



EUROPEAN
COMMISSION

Brussels, 2.10.2018
COM(2018) 664 final

2018/0339 (NLE)

Proposal for a

COUNCIL DECISION

on the position to be taken on behalf of the European Union in the Group of Experts on the European Agreement concerning the work of crews of vehicles engaged in international road transport of the United Nations Economic Commission for Europe

EXPLANATORY MEMORANDUM

1. SUBJECT MATTER OF THE PROPOSAL

This proposal concerns the decision establishing the position to be taken on the Union's behalf in the Group of Experts on AETR of the United Nations Economic Commission for Europe (UNECE) in connection with the envisaged amendment to the European agreement concerning the work of crews of vehicles engaged in international road transport (AETR) regarding the connection to TACHOnet of non-EU AETR Contracting Parties.

2. CONTEXT OF THE PROPOSAL

2.1. The AETR

The European agreement concerning the work of crews of vehicles engaged in international road transport ('the Agreement') aims to harmonise the legislative framework of Contracting Parties to the Agreement as regards driving and rest times for professional drivers, as well as the corresponding technical requirements for the construction and installation of the tachograph. The Agreement entered into force on 5 January 1976.

All Member States are parties to the Agreement¹.

2.2. The Group of Experts on AETR

The Group of Experts on AETR is a technical group that has been set up by the Inland Transport Committee of the UNECE with the objective to develop amendment proposals to the Agreement. Proposals for amendments to the Agreement are adopted by unanimity of the experts of the Group and further submitted to the SC.1 (UNECE Working Party on Road Transport) for adoption by simple majority of the Contracting Parties present and voting.

2.3. The envisaged act of the Group of Experts on AETR

On 15 October 2018, during its 19th session, the Group of Experts on AETR is to decide on the submission to the SC.1 of a proposal for an amendment of the AETR regarding the connection to TACHOnet of non-EU AETR Contracting Parties ('the envisaged act').

The purpose of the envisaged act is to define the technical requirements for the connection of non-EU AETR Contracting Parties to TACHOnet by means of the eDelivery platform developed by the European Commission.

The envisaged act will become binding on the parties in accordance with Article 13 paragraph 1 of the Agreement, which provides: 'All the new provisions of the present Agreement, including its Annex and Appendices 1B and 2, relating to the introduction of a digital control device, shall become mandatory for countries which are Contracting Parties to this Agreement at latest four years after the date of entry into force of the relevant amendments resulting from the procedure specified in Article 21'.

¹ Austria (ratified on 11/6/1975), Belgium (ratified on 30/12/1977), Bulgaria (ratified on 12/5/1995), Croatia (ratified on 3/8/1992), Cyprus (ratified on 5/9/2003), Czech Republic (ratified on 22/6/1993), Denmark (ratified on 30/12/1977), Estonia (ratified on 3/5/1993), Finland (ratified on 16/2/1999), France (ratified on 9/1/1978), Germany (ratified on 9/7/1975), Greece (ratified on 11/1/1974), Hungary (ratified on 22/10/1999), Ireland (ratified on 28/8/1979), Italy (ratified on 28/12/1978), Latvia (ratified on 14/1/1994), Lithuania (ratified on 3/6/1998), Luxembourg (ratified on 30/12/1977), Malta (ratified on 24/9/2004), Netherlands (ratified on 30/12/1977), Poland (ratified on 14/7/1992), Portugal (ratified on 20/9/1973), Romania (ratified on 8/12/1994), Slovakia (ratified on 28/5/1993), Slovenia (ratified on 6/8/1993), Spain (ratified on 3/1/1993), Sweden (ratified on 24/8/1973), United Kingdom (ratified on 4/1/1978).

3. POSITION TO BE TAKEN ON THE UNION'S BEHALF

TACHOnet is the European System for the electronic exchange of information between Member States on tachograph cards. It is an essential tool to ensure enforcement of the rules on driving and rest times in road transport which are set out in Regulation (EU) No 561/2006². The main objective of TACHOnet is to verify that two or more cards are not issued by different Member States to the same driver.

Member States are obliged to connect to TACHOnet in accordance with Article 31§2 of Regulation (EU) No 165/2014³ and with the technical requirements set out in Regulation (EU) 2016/68⁴.

Driving and rest time rules are also applicable to non-EU AETR (European agreement concerning the work of crews engaged in international road transport) Contracting Parties. To ensure enforcement of driving and rest time rules in these countries, it is therefore essential that they are also connected to TACHOnet. Non-EU AETR Contracting Parties are however not allowed to connect directly to TACHOnet. Direct connections are set up via the TESTA (Trans European Services for Telematics between Administrations) network, whose access is reserved to authorities and institutions from the EU, EU Member States, EEA countries, Switzerland and countries acceding to the EU. Non-EU countries which are not acceding to the EU or which are not part of the EEA must be connected to TACHOnet through a country already connected to TESTA, i.e. indirect connection. Such indirect connections are based on bilateral agreements concluded between non-EU AETR Contracting Parties and the country providing the connection.

Andorra, Armenia, Azerbaijan, Bosnia-Herzegovina, Georgia, Liechtenstein, Moldova, Serbia and Ukraine are the 9 non-EU AETR Contracting Parties which are currently connected indirectly to TACHOnet through the hubs provided by France, Croatia, Poland, Romania and Switzerland.

Technical problem to be addressed and proposed solution

The Directorate General for Informatics of the Commission (DIGIT) has recently considered that indirect connections do not comply with the minimum security standards that are required by the Commission. This is due to the fact that the stretch of the network set up between the Member State and the third party does not have to be secured. In addition the occurrence of any kind of attack to that part of the network is potentially not visible to the Commission. This increases the risk of breaches to the security system.

Indirect connections must therefore be removed and replaced by an alternative tool to allow connection to TACHOnet by non-EU AETR Contracting Parties.

² Regulation (EU) No 561/2006 of the European Parliament and of the Council of 15 March 2006 on the harmonisation of certain social legislation relating to road transport and amending Council Regulations (EEC) No 3821/85 and (EC) No 2135/98 and repealing Council Regulation (EEC) No 3820/85 (OJ L 102, 11.4.2006, p.1)

³ Regulation (EU) No 165/2014 of the European Parliament and of the Council of 4 February 2014 on tachographs in road transport, repealing Council Regulation (EEC) No 3821/85 on recording equipment in road transport and amending Regulation (EC) No 561/2006 of the European Parliament and of the Council on the harmonisation of certain social legislation relating to road transport (OJ L 60, 28.2.2014, p.1)

⁴ Commission Implementing Regulation (EU) 2016/68 of 21 January 2016 on common procedures and specifications necessary for the interconnection of electronic registers of driver cards (OJ L 15, 22.1.2016, p.51)

Such connection could be provided by *eDelivery*. *eDelivery* is an overarching platform which was funded by the CEF programme (Connecting Europe Facility). It grants connection through the Internet and makes use of standard security technologies such as PKI (public key infrastructure), for ensuring the authenticity, integrity and confidentiality of the information exchanged. It therefore ensures mutual trust when exchanging information electronically. The *eDelivery* service is provided by DIGIT.

eDelivery has already been used successfully for the provision of several EU-wide services, such as PEPPOL (Pan-European Public Procurement On-line) and e-Codex (electronic connection between legal professionals throughout the EU). The system could be adapted to TACHOnet.

Although no specific deadlines have been provided by DIGIT regarding the shutdown of indirect connections, it has been estimated that the adaptation of *eDelivery* to TACHOnet would take around one year. It is therefore necessary to amend the AETR within the shortest delay so that *eDelivery* is operational as soon as possible.

