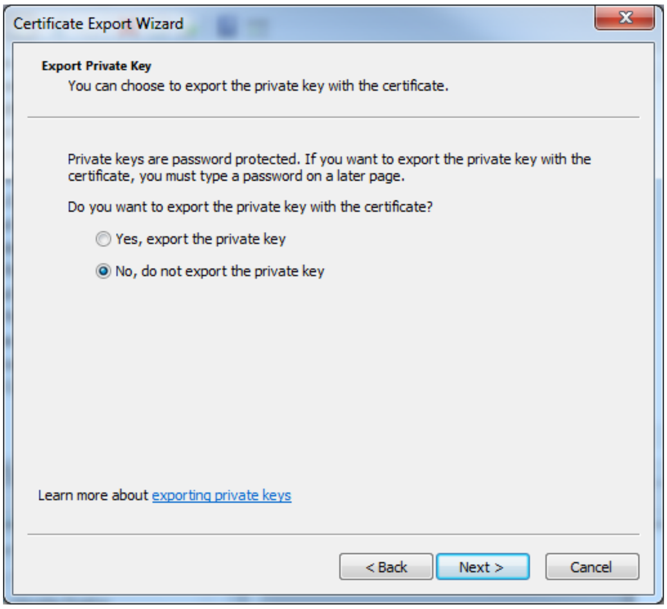
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

5. Select **No, do not export the private key** then click **Next**



Certificate Export Wizard

Export Private Key

You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

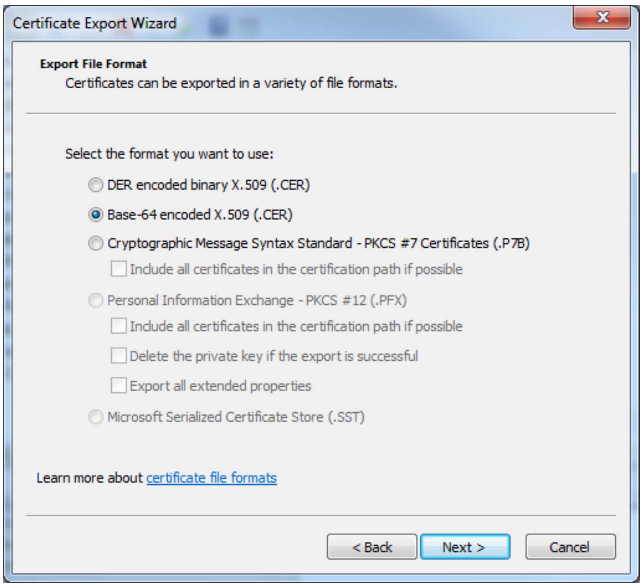
Do you want to export the private key with the certificate?

○ Yes, export the private key

● No, do not export the private key

Learn more about exporting private keys

6. Select **Base-64 encoded X.509 (.CER)** then click **Next**



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

● Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

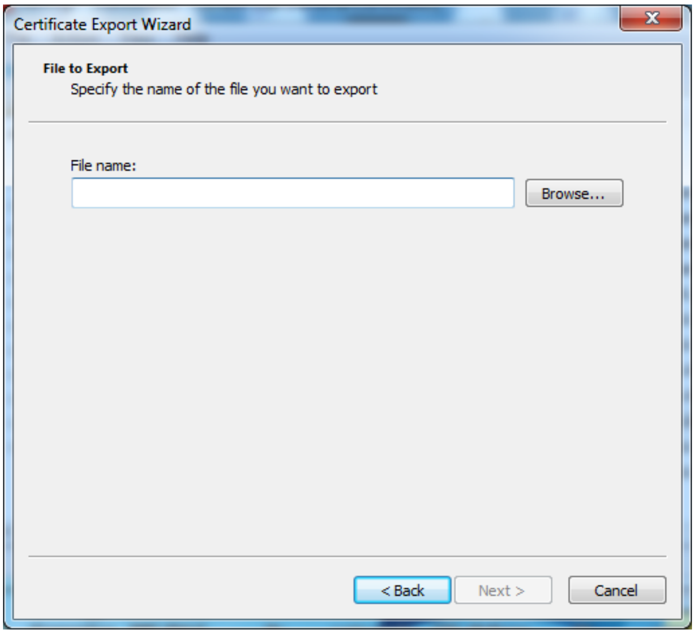
□ Delete the private key if the export is successful

□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

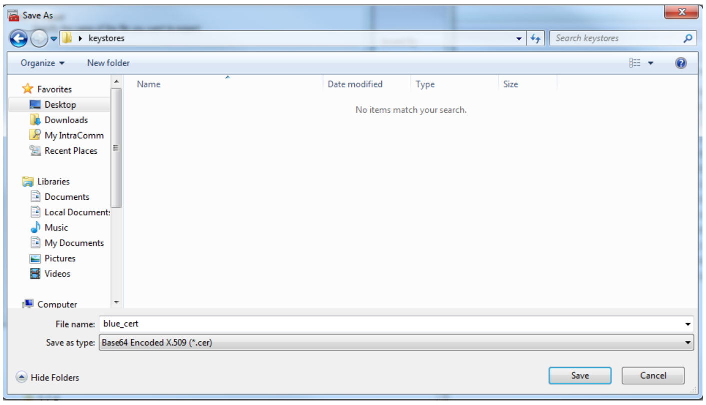
7. Choose where to export it:



Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name:

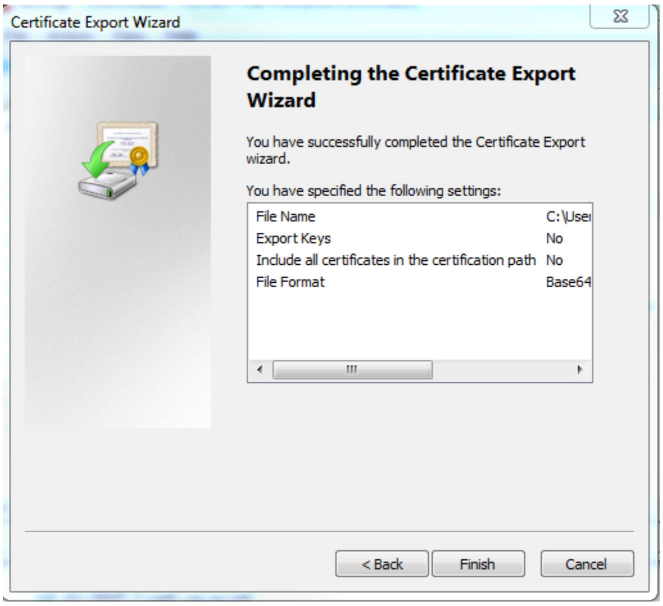


Save As

No items match your search.

File name: blue_cert

Save as type: Base64 Encoded X.509 (*.cer)



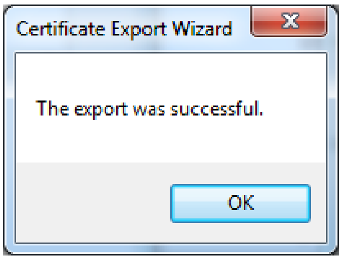
Certificate Export Wizard

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\User
Export Keys	No
Include all certificates in the certification path	No
File Format	Base64



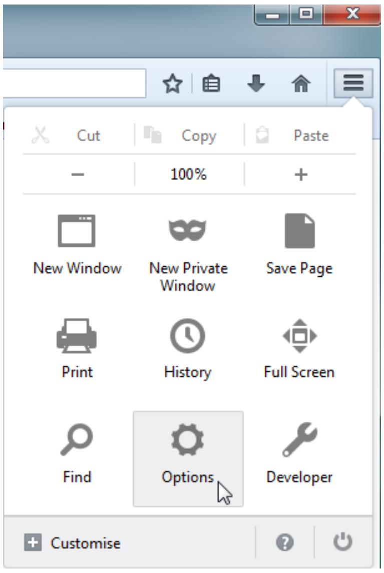
Certificate Export Wizard

The export was successful.

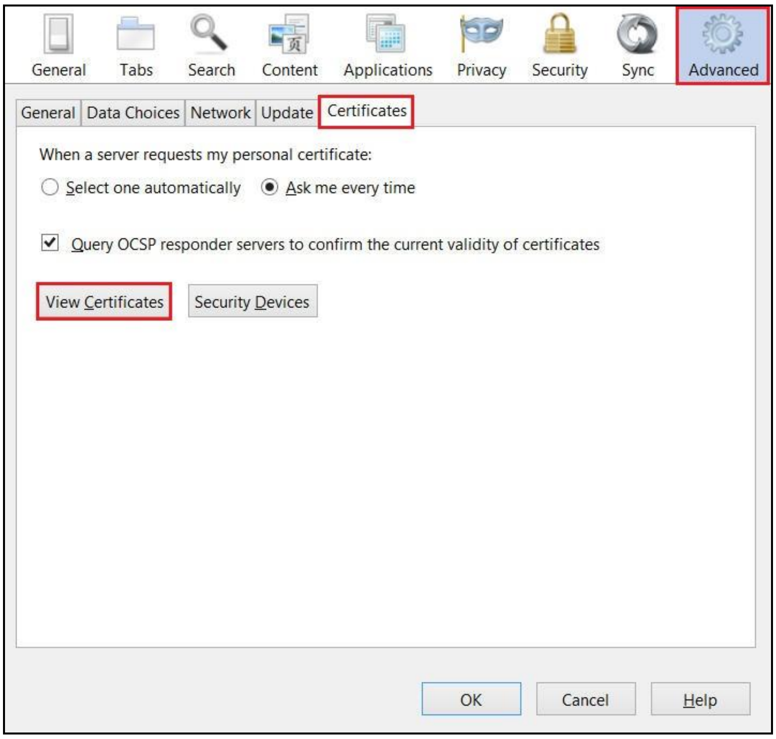
5.4.2. Public Key (certificate): Export for Mozilla Firefox users

Mozilla Firefox uses its own Certificate Repository and a specific procedure to extract the public key (certificate). These are the different steps to execute:

1. In Firefox, go to **Options**.



2. In the **Options** window, click **Advanced**, next, click the **Certificates** tab and then, click **View Certificates**.

