EUROPEAN COMMISSION

DIGIT | DG CNECT
Connecting Europe Facility

CEF eDelivery Building Block

Version 1.2

Trust Models Guidance

Document Status:

Status
Final

Document Approver(s):

Name	Role
Joao Rodrigues Frade	CEF eDelivery Project and Architecture Office

Document Reviewer(s):

Name	Role
Olivier Delos	SEALED
Pim van der Ejik	Sonnenglanz Consulting BV

Summary of Changes:

Version	Date	Created by	Short Description of Changes
1.2	2018-05-25	CEF eDelivery	Document finalisation

Table of Contents

Contents

1. Approach and purpose of the document

This document aims to help businesses and public administrations (hereafter denoted as ‘organisations’) to make an informed decision on the trust model to operate when using the CEF eDelivery Building Block. To support this decision, this document describes the trust models that organisations can choose when implementing the CEF eDelivery components. This document assumes that readers are familiar with the CEF eDelivery components and the generic messaging use case. If not, readers can become familiar with these topics by consulting the CEF Digital website. Within the context of the messaging use case, the CEF eDelivery components rely on a trust model to establish a secure and trusted communication with one another.

1.1. Understanding the concept

[Key Definition] A **trust model** is a collection of rules that ensure the legitimacy of the digital certificates used by the CEF eDelivery components. Digital certificates enable the identification of the organisations using eDelivery and are instrumental for the authenticity, confidentiality, integrity and non-repudiation of the information. Different trust models are available based on different trust anchor models and different rules to create, manage, distribute, store and revoke the digital certificates.

[Key Definition] A **trust anchor** represents an authoritative entity via a public key and associated data. The public key is used to verify digital signatures, and the associated data is used to constrain the types of information for which the trust anchor is authoritative. A relying party uses trust anchors to determine if a digitally signed object is valid by verifying a digital signature using the trust anchor's public key, and by enforcing the constraints expressed in the associated data for the trust anchor.
Source: Internet Engineering Task Force (IETF) | Trust Anchor Management Requirements

This document considers four alternative trust models that can be used in any implementation of CEF eDelivery:

- **Dedicated Domain PKI**: in this model, digital certificates are associated to a single trust anchor. In this case, the trust anchor serves a single domain i.e. it is a dedicated anchor.