Obligations for national authorities for the use of TACHOnet

The use of *eDelivery* for the connection to TACHOnet requires that connected parties assume certain obligations in order to guarantee a proper use of the system and of the information exchanged with their counterparts. Those obligations relate to:

a) Security

National authorities must protect private keys and corresponding digital certificates, by:

- Avoiding unauthorized use of the private keys;
- Refraining from transferring or revealing their private keys to third parties;
- Ensuring confidentiality, integrity and availability of the private keys generated, stored and used for TACHOnet;
- Refraining from using the private key following expiry of the validity period or revocation of the certificate;
- Destroying keys once that they have expired;
- Preventing misuse of the private keys 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.

b) Data protection

Personal data protection needs to be ensured. Given that non-EU AETR Contracting Parties are not bound by the European legislation on data protection, it is necessary to guarantee compliance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. This Convention is the international framework of reference in the field of personal data protection.

c) Technical aspects

Connected parties must carry out a specific set of tests before connection. They must also guarantee a minimum level of service so that TACHOnet is not disrupted due to breakdowns at national level.

Legal instrument

The technical requirements for the connection of the non-EU AETR Contracting Parties to TACHONET should be set out in the appropriate international framework, i.e. the AETR agreement.

There are ongoing negotiations in the UNECE Group of Experts on AETR in view of a modification of the agreement, notably to ensure application of the EU legislation on the smart tachograph by the non-EU AETR Contracting Parties and to allow the EU to accede to the AETR⁵. The technical and legal requirements for the connection of the non-EU AETR Contracting Parties to TACHONET should be formally submitted by the EU to the AETR secretariat as a new appendix to the Agreement. This new appendix will be discussed at the next meeting of the Group of Experts on the AETR and in the Working Party on Road Transport together with the elements of the position of the EU already transmitted to the secretariat of the AETR in 2016.

4. LEGAL BASIS

4.1. Procedural legal basis

4.1.1. Principles

Article 218(9) of the Treaty on the Functioning of the European Union (TFEU) provides for decisions establishing *‘the positions to be adopted on the Union’s behalf in a body set up by an agreement, when that body is called upon to adopt acts having legal effects, with the exception of acts supplementing or amending the institutional framework of the agreement.’*

Article 218(9) TFEU applies regardless of whether the Union is a member of the body or a party to the agreement⁶.

The concept of *‘acts having legal effects’* includes acts that have legal effects by virtue of the rules of international law governing the body in question. It also includes instruments that do not have a binding effect under international law, but that are *‘capable of decisively influencing the content of the legislation adopted by the EU legislature’*⁷.

4.1.2. Application to the present case

The Group of Experts on AETR is a body set up by the Inland Transport Committee of the UNECE.

The act which the Group of Experts on AETR is called upon to set forth to the SC.1 constitutes an act having legal effects. The envisaged act will be binding under international law in accordance with Article 13 of the AETR.

The envisaged act does not supplement or amend the institutional framework of the Agreement.

Therefore, the procedural legal basis for the proposed decision is Article 218(9) TFEU.

⁵ Position of the EU adopted by Council Decision (EU) 2016/1877 of 17 October 2016, submitted to the AETR Secretariat by the Republic of Slovakia

⁶ Judgment of the Court of Justice of 7 October 2014, Germany v Council, C-399/12, ECLI:EU:C:2014:2258, paragraph 64.

⁷ Judgment of the Court of Justice of 7 October 2014, Germany v Council, C-399/12, ECLI:EU:C:2014:2258, paragraphs 61 to 64.

4.2. Substantive legal basis

4.2.1. Principles

The substantive legal basis for a decision under Article 218(9) TFEU depends primarily on the objective and content of the envisaged act in respect of which a position is taken on the Union's behalf. If the envisaged act pursues two aims or has two components and if one of those aims or components is identifiable as the main one, whereas the other is merely incidental, the decision under Article 218(9) TFEU must be founded on a single substantive legal basis, namely that required by the main or predominant aim or component.

4.2.2. Application to the present case

The main objective and content of the envisaged act relate to 'Transport'.

Therefore, the substantive legal basis of the proposed decision is Article 91 of the TFEU.

4.3. Conclusion

The legal basis of the proposed decision should be Article 91, in conjunction with Article 218(9) TFEU.

Proposal for a

COUNCIL DECISION

on the position to be taken on behalf of the European Union in the Group of Experts on the European Agreement concerning the work of crews of vehicles engaged in international road transport of the United Nations Economic Commission for Europe

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 91, in conjunction with Article 218(9) thereof,

Having regard to the proposal from the European Commission,

Whereas:

- (1) The European agreement concerning the work of crews of vehicles engaged in international road transport (AETR) entered into force on 5 January 1976.
- (2) A Group of Experts has been established by the United Nations Economic Commission for Europe in the framework of the AETR. It is a body which is empowered to develop and submit proposals for amending the AETR to the Working Party on Road Transport.
- (3) During its 19th session to take place on 15 October 2018, the Group of Experts on AETR is to adopt a decision on the submission to the UNECE Working Party on Road Transport of a proposal for an amendment to the AETR.
- (4) It is appropriate to establish the position to be taken on the Union's behalf in the Group of Experts on AETR, as the amendment to the AETR will be binding on the Union.
- (5) In its judgment of 31 March 1971, case 22/70, *AETR*, the Court of Justice of the European Union recognized that the area of the work of crews of vehicles engaged in road transport is an external competence of the Union. This competence has been exercised since then in numerous acts of law adopted by the Union legislator, including Regulation (EC) No 561/2006 of the European Parliament and of the Council⁸ and Regulation (EU) No 165/2014 of the European Parliament and of the Council⁹. Since the subject matter of the AETR falls within the scope of Regulation (EC) No 561/2006, the power to negotiate and conclude the Agreement and its modifications lies exclusively with the Union.

⁸ Regulation (EC) No 561/2006 of the European Parliament and of the Council of 15 March 2006 on the harmonisation of certain social legislation relating to road transport and amending Council Regulations (EEC) No 3821/85 and (EC) No 2135/98 and repealing Council Regulation (EEC) No 3820/85 (OJ L 102, 11.4.2006, p. 1).

⁹ Regulation (EU) No 165/2014 of the European Parliament and of the Council of 4 February 2014 on tachographs in road transport and amending Regulation (EC) No 561/2006 of the European Parliament and of the Council on the harmonisation of certain social legislation relating to road transport (OJ L 60, 28.2.2014, p. 1.)