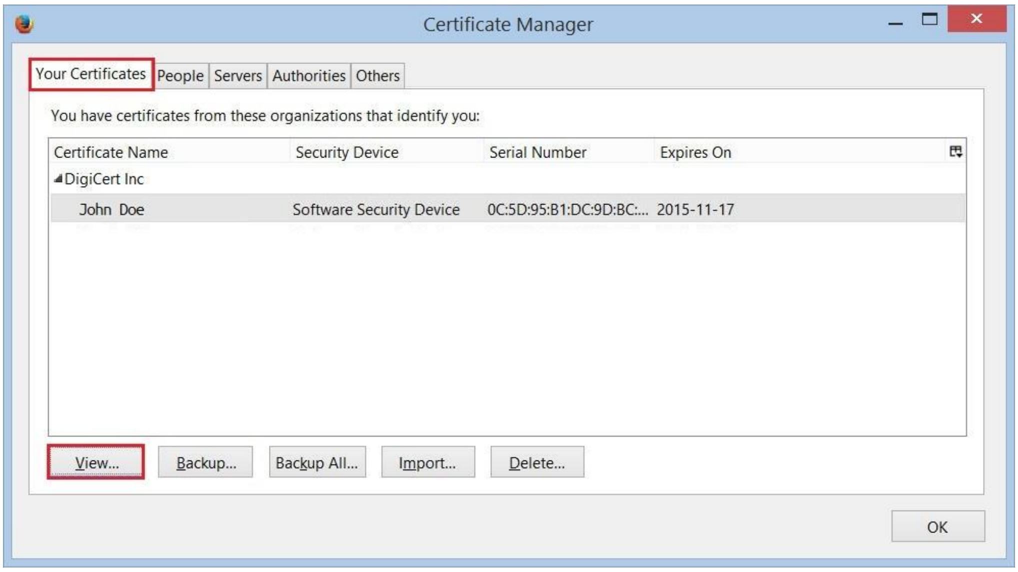


When a server requests my personal certificate:

○ Select one automatically ● Ask me every time

☑ Query OCSP responder servers to confirm the current validity of certificates

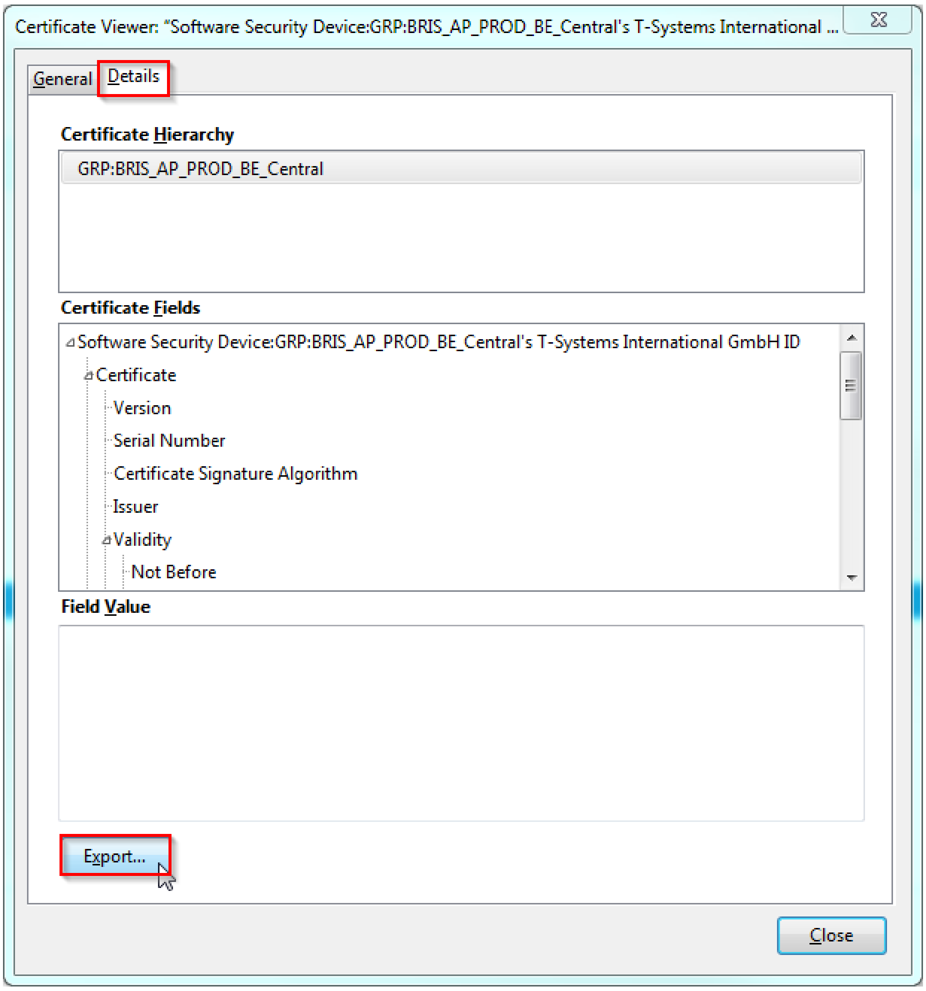
3. In the **Certificate Manager** window, on the **Your Certificates** tab, select your certificate which you want to export and then, click **View**.



You have certificates from these organizations that identify you:

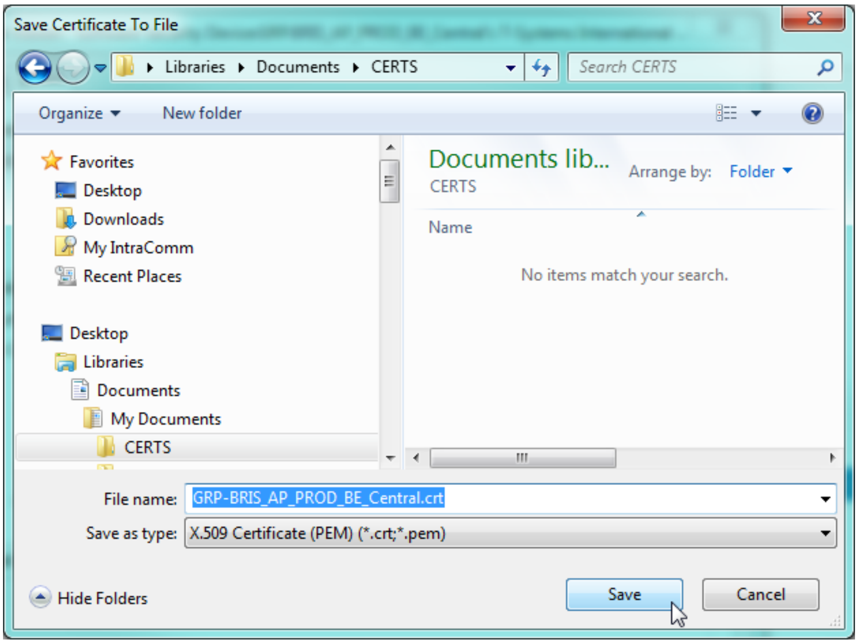
Certificate Name	Security Device	Serial Number	Expires On
◢DigiCert Inc			
John Doe	Software Security Device	0C:5D:95:B1:DC:9D:BC:...	2015-11-17

4. In the **Certificate Viewer** window select the **Details** tab and click on the **Export** button.



Certificate Viewer: "Software Security Device:GRP:BRIS_AP_PROD_BE_Central's T-Systems International ...
General
Details
Certificate Hierarchy
GRP:BRIS_AP_PROD_BE_Central
Certificate Fields
Software Security Device:GRP:BRIS_AP_PROD_BE_Central's T-Systems International GmbH ID
Certificate
Version
Serial Number
Certificate Signature Algorithm
Issuer
Validity
Not Before
Field Value
Export...
Close

5. In the **Save Certificate To File** window, go to where you want to save your public key(certificate) in crt, pem or other format, provide a file name and then click **Save**.



File name: GRP-BRIS_AP_PROD_BE_Central.crt

Save as type: X.509 Certificate (PEM) (*.crt;*.pem)

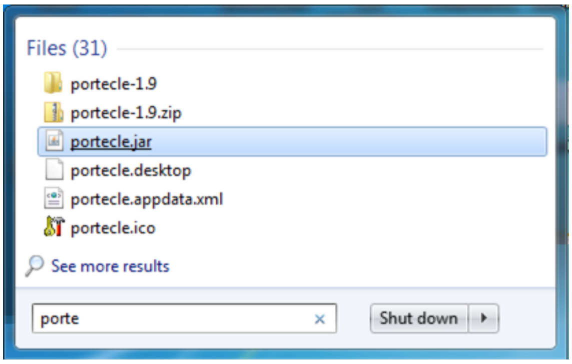
5.5. Keystore Creation

*Now that the Private key has been retrieved, we can either create a **.jks** or a **.p12** keystore file so that it can be used in the configuration of the access points, for example on Domibus (keystore section of Domibus-security.xml).*
The next 2 sections describe the procedure for both options.

5.5.1. OPTION1: JKS Keystore (preferred option)

The Keystore JKS file is used to contain the Access Point's own Private and Public Keys also known as the Key Pair.