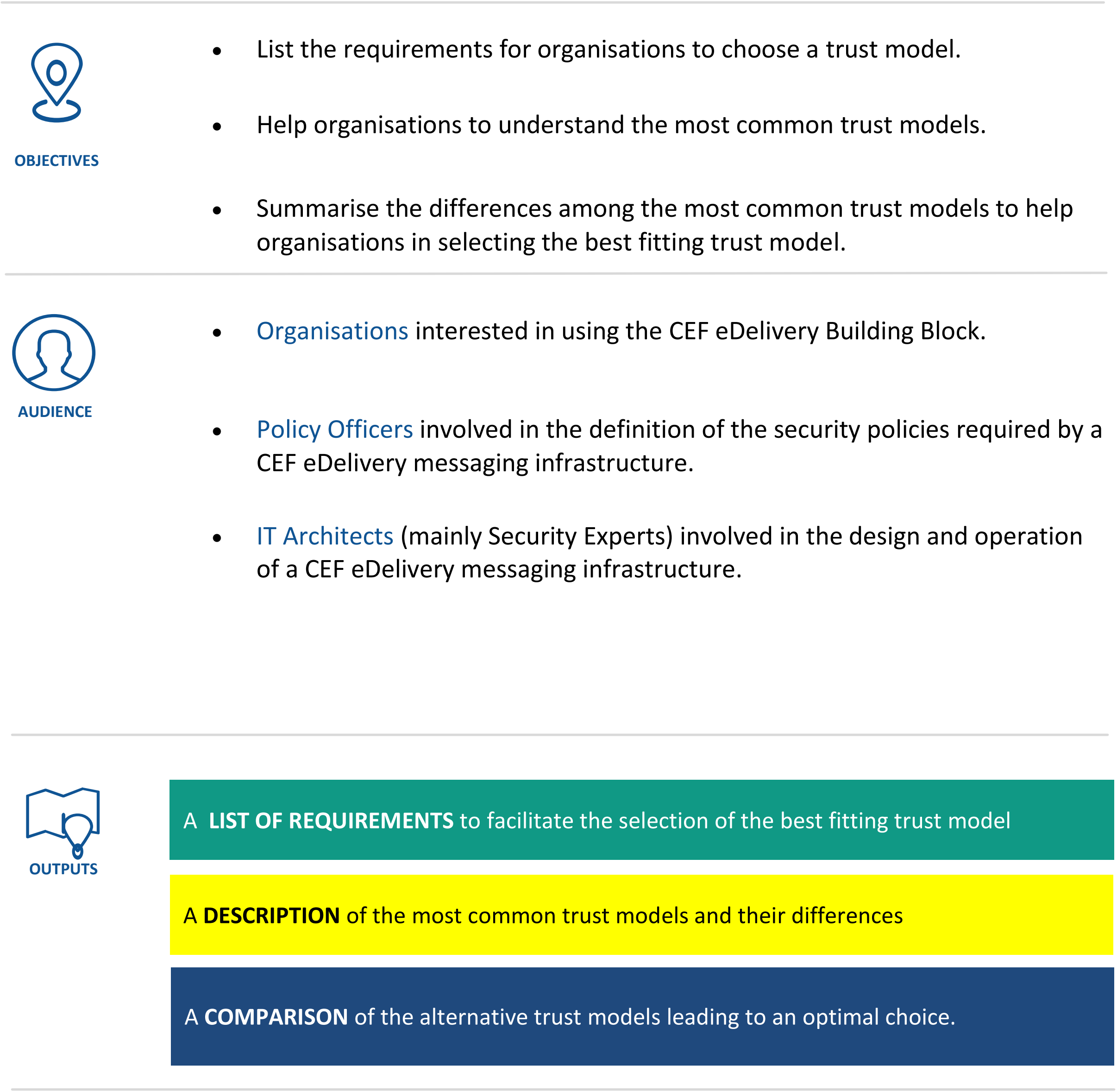
- **Shared Domain PKI**: in this model, digital certificates are associated to a single trust anchor. In this case, the trust anchor serves multiple domains i.e. it is a shared anchor.

- **Mutual exchange**: this model relies on digital certificates from different trust anchors. As there is no single trust anchor, organisations use the trust anchor of their choice (typically, according a set of well-defined criteria).

- **Domain trusted lists**: this model relies on a list containing the trusted certificates and/or trust anchors complying with a common domain policy. As a result, organisations are free to choose their preferred trust anchor from that list.

To facilitate the choice of the best fitting trust model, this document lists general requirements, faced by organisations interested in using the CEF eDelivery Building Block. The assessment of the different trust models is based on expert opinion and industry good practises.

The figure below summarises the objectives, audience and outputs of this document.



OBJECTIVES

- List the requirements for organisations to choose a trust model.
- Help organisations to understand the most common trust models.
- Summarise the differences among the most common trust models to help organisations in selecting the best fitting trust model.

AUDIENCE

- Organisations interested in using the CEF eDelivery Building Block.
- Policy Officers involved in the definition of the security policies required by a CEF eDelivery messaging infrastructure.
- IT Architects (mainly Security Experts) involved in the design and operation of a CEF eDelivery messaging infrastructure.

OUTPUTS

A **LIST OF REQUIREMENTS** to facilitate the selection of the best fitting trust model

A **DESCRIPTION** of the most common trust models and their differences

A **COMPARISON** of the alternative trust models leading to an optimal choice.

Figure 1. Summary of the objectives, audience and outputs of this document

2. GLOSSARY

The key terms used in this **document** are defined in Table 1. The key acronyms used in the eDelivery Building Block are defined in the CEF Glossary on the CEF Digital website:

Table 1. Security controls and recommendations key terms

Term	Description
Access Point	The Access Point (AP) is a key component of the CEF eDelivery building block. The CEF eDelivery AP implements the AS4 message exchange protocol according to the eDelivery profile [1]. This protocol ensures standardised, interoperable, secure and reliable data exchange. For more information, please refer to the CEF Digital Portal [2].
AS4	The eDelivery AS4 profile is the AS4 Usage Profile/ implementation guidelines defined by e-SENS based on the AS4 specification of OASIS, itself a profile of OASIS ebXML Messaging Services Version 3.0, which in turn is based on various Web Services specifications of OASIS.
Backend system	In the context of eDelivery, the Backend systems represent the IT systems used by the business and public administrations, which are the origin of the documents and data to be exchanged through eDelivery. In order to do so, Backend systems must be connected to an eDelivery Access Point, directly or through a connector component.
Certificate Authority (CA)	The Certificate Authority (CA) represents the entity that electronically seals the certificates, issues certificates, validates identities and manages a certificate revocation lists. The Certificate Authority operations are specified and performed by TSPs and QTSPs for qualified certificates.
CEF eDelivery	The eDelivery building block helps public administrations to exchange electronic data and documents with other public administrations, businesses and citizens, in an interoperable, secure, reliable and trusted way.
(digital) Certificate	A (digital) certificate provides an attestation that makes it possible to authenticate and link natural and legal person identities. According to the eIDAS Regulation (Article 3) there are three types of certificates: • Certificate for electronic signature (Article 3(14)): means an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person; • Certificate for electronic seal (Article 3(29)): means an electronic attestation that links electronic seal validation data to a legal person and confirms the name of that person; • Certificate for website authentication (Article 3(38)): means an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the certificate is issued. A qualified certificate is required to be issued by a Qualified TSP.
Dedicated Domain PKI	Dedicated Domain PKI is a trust model following a hierarchical trust based on a common trust anchor used by all digital certificates of the CEF eDelivery components in the network.

Domain	Domains are typically linked to the Directorate-Generals of the European Commission, e.g. DG Justice and DG SANTE that are the organisations of domains such as the eJustice domain and eHealth domain respectively. Policy domains use eDelivery to create a secure messaging infrastructure for the exchange of data and documents.
eIDAS Regulation	The eIDAS Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market provides a predictable regulatory environment to enable secure and seamless electronic interactions between businesses, citizens and public authorities. [3]
Mutual exchange	Mutual exchange trust is a trust model based on the direct mutual exchange of digital certificates between the CEF eDelivery components.
Organisation	Every legal person acting as service provider or using one of the CEF eDelivery components. In the context of this document, organisation refers to businesses and public administrations that benefit from one or more Access Points (AP) in a given policy domain. They typically use eDelivery to create a secure messaging infrastructure for the exchange of data and documents within their domain.
Organizational Unit (OU)	The organizational unit (OU) represents a relative distinguished name identifying an entry with a unique name in the digital certificate path hierarchy. The OU is usually under the common name of the root by representing a type of group. In the context of this document, the organizational unit represents the domain and sub-domains under a business domain owner. For instance, all the certificates of the domain eHealth will be under the OU eHealth. The OU is part of the certificate attributes and is used to filter the domains.
PEPPOL	Pan European Public Procurement On-Line (PEPPOL) is a European platform composed of a set of artefacts and specifications enabling cross-border eProcurement. OpenPEPPOL AISBL (Association Internationale Sans But Lucratif) now maintains PEPPOL.
Public Key Infrastructure (PKI)	Public Key Infrastructure (PKI) denote systems, software, and communication protocols that are used by a TSP to distribute, manage and control public key cryptography based certificates. A PKI publishes digital certificates and establishes trust within an environment by validating and verifying the public keys mapping to an entity.
Public Administration	According to the eIDAS Regulation a Public Administration means a state, a regional or local authority, a body governed by public law or an association formed by one or several such authorities or one or several bodies governed by public law, or a private entity mandated by at least one of those authorities, bodies or associations to provide public services, when acting under such a mandate.
Qualified certificate (QC)	Qualified (digital) certificate is a certificate issued by a Qualified TSP. According to the eIDAS Regulation (Article 3) the three types of certificates are considered to be qualified by meeting their specific requirements as follows: • Qualified certificate for electronic signature (Article 3(15)): means a certificate for electronic signatures, that is issued by a qualified trust service provider and meets the requirements laid down in Annex I of the regulation; • Qualified certificate for electronic seal (Article 3(30)): means a certificate for an electronic seal, that is issued by a qualified trust service provider and meets the requirements laid down in Annex III of the regulation;