- (6) The next meeting of the Group of Experts **on AETR** will take place on **15 October 2018 and the meeting of the Working Party on Road Transport will take place on 16 October 2018**. On that occasion the Group of Experts **and the Working Party** plan to examine proposals made by the Contracting Parties which, if accepted by the Group of Experts, may lead to an amendment of AETR, after a procedure for the revision of AETR is launched and concluded. Once the proposals are accepted by the Group of Experts, as a second step, the Union Member States as Contracting Parties of AETR are under an obligation to cooperate in order to engage the mechanism for the revision of the AETR, in accordance with Council Regulation (EEC) 2829/77¹⁰ and in line with the duty of sincere cooperation pursuant to Article 4(3) TEU, subject to a Council decision in accordance with Article 218(6) as appropriate. The proposed amendments to the AETR will become effective only once the revision of the AETR is completed.
- (7) Regulation (EU) No 165/2014 requires Member States to interconnect their national electronic registers on driver cards through the TACHOnet messaging system or, when using a compatible system, to ensure that exchange of electronic data with all other Member States is possible through the TACHOnet messaging system. TACHOnet is a platform for the exchange of information on driver cards between Member States, in order to ensure that drivers do not hold more than one driver card.
- (8) In order to achieve a pan-European harmonization in the field of electronic exchange of information on driver cards, it is necessary that TACHOnet is used as the single platform by all contracting parties of the AETR.
- (9) The connection to the TACHOnet messaging system is currently carried out either directly through a Trans European Services for Telematics between Administrations ('TESTA') connection or indirectly through a Member State already connected to TESTA. Being TESTA a service which is restricted to Member States and institutions of the Union, non-EU AETR Contracting Parties are obliged to connect to TACHOnet indirectly.
- (10) The Commission has recently assessed the indirect connections to the TACHOnet messaging system and concluded that they do not provide the same level of security as TESTA. In particular, there is not sufficient guarantee about the authenticity, integrity and confidentiality of the information exchanged through indirect connections. Indirect connections to TACHOnet should therefore be replaced by a secure connection.
- (11) eDelivery is a network of connection nodes for digital communications developed by the Commission, where every participant at national level becomes a node using standard transport protocols and security policies. eDelivery is a flexible tool that may be customized to each specific service.
- (12) eDelivery makes use of widely implemented security technologies such as PKI (public key infrastructure), in order to ensure the authenticity, integrity and confidentiality of the information exchanged. Access to TACHOnet of non-EU AETR Contracting Parties should be granted by means of eDelivery.

¹⁰ Council Regulation (EEC) 2829/77 of 12 December 1977 on the bringing into force of the European Agreement concerning the work of crews of vehicles engaged in international road transport (AETR) (OJ L 334, 24.12.1977, p. 11).

- (13) The AETR Contracting Parties should follow a specific procedure to receive the digital certificates and the respective electronic keys granting access to TACHOnet.
- (14) The connection to TACHOnet by means of eDelivery implies that the AETR Contracting Parties are required to ensure that the electronic keys and certificates granting access to the system are protected and cannot be used by non-authorised parties. They should also guarantee that keys covered by certificates having expired are not used anymore.
- (15) It is necessary to guarantee the protection of personal data available to the parties through TACHOnet in accordance with the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 21 January 1981.
- (16) National authorities connected to TACHOnet have the obligation to carry out the relevant technical implementations in order to ensure that TACHOnet operates according to high levels of performance. It is the task of the Commission to set up the tests confirming that those levels of performance are achieved and to implement them in coordination with the national competent authorities.
- (17) As the European Union is not a Contracting Party to the AETR and its status does not allow it to communicate the proposed amendments, Member States, acting in the interest of the Union, should communicate the proposed amendments to the Group of Experts in the spirit of loyal cooperation in order to promote the achievement of the Union's objectives,
- (18) The Union's position is to be expressed by the Member States of the Union that are members of the Group of Experts of the AETR and of the Working Party on Road Transport, acting jointly,

HAS ADOPTED THIS DECISION:

Article 1

The position to be taken on the Union's behalf in the 15th session of the Group of Experts of the European agreement concerning the work of crews of vehicles engaged in international road transport (AETR) shall be in favour of the proposed amendments to the AETR as set out in the document attached to this Decision

Article 2

The position referred to in Article 1 shall be expressed by the Member States of the Union that are members of the AETR, acting jointly.

Formal and minor changes to the position referred to in Article 1 may be agreed without requiring that position to be amended.

Article 3

This Decision is addressed to the Member States.

Done at Brussels,

*For the Council
The President*



Brussels, 2.10.2018
COM(2018) 664 final

ANNEX

ANNEX

to the Proposal for a

COUNCIL DECISION

**on the position to be taken on behalf of the European Union in the Group of Experts on
the European Agreement concerning the work of crews of vehicles engaged in
international road transport of the United Nations Economic Commission for Europe**

Appendix 4

TACHOnet specifications

1. Scope and purpose
 - 1.1. This appendix sets out the terms and conditions regarding the connection of AETR Contracting Parties to TACHOnet through eDelivery.
 - 1.2. Contracting Parties connecting to TACHOnet through eDelivery shall abide by the provisions laid down in this Appendix.
2. Definitions
 - (a) ‘Contracting party’ or ‘party’ means any Contracting party to the AETR;
 - (b) ‘eDelivery’ means the service developed by the European Commission making possible to transmit data between third parties by electronic means, providing evidence relating to the handling of the transmitted data, including proof of sending and receiving the data, and protecting transmitted data against the risk of any unauthorised alteration;
 - (c) ‘TACHOnet’ means the system for the electronic exchange of information on driver cards between contracting parties referred to in Article 31(2) of Regulation (EU) No 165/2014;
 - (d) ‘Central hub’ means the information system enabling the routing of TACHOnet messages between requesting and responding parties;
 - (e) ‘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;
 - (f) ‘Responding party’ means the contracting party to whom the TACHOnet request or notification is addressed;
 - (g) ‘Card issuing authority’ or ‘CIA’ means the entity empowered by a contracting party for the issuing and management of tachograph cards.
3. General responsibilities
 - 3.1. Neither contracting party may conclude agreements for the access to TACHOnet on behalf of another party or in any other way represent the other contracting party on the basis of this Appendix. Neither contracting party acts as the other contracting party’s subcontractor in the operations referred to in this Appendix.
 - 3.2. The contracting parties shall provide access to their national register on driver cards through TACHOnet, in the way and with the level of service set out in Sub-appendix 4.6.
 - 3.3. The contracting 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.
 - 3.4. Each party shall designate contact persons for TACHOnet to the AETR Secretariat. Any change in contact points must be provided to the AETR Secretariat in writing.
4. Tests for connection to TACHOnet

- 4.1. 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.
- 4.2. 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.
- 4.3. The maximum duration of the preliminary tests shall be six months.
5. Trust architecture
- 5.1. Confidentiality, integrity and non-repudiation of the TACHOnet messages shall be ensured by the TACHOnet trust architecture.
- 5.2. The TACHOnet trust architecture shall be based on a public key infrastructure (PKI) service set up by the European Commission, whose requirements are laid down in Sub-appendices 4.8 and 4.9.
- 5.3. 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 referred to in Sub-appendix 4.1 and for the 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:
 - (i) generate the private keys and the corresponding public keys to be included in the certificates to be generated by the Certification Authority;
 - (ii) request the digital certificates to the Certification Authority;
 - (iii) appoint the Trusted Courier.
- 5.4. The Certification Authority and the Registration Authority shall be appointed by the European Commission.
- 5.5. Any contracting party connecting to TACHOnet must request the issuance of a digital certificate in accordance with Sub-appendix 4.9, in order to sign and encrypt a TACHOnet message.
- 5.6. A certificate may be revoked in accordance with Sub-appendix 4.9.

6. Data protection and confidentiality
 - 6.1. 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).
 - 6.2. 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 agree 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.
7. Costs
 - 7.1. The contracting 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 Appendix.
 - 7.2. The services specified in Sub-appendix 4.1, provided by the central hub, are free of charge.
8. Subcontracting
 - 8.1. The parties may subcontract any of the services for which they are responsible under this Appendix.
 - 8.2. Such subcontracting does not relieve the party from the responsibility pursuant to this Appendix, including the responsibility for the appropriate level of service in accordance with Sub-appendix 4.6.