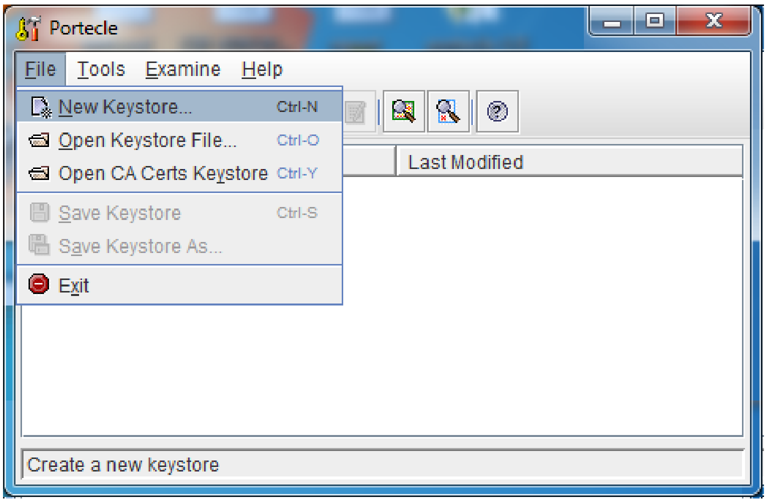
1. start **portecle.jar** (or any other suitable installed tool)



Files (31)

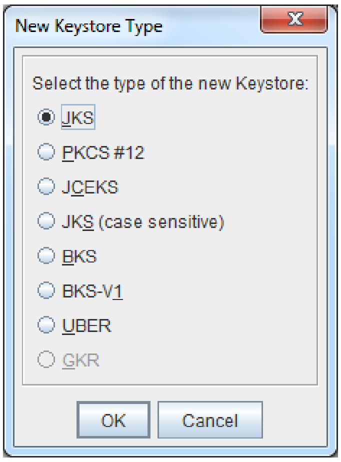
- portecle-1.9
- portecle-1.9.zip
- portecle.jar
- portecle.desktop
- portecle.appdata.xml
- portecle.ico

2. Click on **File** then **New Keystore**



Create a new keystore

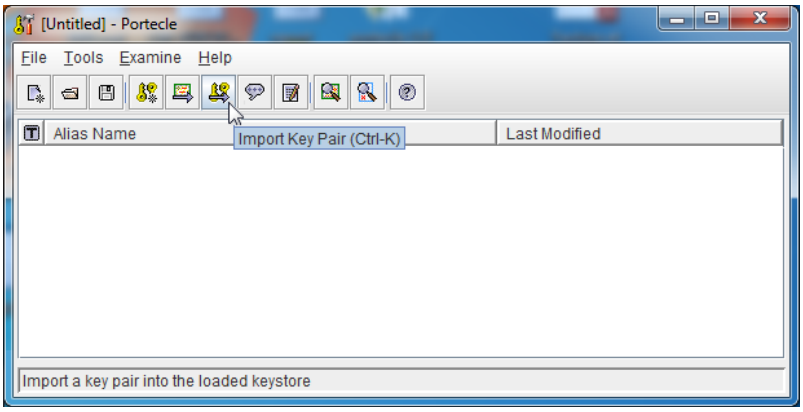
3. Select **JKS** then click on **OK**



Select the type of the new Keystore:

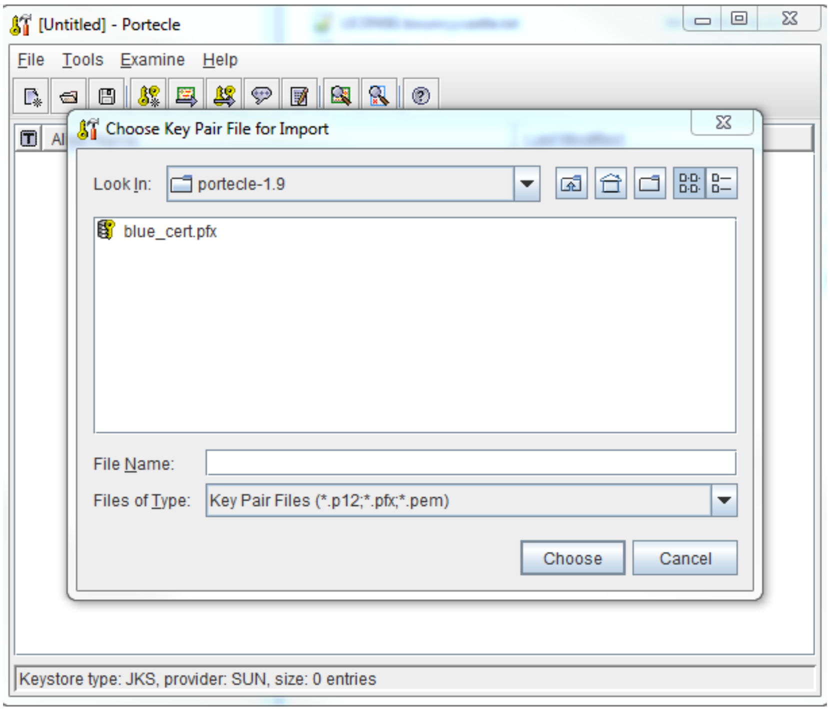
● JKS
○ PKCS #12
○ JCEKS
○ JKS (case sensitive)
○ BKS
○ BKS-V1
○ UBER
○ GKR

4. Click on the **Import Key Pair** icon



Import a key pair into the loaded keystore

5. Locate your exported private key file (.pfx)

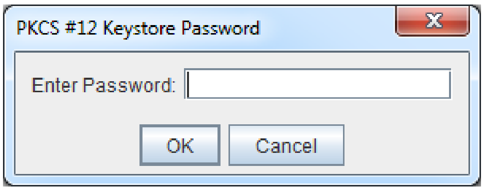


Look In: portecle-1.9

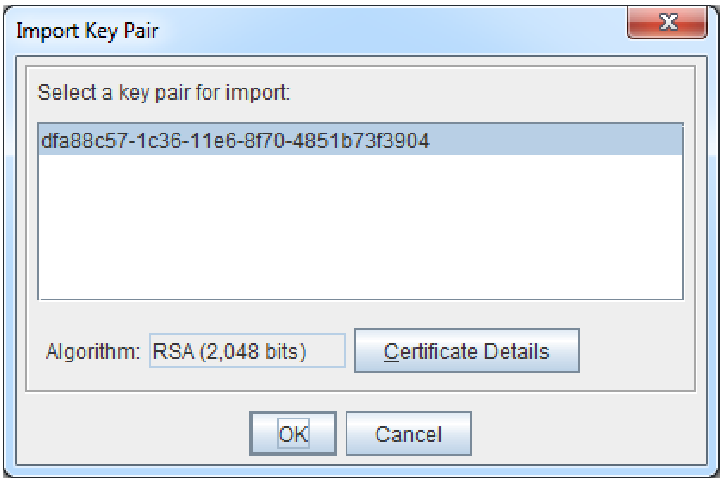
Files of Type: Key Pair Files (*.p12;*.pfx;*.pem)

Keystore type: JKS, provider: SUN, size: 0 entries

6. Enter a Password then click on **OK**



7. Click on **OK**



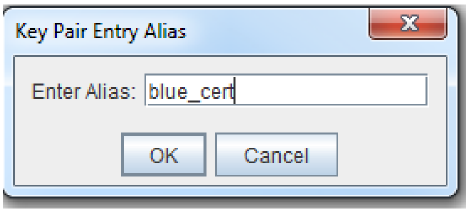
Import Key Pair

Select a key pair for import:

dfa88c57-1c36-11e6-8f70-4851b73f3904

Algorithm: RSA (2,048 bits)

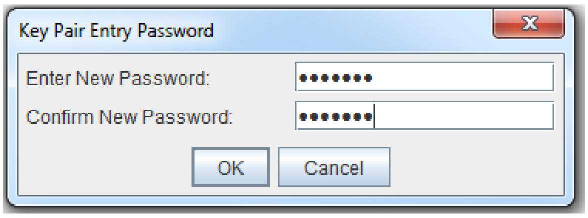
8. Enter an Alias then click on **OK**



Key Pair Entry Alias

Enter Alias: blue_cert

9. Enter Key Pair Password

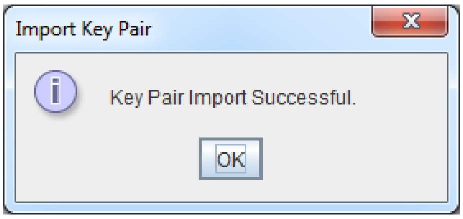


Key Pair Entry Password

Enter New Password: •••••••

Confirm New Password: •••••••

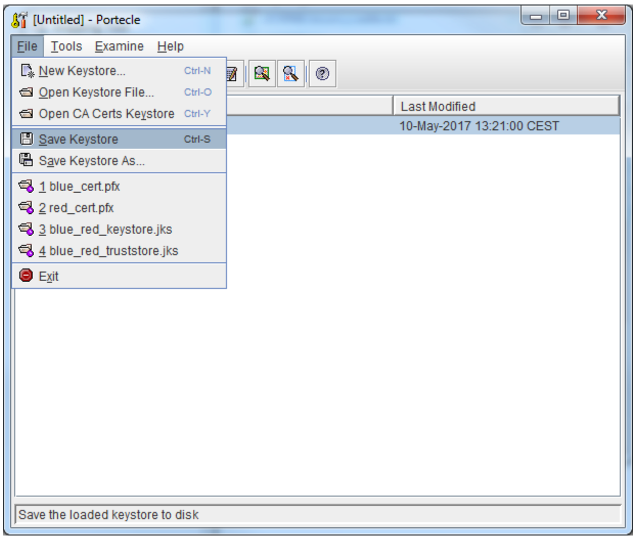
10. Click on **OK**



Import Key Pair

Key Pair Import Successful.

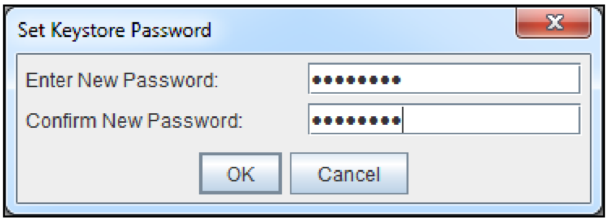
11. Save your Keystore



10-May-2017 13:21:00 CEST

Save the loaded keystore to disk

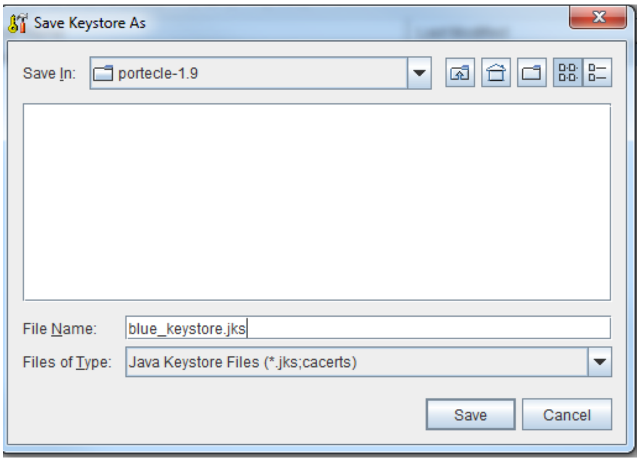
12. Set a Password for the Keystore then click on **OK**