	• Qualified certificate for website authentication (Article 3(39)): means a certificate for website authentication, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV of the regulation.
Qualified Trust Service (QTS)	A Qualified Trust Service means a trust service that meets the applicable requirements laid down in the eIDAS Regulation (Article 4(17)). The qualified status is applicable to the nine different trust services described in the Trust Service definition.
Qualified Trust Service Provider (QTSP)	A Qualified TSP means a trust service provider who provides one or more qualified trust services and is granted the qualified status by the supervisory body.
Registration authority (RA)	The Registration Authority (RA) manages the registration function at the end entity towards one or multiple TSPs. The RA performs identification, authentication and subscription of certificate applicants to then inform and request to the TSP its issuance. The RA plays a central role as part of a PKI by establishing a chain of trust and creating a closed user group within the controlling entity, and ensuring that the TSP receives correctly all the required information.
Service Metadata Locator (SML)	The Service Metadata Locator (SML) is a centralised component that stores a list holding the location of SMPs. The SML has the information that links the message exchange APs to their respective SMP.
Service Metadata Publishers (SMP)	The Service Metadata Publisher (SMP) provides the service location and capabilities of APs, by storing, exchanging and performing capability lookups for other APs. The SMPs are associated to APs and operate in a distributed manner in the CEF eDelivery network. The SMP obtains the service location of other SMPs via the Service Metadata Locator (SML).
Shared Domain PKI	Shared Domain PKI is a trust model that follows a hierarchical trust based on a common shared trust anchor used by all the digital certificates within the CEF eDelivery components.
TLS	Transport Layer Security (TLS) defines security for the protocols that are responsible to transparently transfer data between end systems, or hosts, ensuring a complete data transfer from host to host communication.
Trust	Trust is the characteristic that one organisation is willing to rely upon a second entity to execute a set of actions and/or to make a set of assertions about a set of subjects and/or scopes [4].
Trust anchor	Trust anchor is a core concept within PKI denoting the digital certificate of an entity for which trust is assumed. Trust anchor is required for the validation of the digital certificate trust path between parties.
Trust Establishment	Trust Establishment is the act required to achieve trust via digital certificates in order to initiate the message exchange between CEF eDelivery components.
Trusted list	A trusted list represents a repository containing a set of digital certificates complying with a common policy. Trusted lists can be specific to a domain, relying on a domain specific policy. The eIDAS Regulation (Article 22) formalised the concept of EU Trusted lists, providing the legal basis and mandates to use Trusted Lists for mutual recognition and acceptance at EU level. The EU Trusted Lists are important tools for obtaining the list of trust services with qualified status in the European domain.

Trust Model

A trust model is a collection of rules that ensure the legitimacy of the digital certificates used by the CEF eDelivery components. Digital certificates enable the identification of the organisations using eDelivery and are instrumental for the confidentiality, integrity and non-repudiation of the information exchange. Different trust models are available based on different trust anchors, reflecting different rules to create, manage, distribute, store and revoke the digital certificates to be used in the different CEF eDelivery components.

Trust Service

According to Article 3(16) of the eIDAS Regulation a trust service means an electronic service normally provided for remuneration which consists of:

- the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services; or
- the creation, verification and validation of certificates for website authentication; or
- the preservation of electronic signatures, seals or certificates related to those services.

Trust Service Provider (TSP)

According to Article 3(19) of the eIDAS Regulation, a TSP means a natural or a legal person who provides one or more trust services either as a qualified or as a non-qualified.

3. REFERENCES

[1] “eDelivery AS4 Profile,” [Online]. Available: https://ec.europa.eu/cefdigital/wiki/x/AwFfAQ.

[2] “CEF eDelivery Access Point,” [Online]. Available: https://ec.europa.eu/cefdigital/wiki/x/_wBfAQ.

[3] “eIDAS Regulation (EU) No 910/2014,” [Online]. Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG.

[4] “OASIS Trust,” [Online]. Available: http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/ws-trust.html.

[5] “CEF eDelivery PKI Service,” [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/PKI+Service.

[6] “CEF eDelivery Security Controls,” [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Security+Controls+guidance.

[7] OASIS, “ebCore Agreement Update Specification Version 1.0,” [Online]. Available: http://docs.oasis-open.org/ebcore/ebcore-au/v1.0/ebcore-au-v1.0.html.

[8] IETF, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practises Framework,” [Online]. Available: https://www.ietf.org/rfc/rfc2527.txt.

[9] “ETSI Trusted Lists,” [Online]. Available: http://www.etsi.org/deliver/etsi_ts/119600_119699/119612/01.01.01_60/ts_119612v010101p.pdf.