General aspects of TACHOnet

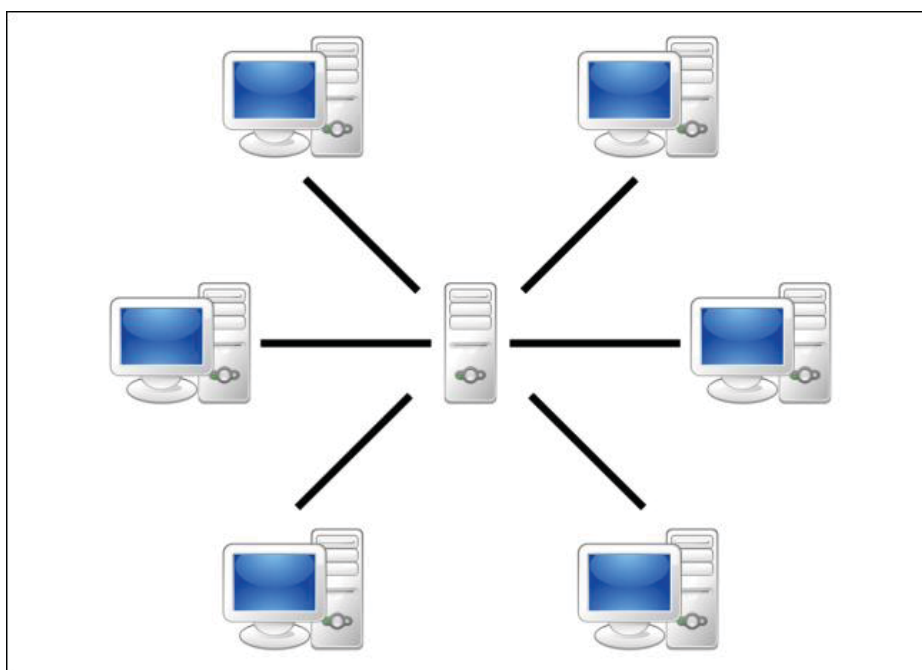
1. General description

TACHOnet is an electronic system for the exchange of information on driver cards between AETR contracting parties. TACHOnet 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:

- 2.1. 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.
- 2.2. 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.
- 3.2. The central hub shall not store data for a period exceeding six months, other than the logging and statistical data set out in Sub-appendix 4.7.

- 3.3. 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.
- 3.4. Each contracting party shall be responsible for:
 - 3.4.1. The setup and management of their national systems, including the interface with the central hub.
 - 3.4.2. The installation and maintenance of their national system, both hardware and software, whether proprietary or commercial.
 - 3.4.3. The correct interoperability of their national system with the central hub, including the management of error messages received from the central hub.
 - 3.4.4. Taking all the measures to ensure the confidentiality, integrity and availability of the information.
 - 3.4.5. The operation of the national systems in accordance with the service levels set out in Sub-appendix 4.6.

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, in order 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 Table 1, 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 Table 1.
5. The card status listed in Table 1 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.

Table 1
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.

Card Status	Definition
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.
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.

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 Sub-appendix 4.2.
 - 2.4. The XML messages shall include at least the minimum requirements laid down in Table 2.

Table 2

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 <i>version</i> 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 central 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

Sub-appendix 4.4

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

Sub-appendix 4.5
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 digital certificates referred to in Sub-appendices 4.8 and 4.9 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.

Sub-appendix 4.6

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.

Sub-appendix 4.7

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.

General provisions regarding digital keys and certificates for TACHOnet

1. The Directorate General for Informatics of the European Commission (DIGIT) shall make available a PKI service¹ (referred to as “CEF PKI service”) to the AETR Contracting Parties connecting to TACHOnet (henceforth the national authorities) through eDelivery.
2. The procedure for request and revocation of digital 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 authority², 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;
 - (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.

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

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.

Description of the PKI service for TACHOnet

1. Introduction

A PKI (Public Key Infrastructure) is a set of roles, policies, procedures and systems needed to create, manage, distribute, and revoke digital certificates³. The CEF PKI service of eDelivery enables issuance and management of digital certificates used to ensure confidentiality, integrity and non-repudiation of the information exchanged between Access Points (AP).

The PKI service of 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 GmbH⁴ apply.

The 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.

2. Certificate Request Process

2.1. Roles and responsibilities

2.1.1. 'Organisation' or 'national authority' requesting the certificate

2.1.1.1. The national authority shall request the certificates in the context of the TACHOnet project.

2.1.1.2. The national authority shall:

- (a) request the certificates from the CEF PKI service;
- (b) generate the private keys and the corresponding public keys to be included in the certificates issued by the Certification Authority;
- (c) download the certificate when approved;
- (d) sign and send back to the Registration Authority:
 - (i) the contact persons and trusted couriers identification form,
 - (ii) the signed individual Power of Attorney⁵.

2.1.2. Trusted Courier

2.1.2.1. The national authority shall appoint a Trusted Courier.

2.1.2.2. The trusted Courier shall:

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/>

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 point 6.

- (a) hand over the public key to the Registration Authority during a face-to-face identification and registration process;
 - (b) get the corresponding certificate from the Registration Authority.
- 2.1.3. Domain Owner
 - 2.1.3.1. DG MOVE shall be the Domain Owner.
 - 2.1.3.2. The Domain Owner shall:
 - (a) validate and coordinate the TACHOnet network and the TACHOnet trust architecture, including the validation of the procedures for the issuance of the certificates;
 - (b) operate the TACHOnet central hub and coordinate the activity of the parties regarding the functioning of TACHOnet;
 - (c) perform, along with national authorities, the tests of connection to TACHOnet.
 - 2.1.4. Registration Authority
 - 2.1.4.1. The Joint Research Centre (JRC) shall be the Registration Authority.
 - 2.1.4.2. The Registration Authority shall be responsible for verifying the identity of the trusted courier, for registering and approving the requests of issuance, revocation and renewal of digital certificates.
 - 2.1.4.3. The registration authority shall:
 - (a) assign the unique identifier to the national authority;
 - (b) authenticate the identity of the national authority, its contact points and trusted couriers;
 - (c) communicate with the CEF Support regarding the authenticity of the national authority, its contact points and trusted couriers;
 - (d) inform the national authority about the approval or rejection of certificate.
 - 2.1.5. Certification Authority
 - 2.1.5.1. The Certification Authority shall be responsible for the provision of the technical infrastructure for the request, issuing and revocation of digital certificates.
 - 2.1.5.2. The Certification Authority shall:
 - (a) provide for the technical infrastructure for certificate requests by national authorities;
 - (b) validate or reject certificate request;
 - (c) communicate with the Registration Authority for the identity verification of the requesting organisation, when required.
 - 2.2. Certificate issuance
 - 2.2.1. The certificate issuance shall be carried out in accordance with the following sequential steps, represented in figure 1:
 - (a) **Step 1:** Trusted courier identification;
 - (b) **Step 2:** Certificate request creation;
 - (c) **Step 3:** Registration at RA;

- (d) **Step 4:** Certificate generation;
- (e) **Step 5:** Certificate publication;
- (f) **Step 6:** Certificate acceptance.