Enter New Password: ••••••••

Confirm New Password: ••••••••

13. Choose the location and a name for the Keystore then click on OK



Save In: portecle-1.9

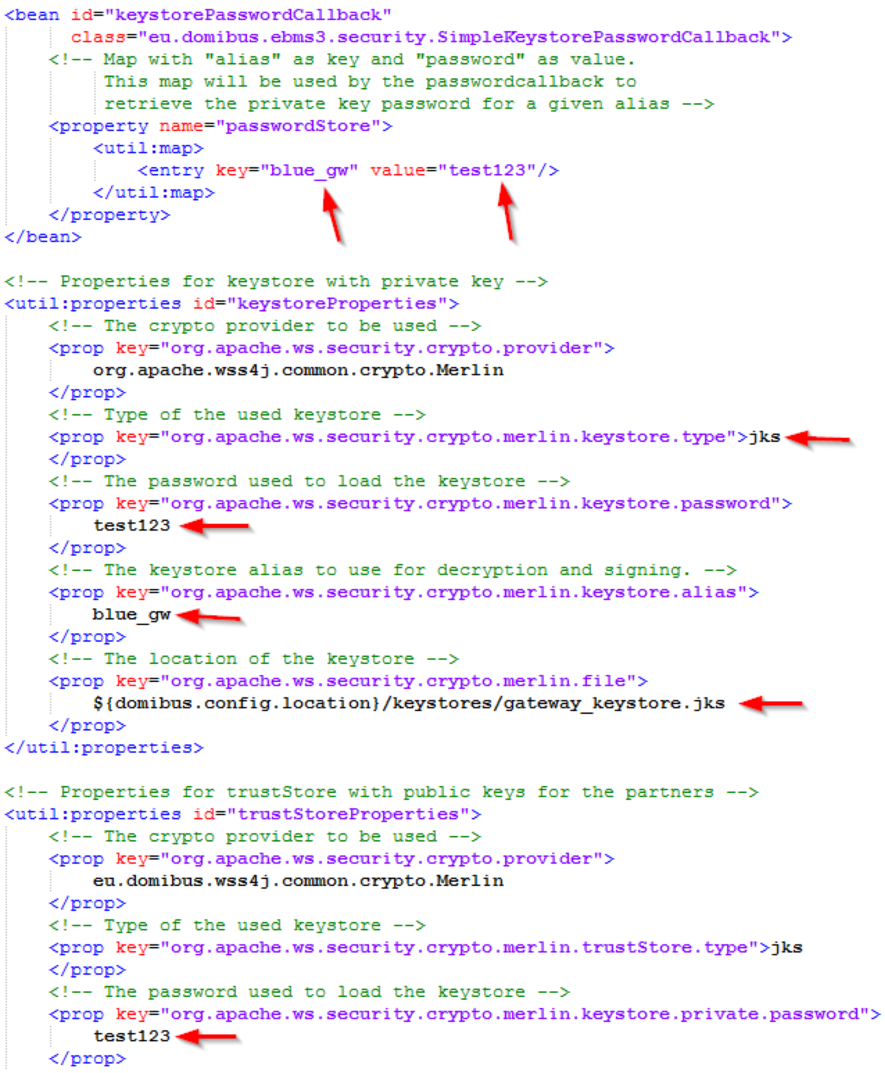
File Name: blue_keystore.jks

Files of Type: Java Keystore Files (*.jks;cacerts)

Configuration changes in domibus-security.xml / domibus.properties for the .JKS option:

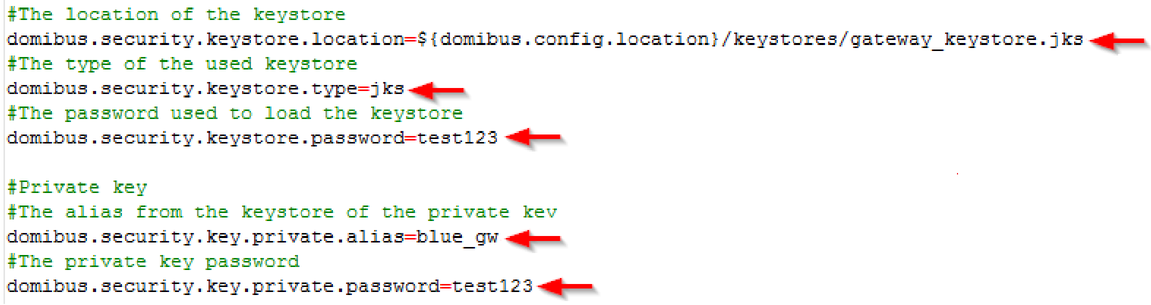
Depending on the version of Domibus that is being used, either domibus-security.xml (for version 3.2.5 and before) or domibus.properties (for version 3.3 and after) have to be updated with the keystore details included the JKS Keystore file, the chosen certificate alias and password, as shown in the examples below:

domibus-security.xml:



```
<bean id="keystorePasswordCallback"
      class="eu.domibus.ebms3.security.SimpleKeystorePasswordCallback">
    <!-- Map with "alias" as key and "password" as value.
         This map will be used by the passwordcallback to
         retrieve the private key password for a given alias -->
    <property name="passwordStore">
        <util:map>
            <entry key="blue_gw" value="test123"/>
        </util:map>
    </property>
</bean>

<!-- Properties for keystore with private key -->
<util:properties id="keystoreProperties">
    <!-- The crypto provider to be used -->
    <prop key="org.apache.ws.security.crypto.provider">
        org.apache.wss4j.common.crypto.Merlin
    </prop>
    <!-- Type of the used keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.type">jks
    </prop>
    <!-- The password used to load the keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.password">
        test123
    </prop>
    <!-- The keystore alias to use for decryption and signing. -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.alias">
        blue_gw
    </prop>
    <!-- The location of the keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.file">
        ${domibus.config.location}/keystores/gateway_keystore.jks
    </prop>
</util:properties>

<!-- Properties for trustStore with public keys for the partners -->
<util:properties id="trustStoreProperties">
    <!-- The crypto provider to be used -->
    <prop key="org.apache.ws.security.crypto.provider">
        eu.domibus.wss4j.common.crypto.Merlin
    </prop>
    <!-- Type of the used keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.trustStore.type">jks
    </prop>
    <!-- The password used to load the keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.private.password">
        test123
    </prop>
```

domibus.properties:

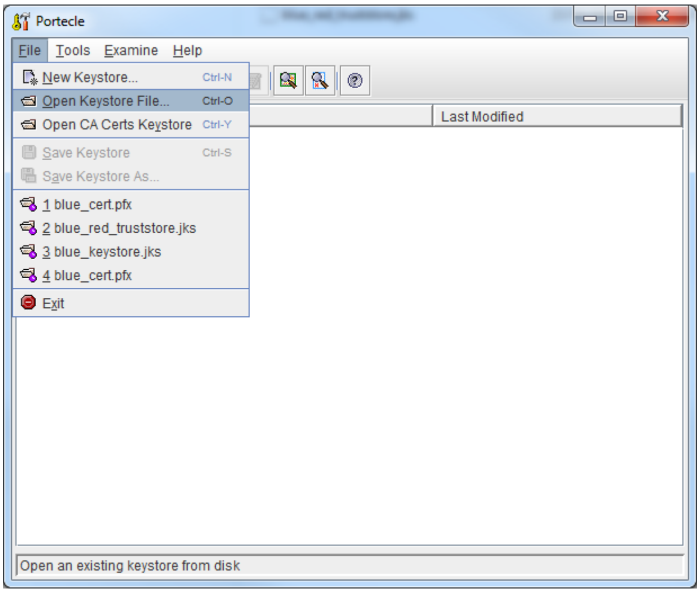


```
#The location of the keystore
domibus.security.keystore.location=${domibus.config.location}/keystores/gateway_keystore.jks
#The type of the used keystore
domibus.security.keystore.type=jks
#The password used to load the keystore
domibus.security.keystore.password=test123

#Private key
#The alias from the keystore of the private kev
domibus.security.key.private.alias=blue_gw
#The private key password
domibus.security.key.private.password=test123
```

5.5.2. OPTION2: PKCS12 Keystore (optional special request by some users)

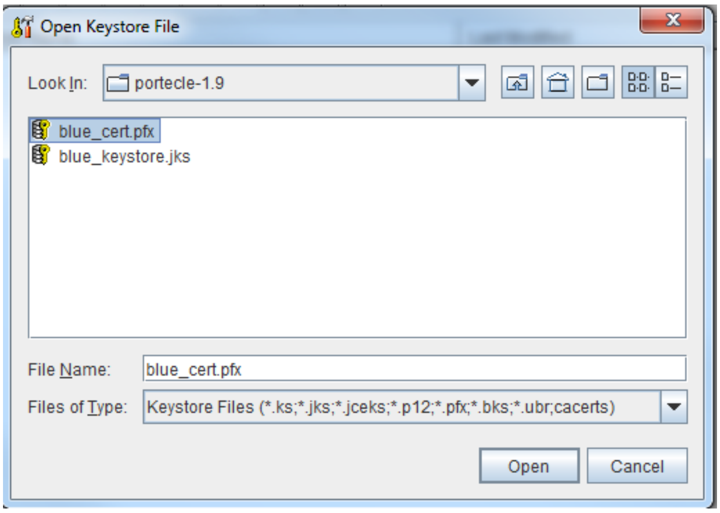
We need to make sure that the correct Alias is used in the PKCS12 Keystore, then rename it to have a .p12 extension instead of the default .pfx extension.