4. Introduction

The eDelivery building block of the Connecting Europe Facility (CEF) enables businesses and public administrations (both hereafter referred to as 'organisations') to exchange electronic data and documents in an interoperable, secure, reliable and trusted way. Trust models regulate the use of digital certificates to ensure trust between CEF eDelivery components and organisations.

4.1. Context

Most eDelivery messaging infrastructures implement a simple messaging topology known as the four-corner model. This is illustrated in the figure below. This means that the original sender and final recipient rely on the components of the CEF eDelivery Building Block to exchange messages in a secure and trusted manner according to a set of security controls [6]. Most of these controls rely on digital certificates. The lifecycle of these certificates is regulated by a trust model. As a result, trust models are an essential element of every messaging infrastructure based on the CEF eDelivery Building Block. In essence, each trust model defines the permissible trust anchors of the digital certificates used in an eDelivery messaging infrastructure. The models apply to the exchange of information between Access Points (AP) and, when using dynamic discovery, to the interactions with Service Metadata Publishers (SMP) and also with the Service Metadata Locator (SML).

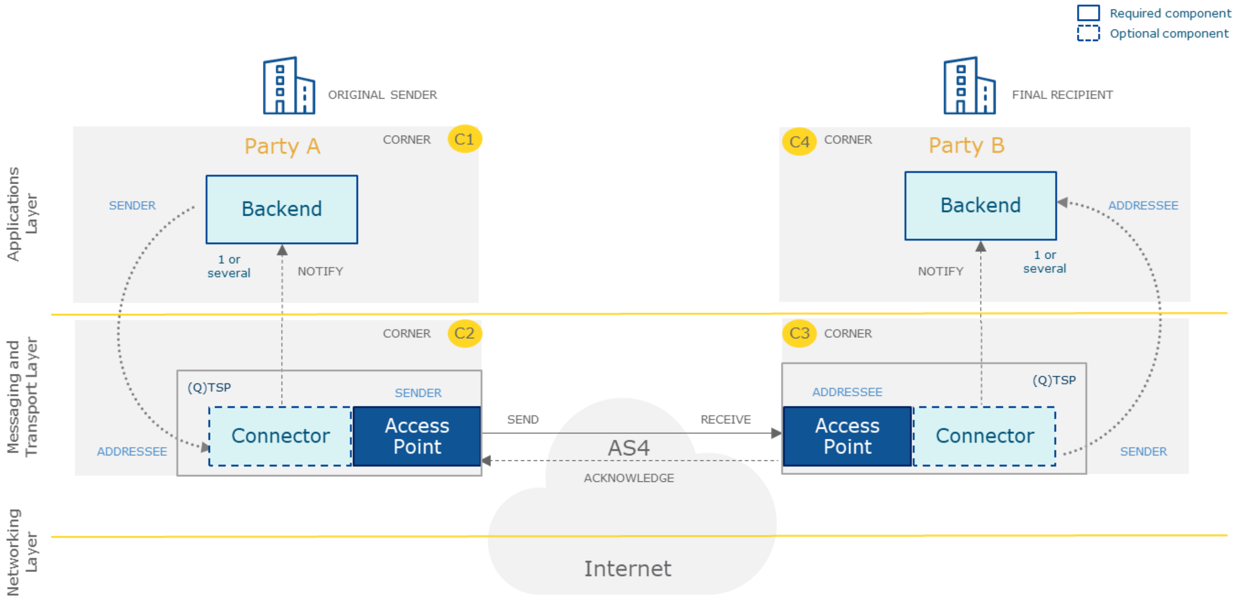


Figure 2. CEF eDelivery four-corner model

For additional information and description of CEF eDelivery, the reader is invited to visit the CEF Digital website.

4.2. Objectives

The main **objective** of this document is to **help organisations** to:

- Understand the requirements to be taken into account when choosing a trust model;
- Understand the most common trust models and their differences;
- Select the best fitting trust model.

4.3. Scope

As shown in Figure 2, each communication layer requires one or more digital certificates[1], in particular:

- *Transport layer:* The components of CEF eDelivery use TLS certificates to authenticate each other and encrypt the data at transport layer [5];
- *Messaging layer:* The authenticity, integrity and confidentiality of the data is guaranteed through electronic sealing and encryption at messaging layer using digital certificates [5]:
  - The digital certificate of the sending Access Point is used to electronic seal the message with the objective to guarantee the integrity and origin of the data.
  - The digital certificate of the receiving Access Point is used to encrypt the message with the objective to ensure its confidentiality;
- *Application layer:* The encryption of the data payload can optionally provide an additional layer of security. In this case, the original sender encrypts the data at application layer (i.e. the payload of the eDelivery message) by using the digital certificate of the final recipient [5].