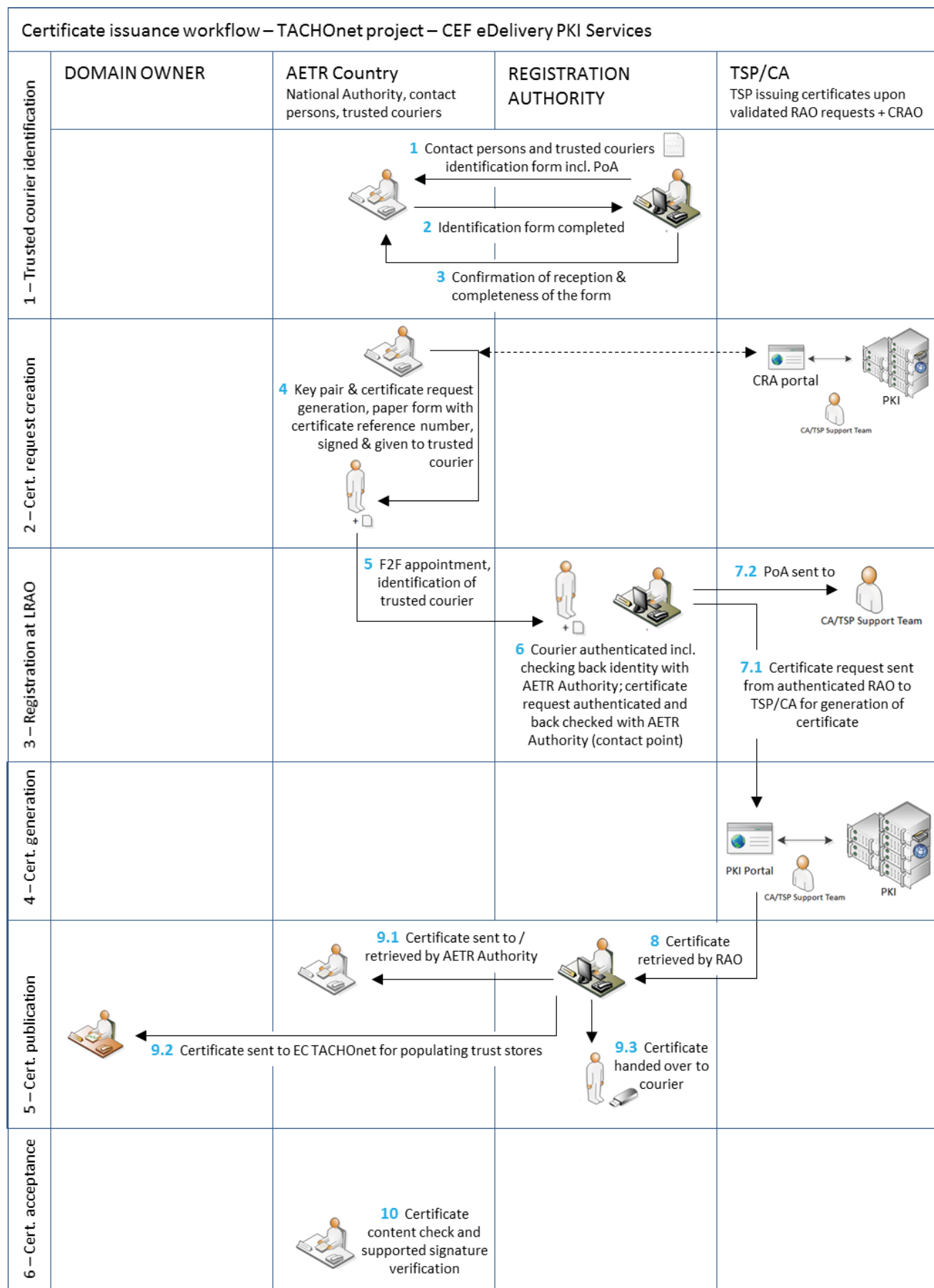


Figure 1 - Certificate issuance workflow

2.2.2. Step 1: Trusted Courier identification

The following process shall be carried out for the Trusted Courier identification:

- (a) The Registration Authority shall send to the national authority the contact persons and trusted couriers' identification form⁶. This form shall also include a power of attorney (PoA) that the organisation (AETR Authority) shall sign.
- (b) The national authority shall send back the completed form and signed PoA to the Registration Authority.
- (c) The Registration Authority shall acknowledge the good reception and completeness of the form.
- (d) The Registration Authority shall provide an updated copy of the list of contact persons and trusted couriers to the domain owner.

2.2.3. Step 2: Certificate request creation

2.2.3.1. The request and the retrieval of the certificate shall be done on the same computer and with the same browser.

2.2.3.2. The following process shall be carried out for the certificate request creation:

- (a) The Organisation shall navigate to the user web interface to request the certificate via the URL <https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en:> , and shall enter the username '**sbca/CEF_eDelivery.europa.eu**' and the password '**digit.333**'

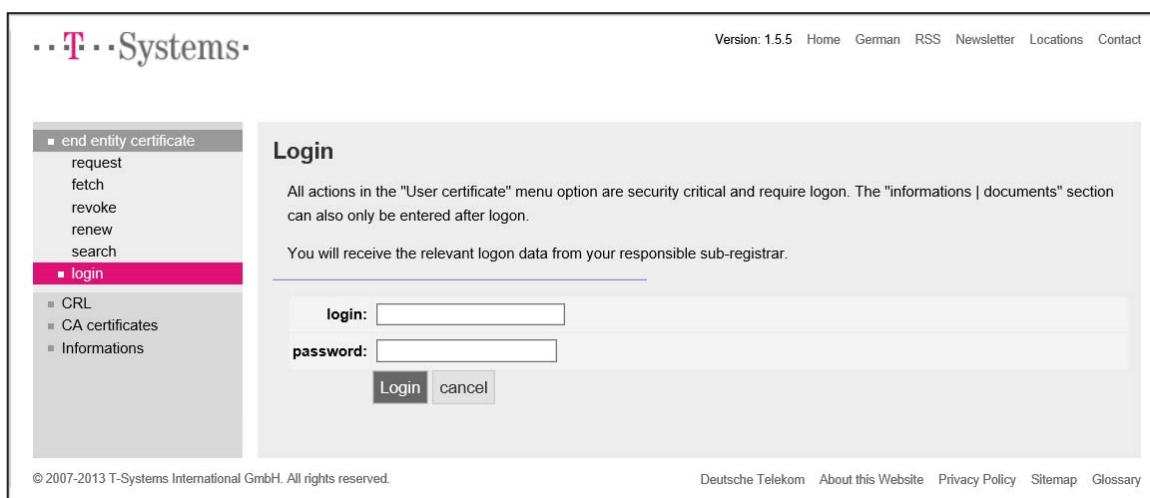


Figure 2

- (b) The Organisation shall click on 'request' on the left side of the panel and shall select 'CEF_TACHOnet' in the dropdown list.

⁶

See point 5

Figure 3

- (c) The Organisation shall populate the certificate request form lied down in figure 4 with the information in Table 3, clicking on 'Next (soft-PSE)' to finish the process.

Figure 4

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

Table 3. Complete details of each requested field

(d) The selected key length shall be 2048(High Grade).

Version: 1.7.14 Home German RSS Newsletter Locations Contact

Login at: CEF_eDelivery.europa.eu

• End entity certificate
• request
 fetch
 revoke
 renew
 search
 logout

• CRL
• CA certificates
• Information

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)

Request Cancel

© 2007-2010 T-Systems International GmbH. All rights reserved. Deutsche Telekom About this Website Privacy Policy Sitemap Glossary

Figure 5

- (e) The Organisation shall record the reference number to retrieve the certificate.