1. Start **portecle.jar** and choose **open Keystore file**



Open an existing keystore from disk

2. Select the .pfx private key that was exported earlier

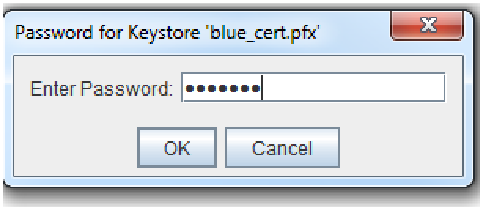


Look In: portecle-1.9

File Name: blue_cert.pfx

Files of Type: Keystore Files (*.ks;*.jks;*.jceks;*.p12;*.pfx;*.bks;*.ubr;cacerts)

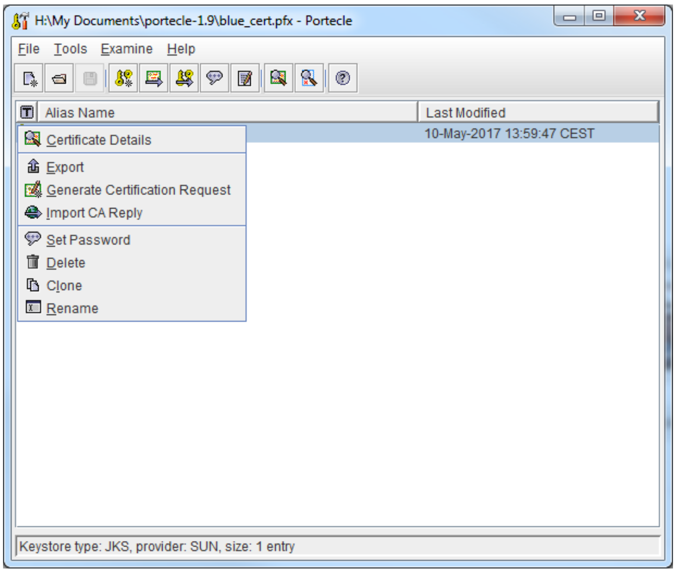
3. Enter the password



Password for Keystore 'blue_cert.pfx'

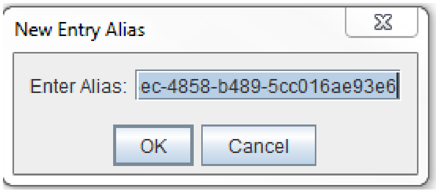
Enter Password: •••••••

4. Right click and choose rename


H:\My Documents\portecle-1.9\blue_cert.pfx - Portecle

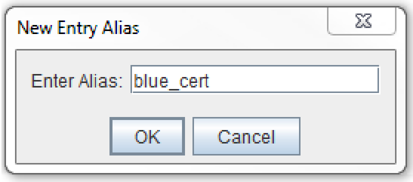
10-May-2017 13:59:47 CEST

Keystore type: JKS, provider: SUN, size: 1 entry


New Entry Alias

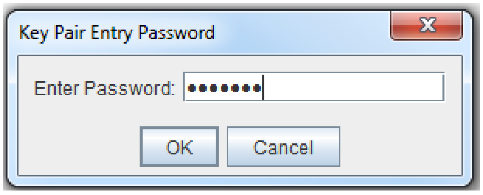
Enter Alias: ec-4858-b489-5cc016ae93e6

5. Replace the Alias with a new name


New Entry Alias

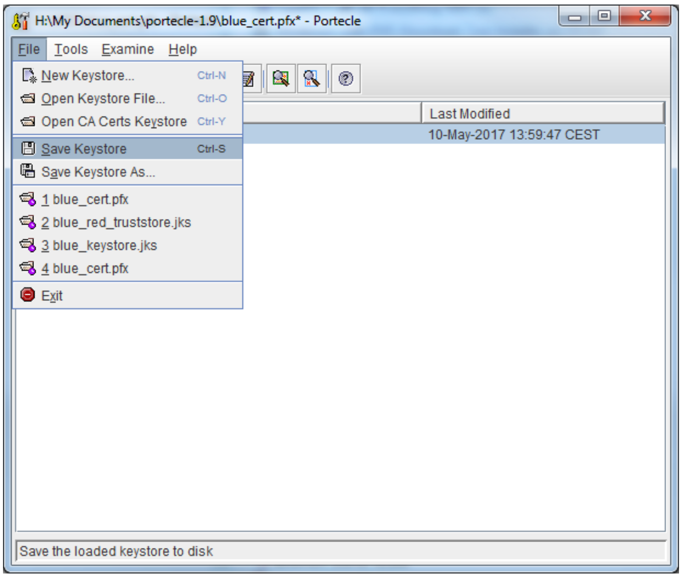
Enter Alias: blue_cert

6. Enter the password for the key pair


Key Pair Entry Password

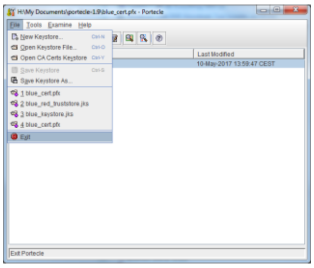
Enter Password: •••••••

7. Save the Keystore


H:\My Documents\portecle-1.9\blue_cert.pfx* - Portecle
File
Tools
Examine
Help
New Keystore... Ctrl-N
Open Keystore File... Ctrl-O
Open CA Certs Keystore Ctrl-Y
Save Keystore Ctrl-S
Save Keystore As...
1 blue_cert.pfx
2 blue_red_truststore.jks
3 blue_keystore.jks
4 blue_cert.pfx
Exit
Last Modified
10-May-2017 13:59:47 CEST

Save the loaded keystore to disk

8. Exit



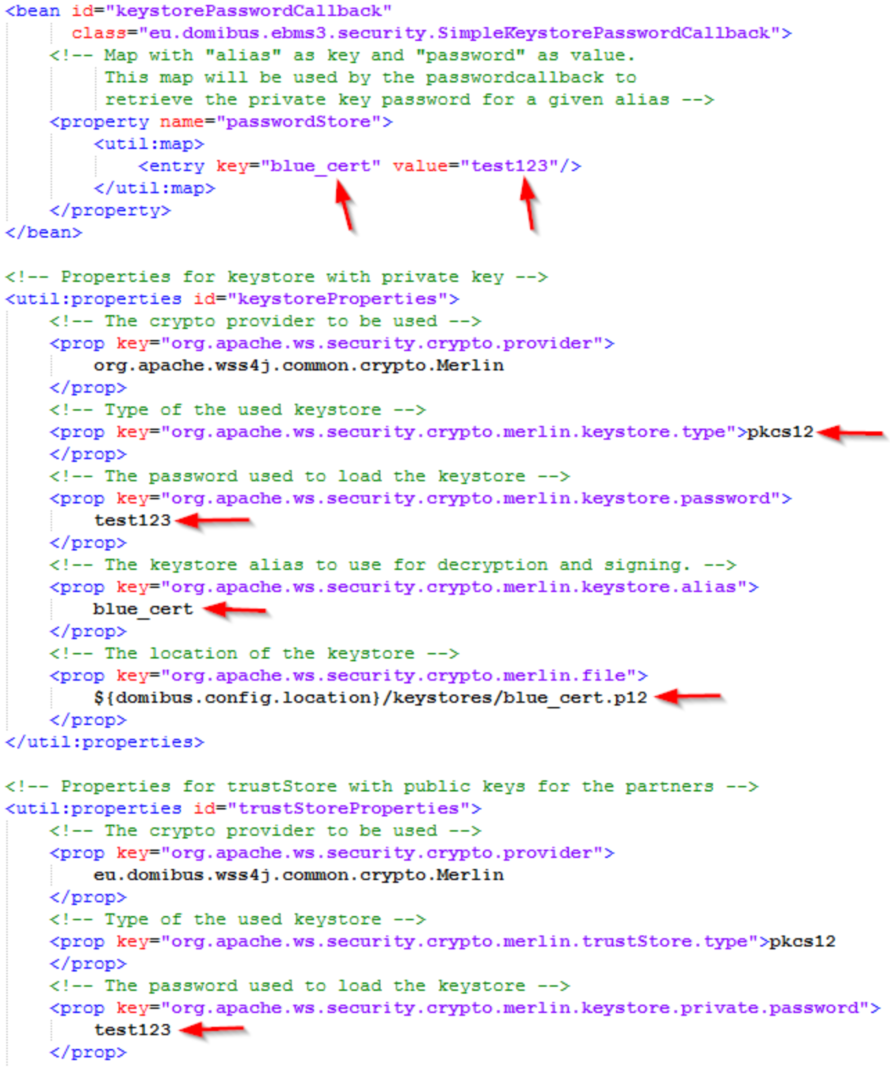
Exit Portecle

9. Change the Keystore file extension from **.pfx** to **.p12**. (e.g.: ***ren blue_cert.pfx blue_cert.p12***)

Configuration changes in domibus-security.xml / domibus.properties for the .PKCS12 option:

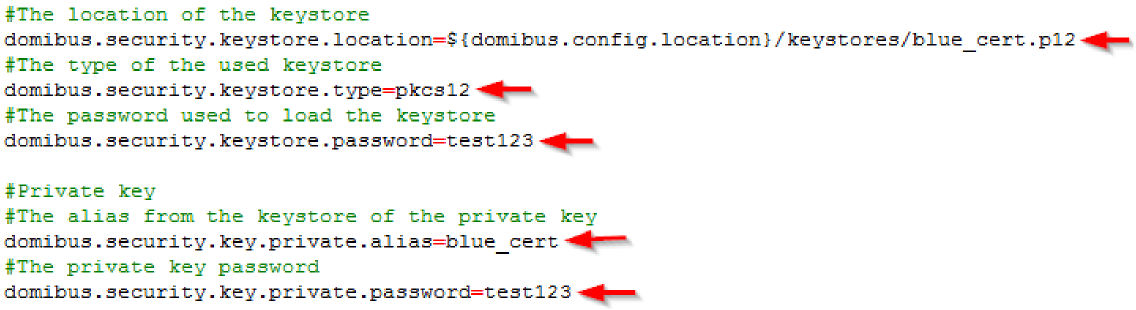
Depending on the version of Domibus that is being used, either domibus-security.xml (for version 3.2.5 and before) or domibus.properties (for version 3.3 and after) have to be updated with the keystore details included the PKCS12 keystore file, the chosen certificate alias and password, as shown in the examples below:

domibus-security.xml:



```
<bean id="keystorePasswordCallback"
      class="eu.domibus.ebms3.security.SimpleKeystorePasswordCallback">
    <!-- Map with "alias" as key and "password" as value.
         This map will be used by the passwordcallback to
         retrieve the private key password for a given alias -->
    <property name="passwordStore">
        <util:map>
            <entry key="blue_cert" value="test123"/>
        </util:map>
    </property>
</bean>

<!-- Properties for keystore with private key -->
<util:properties id="keystoreProperties">
    <!-- The crypto provider to be used -->
    <prop key="org.apache.ws.security.crypto.provider">
        org.apache.wss4j.common.crypto.Merlin
    </prop>
    <!-- Type of the used keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.type">pkcs12
    </prop>
    <!-- The password used to load the keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.password">
        test123
    </prop>
    <!-- The keystore alias to use for decryption and signing. -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.alias">
        blue_cert
    </prop>
    <!-- The location of the keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.file">
        ${domibus.config.location}/keystores/blue_cert.p12
    </prop>
</util:properties>

<!-- Properties for trustStore with public keys for the partners -->
<util:properties id="trustStoreProperties">
    <!-- The crypto provider to be used -->
    <prop key="org.apache.ws.security.crypto.provider">
        eu.domibus.wss4j.common.crypto.Merlin
    </prop>
    <!-- Type of the used keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.trustStore.type">pkcs12
    </prop>
    <!-- The password used to load the keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.private.password">
        test123
    </prop>
```

domibus.properties:

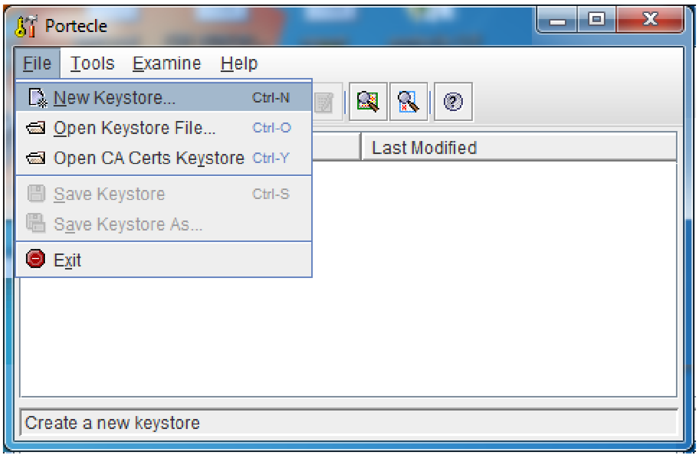


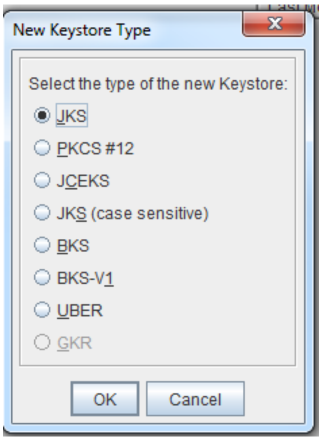
```
#The location of the keystore
domibus.security.keystore.location=${domibus.config.location}/keystores/blue_cert.p12
#The type of the used keystore
domibus.security.keystore.type=pkcs12
#The password used to load the keystore
domibus.security.keystore.password=test123

#Private key
#The alias from the keystore of the private key
domibus.security.key.private.alias=blue_cert
#The private key password
domibus.security.key.private.password=test123
```

5.6. Truststore Creation

Now that the public key has been retrieved, we can include it in a newly created (or existing) ***.jks*** *keystore file called truststore file (public keys), which will be used in the configuration of Domibus (truststore section of domibus-security.xml).*
These are the steps to follow:

1. Run Portecle, click on **File** then **New Keystore (**or **open Keystore File** if already exists**)**

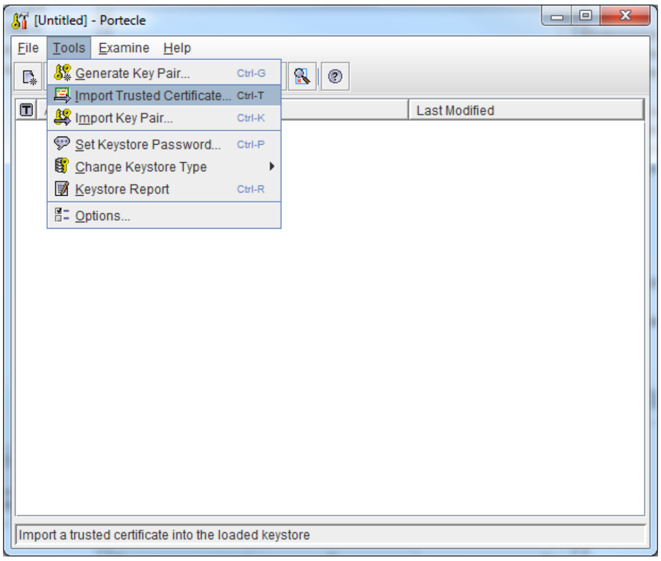




Select the type of the new Keystore:

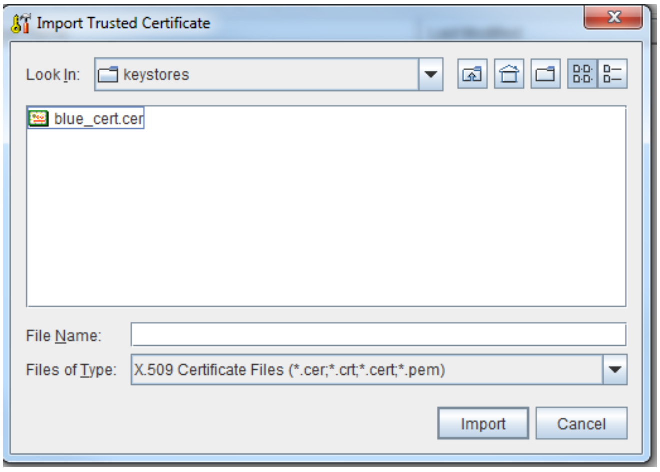
- ● JKS
- ○ PKCS #12
- ○ JCEKS
- ○ JKS (case sensitive)
- ○ BKS
- ○ BKS-V1
- ○ UBER
- ○ GKR

2. Click on the **Import Trusted Certificate** menu option.


[Untitled] - Portecle
File
Tools
Examine
Help
Generate Key Pair... Ctrl-G
Import Trusted Certificate... Ctrl-T
Import Key Pair... Ctrl-K
Set Keystore Password... Ctrl-P
Change Keystore Type
Keystore Report Ctrl-R
Options...
Last Modified

Import a trusted certificate into the loaded keystore

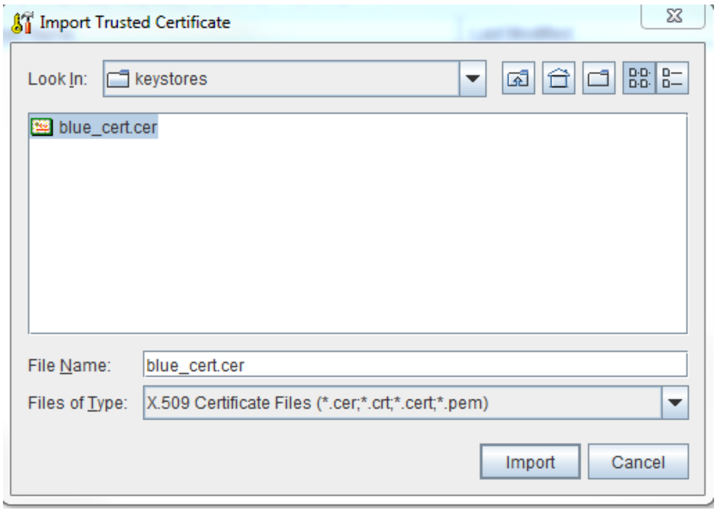
3. Select the public key that you exported (**.cer** extension) then click on **Import**



Look In: keystores

File Name:

Files of Type: X.509 Certificate Files (*.cer;*.crt;*.cert;*.pem)

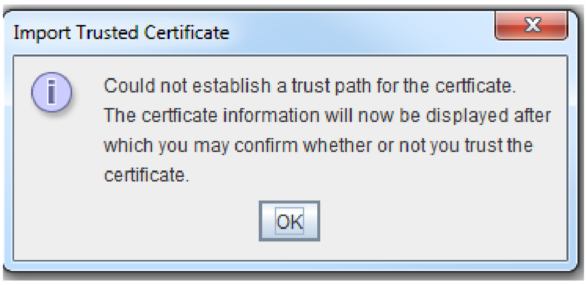


Look In: keystores

File Name: blue_cert.cer

Files of Type: X.509 Certificate Files (*.cer;*.crt;*.cert;*.pem)

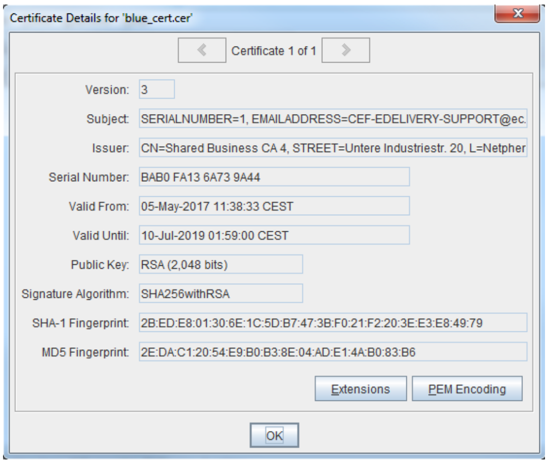
4. Click on **OK**



Import Trusted Certificate

Could not establish a trust path for the certficate. The certficate information will now be displayed after which you may confirm whether or not you trust the certificate.

5. Click on **OK**



Certificate Details for 'blue_cert.cer'

Certificate 1 of 1

Version: 3

Subject: SERIALNUMBER=1, EMAILADDRESS=CEF-EDELIVERY-SUPPORT@ec.

Issuer: CN=Shared Business CA 4, STREET=Untere Industriestr. 20, L=Netpher

Serial Number: BAB0 FA13 6A73 9A44

Valid From: 05-May-2017 11:38:33 CEST

Valid Until: 10-Jul-2019 01:59:00 CEST

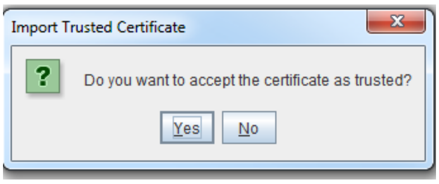
Public Key: RSA (2,048 bits)

Signature Algorithm: SHA256withRSA

SHA-1 Fingerprint: 2B:ED:E8:01:30:6E:1C:5D:B7:47:3B:F0:21:F2:20:3E:E3:E8:49:79

MD5 Fingerprint: 2E:DA:C1:20:54:E9:B0:B3:8E:04:AD:E1:4A:B0:83:B6

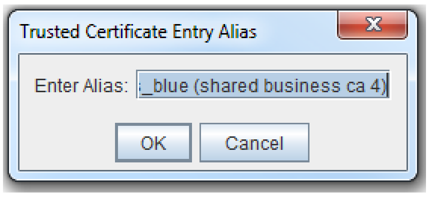
6. Click on **Yes**



Import Trusted Certificate

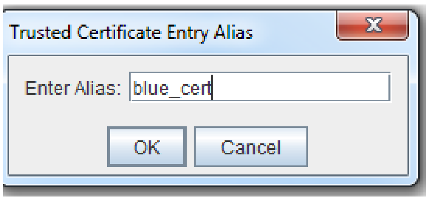
Do you want to accept the certificate as trusted?