This document focuses on the trust models governing the digital certificates at the messaging layer. The transport layer (i.e. server or TLS certificate) and application layer (i.e. end-user certificates) are **out of scope**. Nonetheless, the trust models of those layers adhere to similar rules.

[1] It is important to note that each communication layer requires different types of certificates. It is also recommended to use different certificates (key pairs) for distinct use cases, like signing and encrypting. For instance, the message signing and payload encryption requires the usage of two different digital certificates, such as an electronic seal and an encryption certificate.

4.4. Structure

This document is organised as follows:

- **Chapter 4** lists the requirements that organisations should consider when choosing a trust model. These requirements have been devised from different real life use cases;
- **Chapter 5** assesses the alternative trust models. This includes:
    - the Dedicated Domain PKI (e.g. the PEPPOL[2] eProcurement network);
    - the Shared Domain PKI (e.g. the CEF eDelivery PKI service[3], covering multiple domains);
    - the Mutual Exchange of Certificates (e.g. e-CODEX[4], in the eJustice domain) and
    - the Domain Trusted Lists (e.g. the Noble project[5], in the postal services domain).
- **Chapter 6** summarises the findings and highlights the differences between the alternative trust models.

[2] PEPPOL dedicated PKI: https://peppol.helger.com/public/menuitem-docs-peppol-pki

[3] CEF eDelivery PKI: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/PKI+Service

[4] e-CODEX: https://www.e-codex.eu/

[5] Noble project: http://www.mju.gov.si/si/delovna_podrocja/informatika/mednarodni_projekti/noble/

5. Requirement areas

As already explained in this document, a trust model is a collection of rules that ensure the legitimacy of the digital certificates used by the CEF eDelivery components. Digital certificates enable the identification of the organisations using eDelivery and are instrumental for the confidentiality, integrity and non-repudiation of the information exchange. Alternative trust models are available based on different trust anchor models and different rules to create, manage, distribute, store and revoke the digital certificates. This section outlines a set of generics requirements that can be used by organisations to choose their trust model.

Table 2. Requirements

Area	Requirement to be taken into account when choosing a trust model
Setup	This involves the following elements: • *Policies:* the policies specify the operational, issuing and security level requirements of the certificates. These policies follow industry standards and may also specify technical provisions. Qualified auditing procedures may be used to enforce the policy requirements and rules. • *Trust Service Provider (TSP):* represents the (legal) entity that generates and issues certificates. It can therefore play the role of a Certification Authority. A TSP also manages a certificate revocation list. The TSPs receive certificate requests for issuance, revocation and renewal of the digital certificates from a Registration Authority (RA). The TSP is often externalised. • *PKI factory:* refers to the infrastructure required for creating, renewing and revoking digital certificates. Organisations will typically use the factory of the (external) TSP. • *Registration authority* (RA): indicates the (legal) entity performing the identification, authentication and subscription of applicants. It guarantees that the TSP receives valid information. Unlike the TSP, the RA must be fulfilled by an organisation that understands the project using the CEF eDelivery Building Block.
Operational effort	The Operational effort includes the effort to maintain and operate the trust model, such as the policies, infrastructure and local trust stores initiated during setup. This includes the day-to-day operations of: • *Certificate and key storage*: the configurations required to store digital certificates and associated public and private keys. For instance, the additional security provisions required to keep the embedded private key secure. • *Certificate and key management*: the configurations to ensure the certificate and key validity, security and lifecycle management. This includes updating expired or revoked certificates or reissuing certificates.
Scalability	The ability to efficiently extend the trust model and support different: messaging topologies, number of users, configurations and security levels (supports strong & semi-strong models).