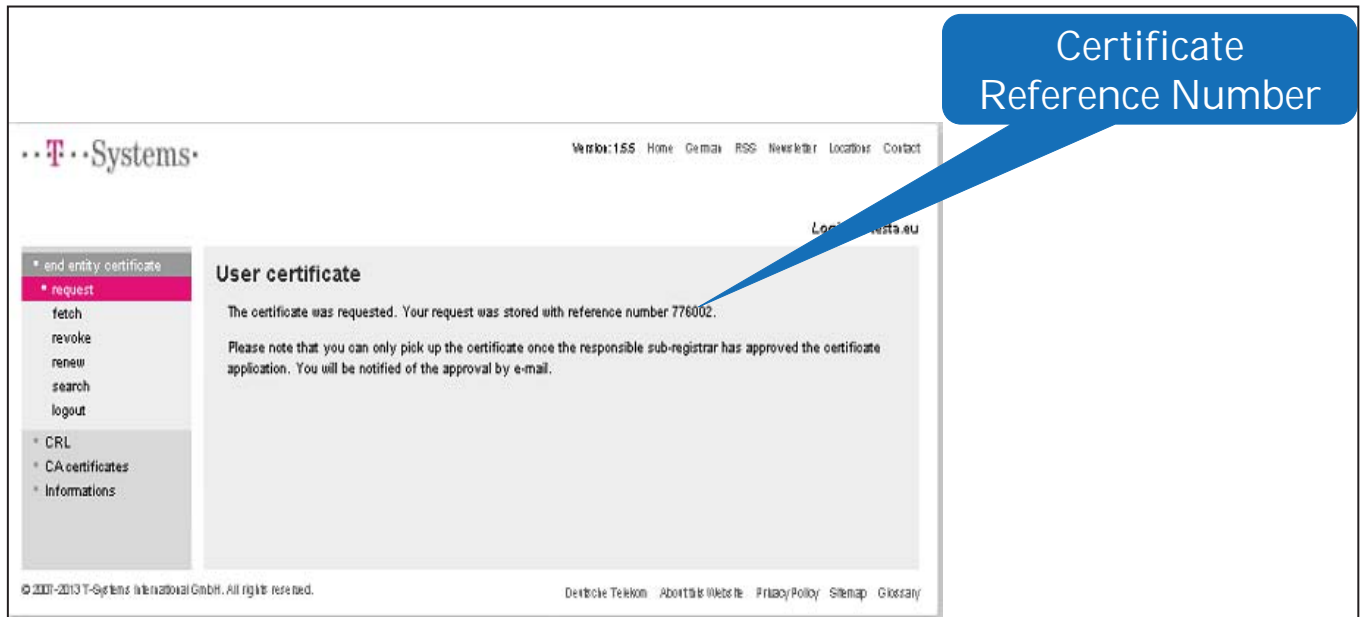


Figure 6

- (f) The CEF Support Team shall check for new requests of certificates and verify if the information in the certificate request is valid, i.e. that it conforms to the naming convention specified in Appendix 5.1 Certificate Naming Convention.
- (g) The CEF Support Team shall verify that the information entered in the request is in a valid format.
- (h) When either check from points 5 or 6 above fails, the CEF Support Team shall send 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 shall be cancelled.
- (i) The CEF Support Team shall send an email to the Registration Authority about the validity of the request. The email shall include:
- (1) the name of the Organisation, available in the field “Organisation (O)” of the certificate request;
 - (2) the certificate data 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;
 - (3) the certificate reference number;
 - (4) the address of the Organisation, its email and the name of the person representing it.

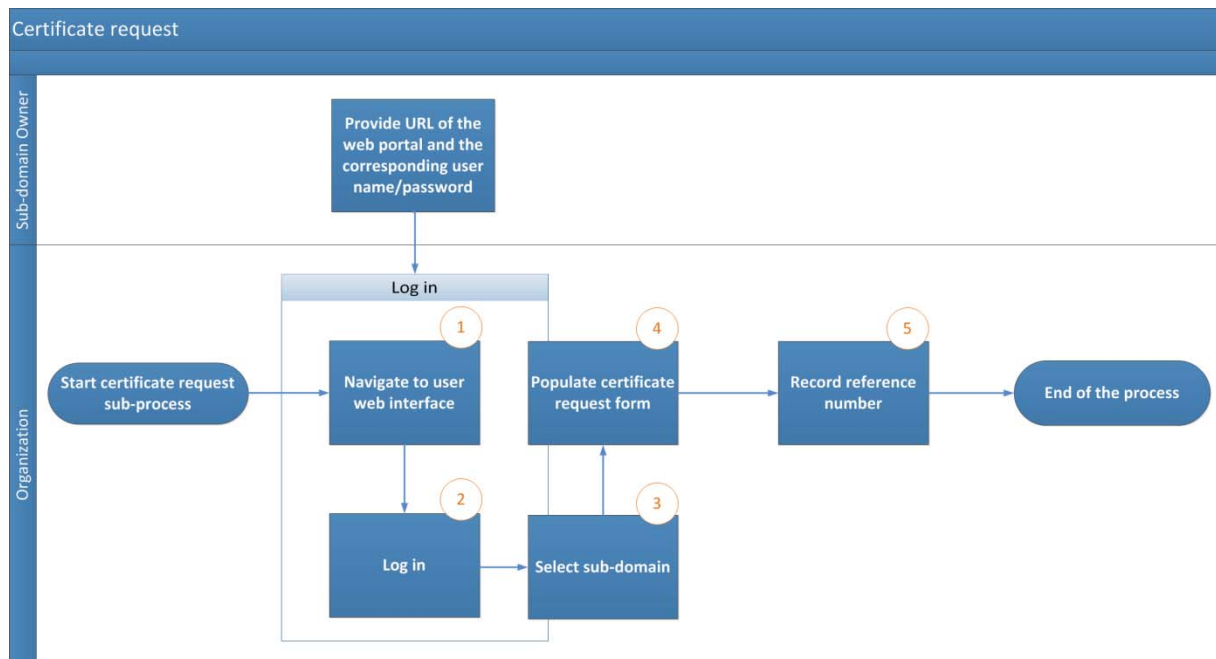


Figure 7 – Certificate request process

2.2.4. Step 3: Registration at Registration Authority (Certificate approval)

2.2.4.1. The Trusted Courier or contact point shall make an appointment with the Registration Authority via email exchange, identifying the Trusted Courier who will proceed to the face-to-face meeting.

2.2.4.2. The Organisation shall prepare the documentary package consisting in:

- (a) the filled-in and signed power of attorney;
- (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 signed by one of the points of contact of the Organisation.

2.2.4.3. The Registration Authority shall receive the Trusted Courier after identity screening at the building reception. The Registration Authority shall conduct the face-to-face registration of the certificate request by:

- (a) identifying and authenticating the Trusted Courier;
- (b) verifying the trusted courier physical appearance against the passport presented by the Trusted Courier;
- (c) verifying the validity of the passport presented by the Trusted Courier;
- (d) 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 identified points of contact of the Organisation. Signature is authenticated against the original “trusted courier and contact points identification form”;
- (e) verifying the filled-in and signed power of attorney;
- (f) verifying certificate request paper form and its signature against the original “trusted courier and contact points identification form”;

- (g) calling the signatory contact point to double check the identity of the trusted courier and the content of the certificate request.
- 2.2.4.4. The Registration Authority shall confirm to the CEF Support Team that the national authority 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 shall be sent using a "CommiSign" certificate secure email, attaching a scanned copy of the authenticated face-to-face documentary package and of the signed process check list carried out by the Registration Authority.
- 2.2.4.5. If the Registration Authority confirms the validity of the request, the process shall carry on as set out in 2.2.4.6 and 2.2.4.7. Otherwise the certificate issuance shall be rejected and the Organisation shall be informed.
- 2.2.4.6. The CEF Support Team shall approve the certificate request and shall notify the Registration Authority the approval of the certificate.
- 2.2.4.7. The Registration Authority shall notify the Organisation that the certificate can be retrieved via the user portal.