7. Enter an Alias for the Trusted Certificate. (e.g.: blue_cert)



Trusted Certificate Entry Alias

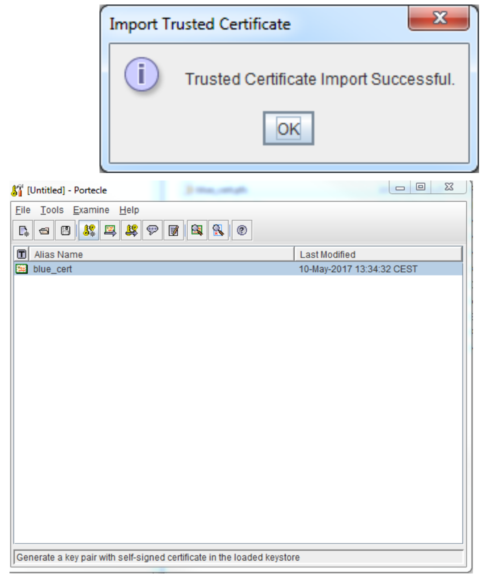
Enter Alias: :_blue (shared business ca 4)



Trusted Certificate Entry Alias

Enter Alias: blue_cert

8. Click on **OK**



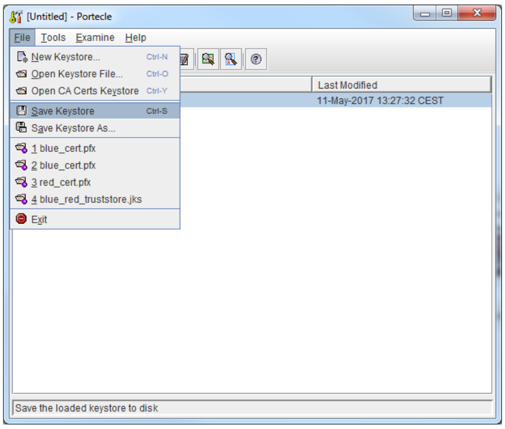
Import Trusted Certificate

Trusted Certificate Import Successful.

Alias Name	Last Modified
blue_cert	10-May-2017 13:34:32 CEST

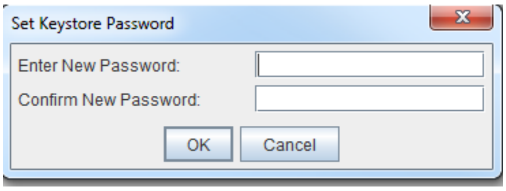
Generate a key pair with self-signed certificate in the loaded keystore

9. Save Keystore



Save the loaded keystore to disk

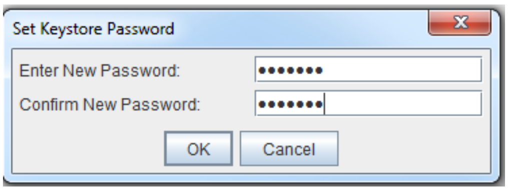
10. Choose a password for the keystore



Set Keystore Password

Enter New Password:

Confirm New Password:

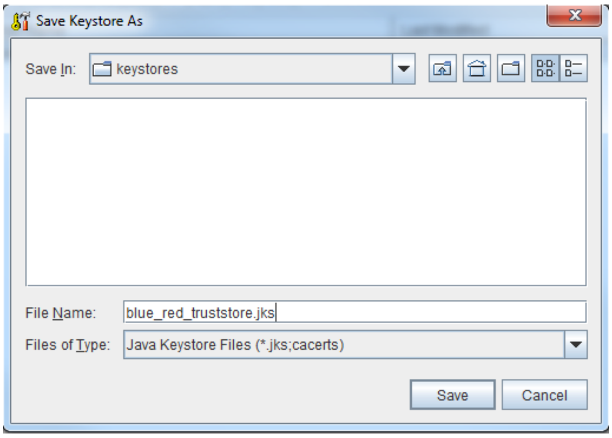


Set Keystore Password

Enter New Password: •••••••

Confirm New Password: •••••••

11. Choose a name for the Keystore (e.g.:blue_red_truststore.jks)



File Name: blue_red_truststore.jks

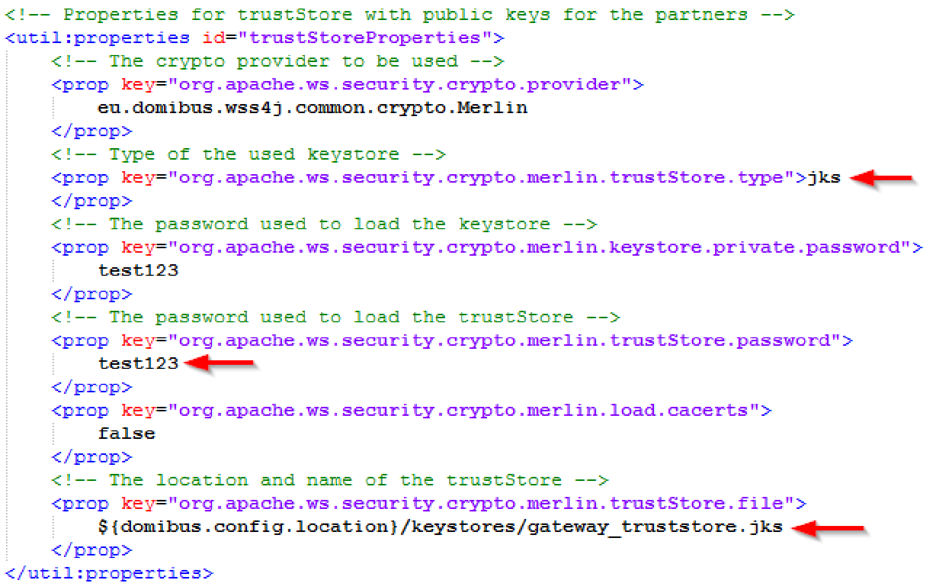
Files of Type: Java Keystore Files (*.jks;cacerts)

NOTE: ***Steps 2 to 13 can be repeated to import other public keys into the Truststore.***

Configuration changes in the domibus-security.xml / domibus.properties for the JKS/PKCS12 option:

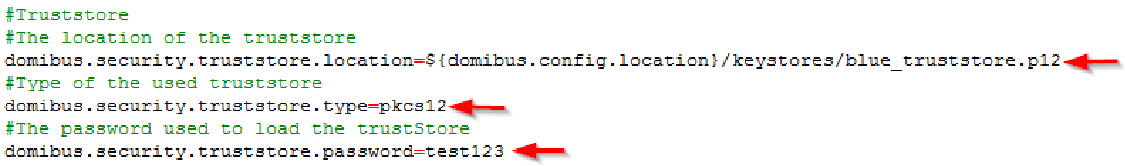
Depending on the version of Domibus that is being used, either domibus-security.xml (for version 3.2.5 and before) or domibus.properties (for version 3.3 and after) have to be updated with the truststore details included the JKS/PKCS12 truststore file and password, as shown in the examples below:

domibus-security.xml (with JKS option):



```
<!-- Properties for trustStore with public keys for the partners -->
<util:properties id="trustStoreProperties">
    <!-- The crypto provider to be used -->
    <prop key="org.apache.ws.security.crypto.provider">
        eu.domibus.wss4j.common.crypto.Merlin
    </prop>
    <!-- Type of the used keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.trustStore.type">jks
    </prop>
    <!-- The password used to load the keystore -->
    <prop key="org.apache.ws.security.crypto.merlin.keystore.private.password">
        test123
    </prop>
    <!-- The password used to load the trustStore -->
    <prop key="org.apache.ws.security.crypto.merlin.trustStore.password">
        test123
    </prop>
    <prop key="org.apache.ws.security.crypto.merlin.load.cacerts">
        false
    </prop>
    <!-- The location and name of the trustStore -->
    <prop key="org.apache.ws.security.crypto.merlin.trustStore.file">
        ${domibus.config.location}/keystores/gateway_truststore.jks
    </prop>
</util:properties>
```

domibus.properties (with PKCS12 option):



```
#Truststore
#The location of the truststore
domibus.security.truststore.location=${domibus.config.location}/keystores/blue_truststore.p12
#Type of the used truststore
domibus.security.truststore.type=pkcs12
#The password used to load the trustStore
domibus.security.truststore.password=test123
```

5.7. General Terms and Conditions (GTC) of the CEF PKI service

Context

In its capacity as Solution Provider of the eDelivery Building Block of the Connecting Europe Facility, DIGIT makes available a PKI service[8] (referred to as "CEF PKI service") to the European Institutions, other Public Administrations and Businesses. The CEF PKI service is used by Organisations (referred to as "end-Users") participating in projects that deploy the components of CEF eDelivery.

DIGIT is a PKI tenant within the TeleSec Shared-Business-CA solution (referred to as "SBCA") operated in the Trust Center of the Group unit T-Systems International GmbH (referred to as "T-Systems"[9]). DIGIT plays the role of Master Registrar of the 'CEF_eDelivery.europa.eu' domain of the SBCA. In this role, DIGIT creates sub-domains within the 'CEF_eDelivery.europa.eu' domain for each project using the CEF PKI service.

This document provides details on the terms and conditions of the **TACHOnet project** (referred to as "the project") sub-domain. DIGIT plays the role of sub-Registrar of this sub-domain. In this capacity, it issues, revokes and renews the certificates of this project.

Disclaimer on liability

The European Commission accepts no responsibility or liability whatsoever with regard to the content of the certificate which lies exclusively with the certificate owner. It is the responsibility of the certificate owner to check the accuracy of the certificate content.

The European Commission accepts no responsibility or liability whatsoever with regard to the use of the certificate by its owner being a third legal entity outside the European Commission.

This disclaimer is not intended to limit the liability of the European Commission in contravention of any requirements laid down in applicable national law or to exclude its liability for matters which may not be excluded under that law.

Authorised /prohibited uses of certificates

Permitted usage of certificates

Once the certificate is issued, the end-User, referred to as the "certificate owner"[10], shall use the certificate only in the context of the aforementioned project. Within this context, the certificate can be used to:

- authenticate the origin of data;
- encrypt data;

[8] A PKI (Public Key Infrastructure) is a set of roles, policies, procedures and systems needed to create, manage, distribute, and revoke digital certificates.

[9] The trusted role of the Trust Center operator, located in the T-Systems Trust Center, also performs the task of internal registration authority.

[10] Identified by the "O=" attribute value in the Subject Distinguished Name of the issued certificate

- ensure detection of integrity breaches of data.