Flexibility & Interoperability	The ability to integrate with other trust models, e.g. when organisations participate in different policy domains[6].
Readiness*	The readiness state indicates the current state of the organisations to support a trust model. This includes their technological maturity and technical skills to implement, support and maintain the trust model.
Trustworthiness*	This represents the trust level defined by the security and certificate policies. The trust level reflects the quality and security assurance for electronic transactions. This must be respected by the TSP according to the requirements put forth by the eIDAS Regulation [3] either according to the qualified or non-qualified level. Both levels benefit from non-discrimination clause as a legal evidence. However, due to the stringent requirements for the TSP to obtain qualified status, qualified status provides a stronger legal binding at European level.
Cost*	This includes the setup cost and the recurrent costs to run, maintain and support the trust model, such as: • Digital certificates: the price of acquiring digital certificates; • Infrastructure: the price of maintaining and operating the infrastructure supporting the trust model. The cost is directly dependent on the sourcing model of organisations.

(*) It should be noted that the requirements related to the readiness, trustworthiness and cost depend on multiple factors. For instance, the outsourcing of operational efforts, the use of centralised services, and the use of automated digital certificate exchange such as ebCore Agreement Update Specification [7] may facilitate and limit the day-to-day operational effort.

This document classifies, according to expert opinion, the efforts to be employed by organisations when implementing the different trust models:

- 🟩 Low: The changes employed by organisations are minimal, requiring limited number of updates and extra configurations.
- 🟧 Medium: Additional configuration and implementation effort are required.
- 🟥 High: There is the need of a full setup and implementation.

[6] A similar approach applies to service providers covering multiple domains.

6. Trust models

This section describes and elaborates on the strengths and weaknesses of the different trust models:

- **Dedicated Domain PKI**: in this model, digital certificates are associated to a single trust anchor. In this case, the trust anchor serves a single domain i.e. it is a dedicated anchor. For example, in the eProcurement domain, PEPPOL PKI[7] operates a dedicated PKI;

- **Shared Domain PKI**: in this model, digital certificates are also associated to a single trust anchor but, in this case, the trust anchor serves multiple domains i.e. it is a shared anchor. For instance, the CEF eDelivery PKI service offering[8] operates a shared PKI model with a single TSP as its provider;

- **Mutual exchange**: this model relies on digital certificates from different trust anchors. As there is no single trust anchor, organisations are typically free to choose their preferred trust anchor. For example, the Pan-European project in the eJustice domain[9] implemented this model;

- **Domain trusted lists**: this model relies on a list containing the list of trusted certificates and/ or trust anchors complying with a common domain policy. For example, the Noble project[10] in the Postal Services domain implemented this model."

The figure below illustrates the alternative trust models and associated trust anchors.