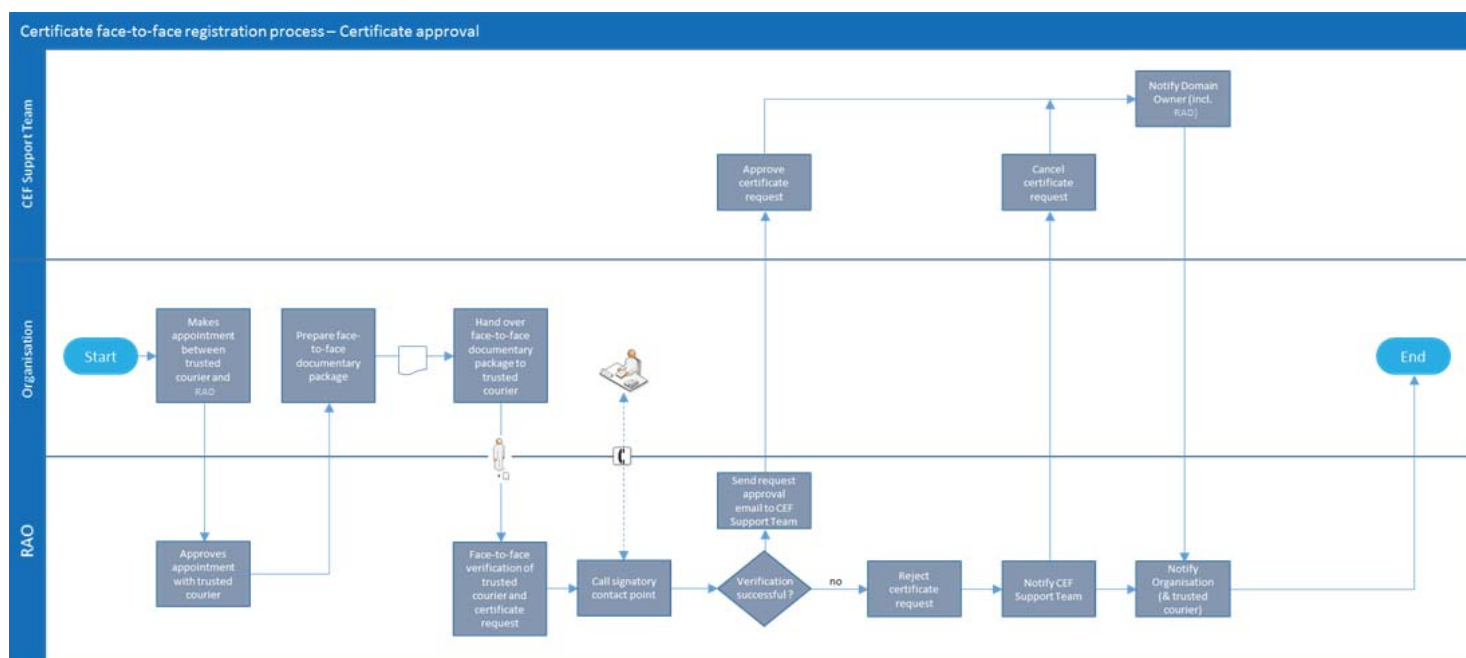


Figure 8 - Certificate approval

- 2.2.5. Step 4: Certificate generation
- Upon approval of the certificate request, the certificate shall be generated.
- 2.2.6. Step 5: Certificate publication and retrieval
- 2.2.6.1. Following approval of the certificate request, the Registration Authority shall retrieve the certificate and hand over a copy to the Trusted Courier.
- 2.2.6.2. The Organisation shall receive the notification from the Registration Authority that the certificates can be retrieved.
- 2.2.6.3. The Organisation shall navigate to the user portal at <https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en> and shall log in with the username "sbca/CEF_eDelivery.europa.eu" and the password "digit.333".

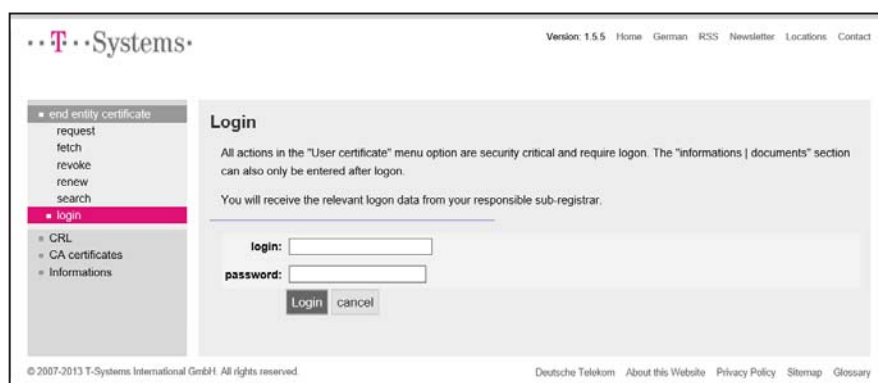


Figure 9

2.2.6.4. The Organisation shall click on the “fetch” button on the left-hand side and shall provide the reference number recorded during the certificate request process;



Figure 10

2.2.6.5. The Organisation shall install the certificates by clicking on the install button;

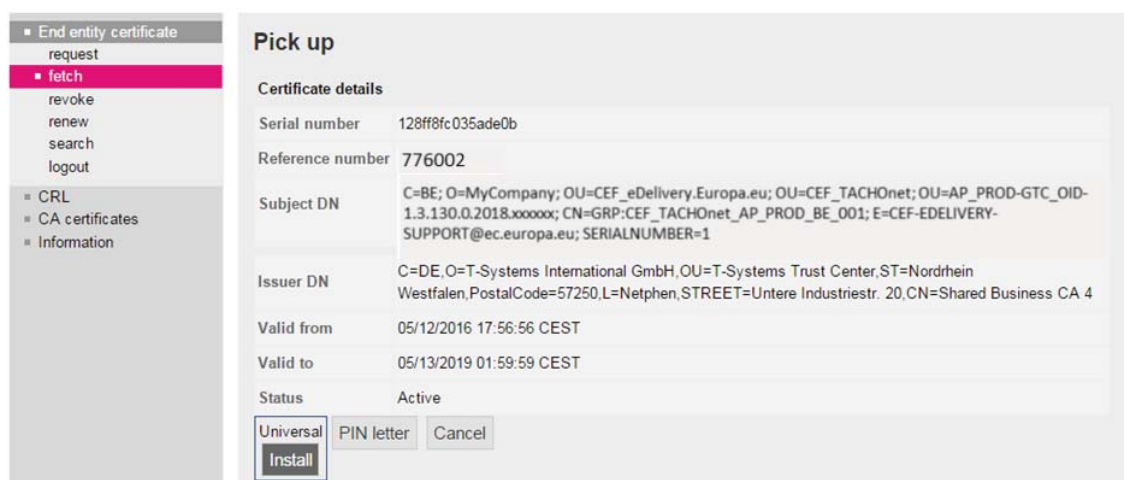


Figure 11

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

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

- (a) export the private key and the certificate,

- (b) create the keystore and the truststore,
- (c) install the keystore and the truststore on the access point.