Prohibited usage of certificates

Any usage not explicitly authorised as part of the permitted usages of the certificate is prohibited.

Additional obligations of the certificate owner

The detailed terms and conditions of the SBCA are defined by T-Systems in the Certificate Policy (CP)/Certification Practice Statement (CPS) of the SBCA service11. This document includes security specifications and guidelines regarding technical and organizational aspects and describes the activities of the Trust Centre operator in the roles of Certification Authority (CA) and Registration Authority (RA) as well as the Registration Authority's (RA) delegated third party.

It should be highlighted that:

- Only entities authorised to participate in the aforementioned project can request a certificate, as described in the Service Offering Description document of the CEF PKI service for the aforementioned project.
- Regarding certificate acceptance, clause 4.4.1 of the SBCA CP/CPS applies, furthermore the terms of use and provisions described in the present document are deemed accepted by the organization to which the certificate is issued ("O=") when first used.
- Regarding publication of the certificate, clause 2.2 of the SBCA CP/CPS applies.
- All certificate owners and certified end-entities shall comply with the following requirements:
  - Protect their private key against unauthorized use.
  - Refrain from transferring or revealing their private key to third parties, even as representatives.
  - Refrain from continued use of the private key following expiry of the validity period or revocation of the certificate, other than to view encrypted data (e.g., decrypting e-mails).
  - The certificate owner is responsible for copying or forwarding the key to the end entity or entities.
  - The certificate owner must obligate the end entity/all end entities to comply with the present terms and conditions, including the SBCA CP/CPS, when dealing with the private key.
  - Certificate owner must provide the identification of those authorised representatives who are authorized to request revocation of certificates issued to the organisation with the details of events that lead to revocation and the revocation password.
  - For certificates associated to groups of persons and functions and/or legal persons, after a person leaves the group of end entities (e.g. termination of

[11] The latest version of the T-Systems SBCA CP/CPS is available from https://www.telesec.de/en/sbca-en/support/download-area/.

    the employment relationship), the certificate owner must prevent misuse of the private key by revoking the certificate.
    - Certificate owner is responsible and has obligation to request revocation of certificate under circumstances identified in clause 4.9.1 of the SBCA CP/CPS.
- Regarding renewal or rekey of certificates, clause 4.6 or 4.7 of the SBCA CP/CPS applies.
- Regarding amendment of certificate, clause 4.8 of the SBCA CP/CPS applies.
- Regarding certificate revocation, clause 4.9 of the SBCA CP/CPS applies.

5.8. Contact persons and trusted couriers identification form (sample)

Please print the text of this document on your letterhead, add your organisation stamp and have it signed by an authorised representative of your organisation.

TACHOnet contact persons and trusted couriers identification form

I, *[name and address of the organisation representative]*, **certifies that the following information are to be used in the context of the request, generation and retrieval of public key digital certificates for TACHOnet access points supporting the confidentiality, integrity and non-repudiation of the TACHOnet messages:**

Contact person information**:**

Contact person #1	**Contact person #2**
Name:	Name:
First names:	First names:
Mobile phone:	Mobile phone:
Telephone:	Telephone:
Email:	Email:
Specimen handwritten signature:	Specimen handwritten signature:

Please duplicate the above table when more than two contact persons are required.

Trusted courier information**:**

Trusted courier #1	**Trusted courier #2**
Name:	Name:
First names:	First names:
Mobile phone:	Mobile phone:
Email:	Email:
Passport issuing country:	Passport issuing country:
Passport number:	Passport number:
Passport validity end date:	Passport validity end date:

Please duplicate the above table when more than two contact persons are required.

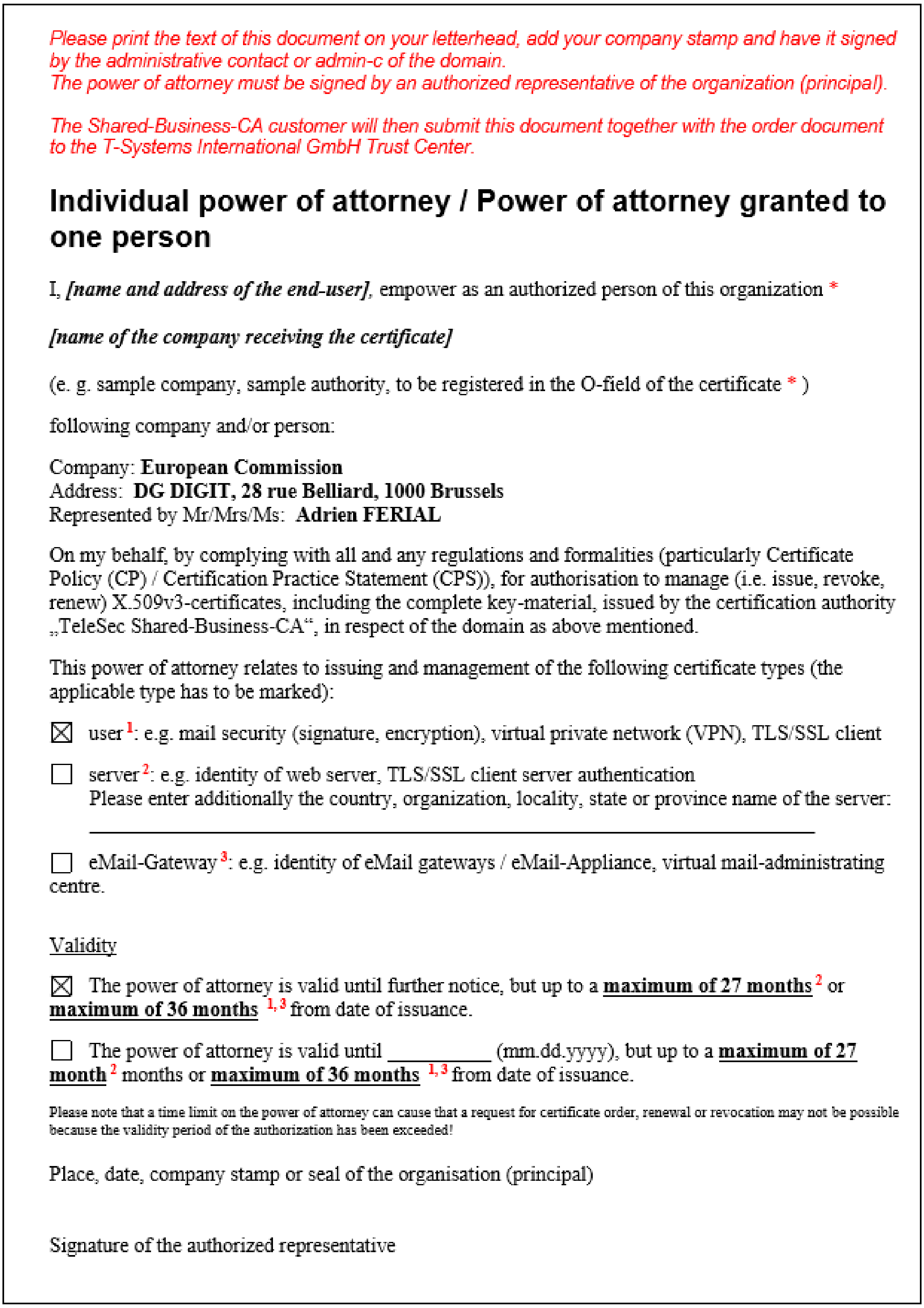
Please attach a high resolution copy of page 2 of the passport for all trusted couriers.

Place, date, company stamp or seal of the Organisation:

Signature of the authorised representative:

5.9. Individual Power of Attorney (sample)

A sample of the individual Power of Attorney that must be signed and presented by the trusted courier during face-to-face registration at RAO can be found here:



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

5.10. Certificate request paper form (sample)

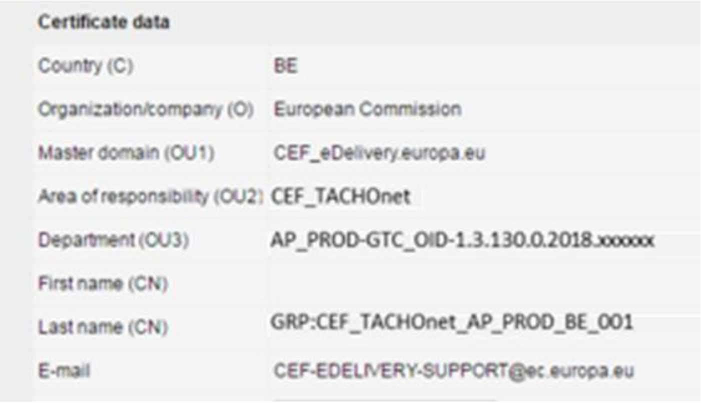
A sample of the certificate request paper form that must be signed and presented by the trusted courier during face-to-face registration at RAO can be found here:

Please print the text of this document on your letterhead, add your organisation stamp and have it signed by an authorised representative of your organisation.

TACHOnet certificate request paper form

I, *[name and address of the organisation representative]*, **certifies that the following information are to be used in the context of the request, generation and retrieval of public key digital certificates for TACHOnet access points supporting the confidentiality, integrity and non-repudiation of the TACHOnet messages:**

Please reproduce the certificate data information provided by CEF Support Team acknowledging the completeness of the electronic certificate request, e.g.:



Certificate data	
Country (C)	BE
Organization/company (O)	European Commission
Master domain (OU1)	CEF_eDelivery.europa.eu
Area of responsibility (OU2)	CEF_TACHOnet
Department (OU3)	AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First name (CN)	
Last name (CN)	GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail	CEF-EDELIVERY-SUPPORT@ec.europa.eu

Certificate request reference number: ***insert reference number (e.g. 776002)***

Identification of the trusted courier proceeding to the face-to-face registration of the request: ***please fill in***

Trusted courier #1
Name:
First names:
Mobile phone:
Email:
Passport issuing country:
Passport number:
Passport validity end date:

Place, date, company stamp or seal of the Organisation:

Signature of the authorised representative:

6. LIST OF FIGURES

7. List of tables

8. Contact Information

CEF Support Team

By email: CEF-EDELIVERY-SUPPORT@ec.europa.eu

By phone: +32 2 299 09 09

- **Standard Service: 8am to 6pm (Normal EC working Days)**
- **Standby Service*: 6pm to 8am (Commission and Public Holidays, Weekends)**

**** Only for critical and urgent incidents and only by phone***