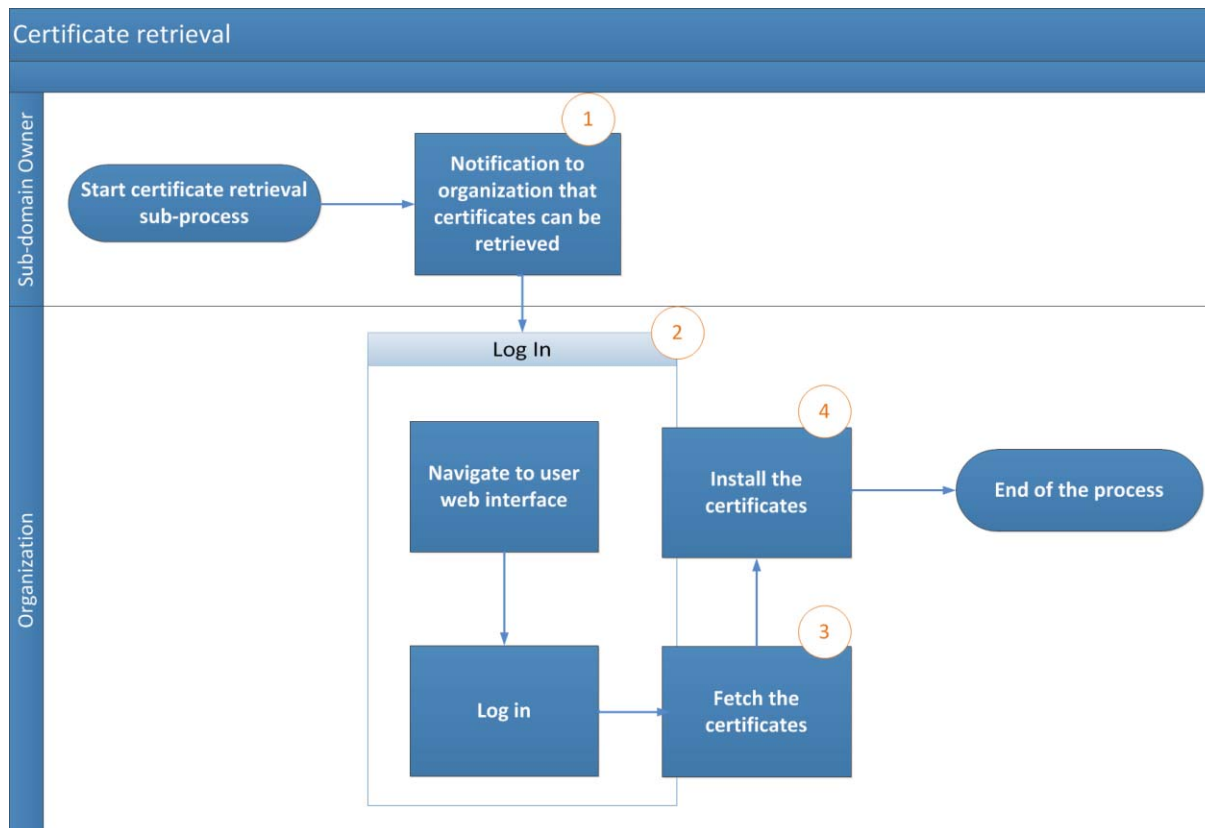


Figure 12 - Certificate retrieval

- 3. Certificate revocation process
 - 3.1. The Organization shall submit a revocation request through the user web portal;
 - 3.2. The CEF Support Team shall execute the certificate revocation.

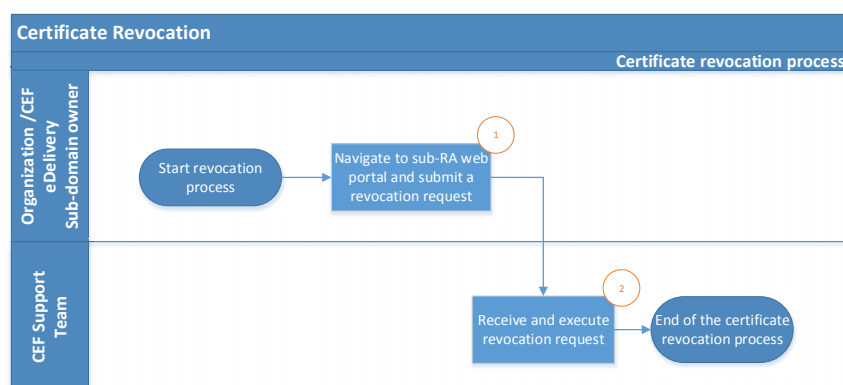


Figure 13 - Certificate revocation

- 4. General Terms and conditions of the CEF PKI service
 - 4.1. Context

In its capacity as Solution Provider of the eDelivery Building Block of the Connecting Europe Facility, DIGIT shall make available a PKI service⁷ ('CEF PKI service') to the AETR Contracting Parties. The CEF PKI service shall be used by national authorities ('end-Users') participating in TACHOnet.

DIGIT is a PKI tenant within the TeleSec Shared-Business-CA solution ('SBCA') operated in the Trust Center of the Group unit T-Systems International GmbH ('T-Systems'⁸). 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 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.

4.2. 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.

4.3. Authorised /prohibited uses of certificates

4.3.1. Permitted usage of certificates

Once the certificate is issued, the certificate owner⁹ shall use the certificate only in the context of TACHOnet. Within this context, the certificate can be used to:

- authenticate the origin of data;
- encrypt data;
- ensure detection of integrity breaches of data.

4.3.2. Prohibited usage of certificates

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

4.4. 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 service¹⁰.

⁷ A PKI (Public Key Infrastructure) is a set of roles, policies, procedures and systems needed to create, manage, distribute, and revoke digital certificates.

⁸ The trusted role of the Trust Center operator, located in the T-Systems Trust Center, also performs the task of internal registration authority.

⁹ Identified by the "O=" attribute value in the Subject Distinguished Name of the issued certificate

¹⁰ The latest version of the T-Systems SBCA CP/CPS is available from <https://www.telesec.de/en/sbca-en/support/download-area/>.

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.

Only entities authorised to participate TACHOnet can request a certificate.

Regarding certificate acceptance, clause 4.4.1 of the SBCA Certificate Policy and Certification Practice Statement ('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 shall comply with the following requirements:

- (1) protect their private key against unauthorized use;
- (2) refrain from transferring or revealing their private key to third parties, even as representatives.
- (3) 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).
- (4) the certificate owner is responsible for copying or forwarding the key to the end entity or entities.
- (5) 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.
- (6) The 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.
- (7) 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 the employment relationship), the certificate owner must prevent misuse of the private key by revoking the certificate.
- (8) The certificate owner is responsible and shall request revocation of the certificate under the circumstances referred to 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. Contact persons and trusted couriers identification form (sample)

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:

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:

Place, date, company stamp or seal of the Organisation:**Signature of the authorised representative:**

6. Documents

6.1. 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 FERIAI**

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

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

- ☒ user¹: e.g. mail security (signature, encryption), virtual private network (VPN), TLS/SSL client
- ☐ server²: e.g. identity of web server, TLS/SSL client server authentication
Please enter additionally the country, organization, locality, state or province name of the server:
-
- ☐ eMail-Gateway³: e.g. identity of eMail gateways / eMail-Appliance, virtual mail-administrating centre.

Validity

- ☒ The power of attorney is valid until further notice, but up to a **maximum of 27 months²** or **maximum of 36 months^{1,3}** from date of issuance.
- ☐ The power of attorney is valid until _____ (mm.dd.yyyy), but up to a **maximum of 27 month²** months or **maximum of 36 months^{1,3}** from date of issuance.

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

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

Signature of the authorized representative

6.2. 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:

7. Glossary

The key terms used in this Sub-appendix 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>