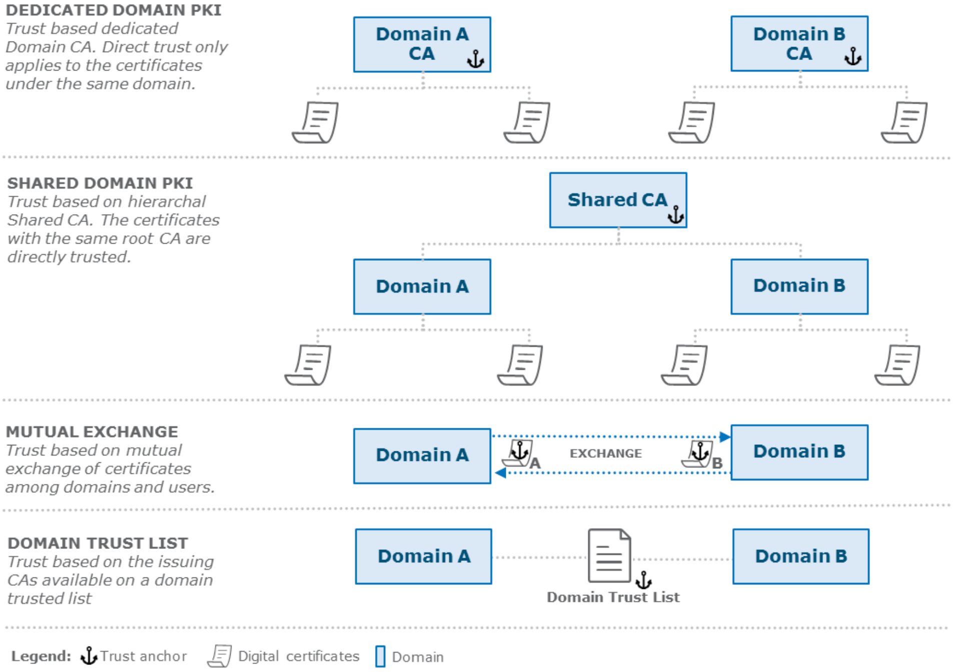

DEDICATED DOMAIN PKI
Trust based dedicated Domain CA. Direct trust only applies to the certificates under the same domain.
Domain A CA ⚓
Domain B CA ⚓
SHARED DOMAIN PKI
Trust based on hierarchal Shared CA. The certificates with the same root CA are directly trusted.
Shared CA ⚓
Domain A
Domain B
MUTUAL EXCHANGE
Trust based on mutual exchange of certificates among domains and users.
Domain A
⚓A
EXCHANGE
⚓B
Domain B
DOMAIN TRUST LIST
Trust based on the issuing CAs available on a domain trusted list
Domain A
Domain Trust List
Domain B
Legend: ⚓ Trust anchor
Digital certificates
Domain

Figure 3. Trust models overview

[7] PEPPOL PKI for eProcurement: https://peppol.helger.com/public/menuitem-docs-peppol-pki

[8] CEF eDelivery PKI: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/PKI+Service

[9] eJustice domain: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/2017/06/07/European+e-Justice+Portal

[10] Noble project: http://www.mju.gov.si/si/delovna_podrocja/informatika/mednarodni_projekti/noble/

4.5. Dedicated Domain PKI

In this model, digital certificates are associated to a single trust anchor. In this case, the trust anchor serves a single domain i.e. it is a dedicated anchor. For example, in the eProcurement domain, PEPPOL PKI operates a dedicated PKI.

Key attributes of every trust model	**Specific characteristics of this model**
Trust Anchor	Single anchor ***Note:*** The creation of a dedicated issuing CA will most likely require extra administrative workload for the definition and creation of the certificate and security policies which are tailored and specific to the domain.
Number of supported domains	Single domain ***Note:*** The dedicated anchor and the set of certificate attributes defined by the certificate policy is the same for all organisations and components in the domain.
Use of local trust stores	Can be circumvented ***Note:*** If combined with dynamic discovery, there is no need to maintain a local trust store as all certificates issued by the anchor can be trusted. Dynamic discovery is the process where a sending endpoint uses the functionality provided by the central SML to obtain the location of the receiving endpoint’s SMP. The sender then queries the SMP to obtain the location and requirements of the receiving endpoint and is able to transmit the message.
Example	The PEPPOL PKI operates under this model for the eProcurement domain. In this case, all the CEF eDelivery components require having digital certificates issued by PEPPOL's dedicated root CA. The PEPPOL PKI also separates the certificates of each component through the use of intermediate CAs under the dedicated issuing CA. However, as all certificates are issued under the same root CA, all components only require to trust the eProcurement dedicated issuing CA (i.e. root CA).

The table below summarises the main strengths and weaknesses of this model.

Table 3. Dedicated domain PKI model main strengths and weaknesses

Requirements	Model strengths	Model weaknesses
Setup		Domain owners are responsible for creating and establishing the specific policy and publishing the certificate policy documents to be used by the organisations in the dedicated domain. This requires to establish and request a domain specific CA from TSPs, which increases the technical and administrative workload to setup this model.
Operational effort	This model is restricted to single domain and closed group environments, and it provides: • Transparent and single certificate policy used by all organisations in the same domain, allowing for better control of the security and configurations. • No need to setup a local trusted store as trust is directly attained via the dedicated issuing CA.	
Scalability	Domain topology can be changed as the model allows for issuing digital certificates directly under the same dedicated CA for new organisations and components joining the same specific domain. The issuing of new digital certificates is managed by a domain specific RA.	
Flexibility & interoperability		It is a single domain solution that does not allow other domains to use their own CAs. The interoperability with other domains and models relying on different CAs requires cross-certification and setting up a local trust store which increases the operational effort for organisations.
Readiness	This model is highly dependent on the level of maturity of domain owners.	
Trustworthiness	Trust is limited to the domain and the dedicated CA used to generate digital certificates. Obtaining qualified status requires extra effort.	
Cost		Tailored certificate policies and dedicated CA may imply extra costs.

4.6. Shared Domain PKI

In this model, digital certificates are associated to a single trust anchor. In this case, the trust anchor serves multiple domains i.e. it is a shared anchor. The CEF eDelivery PKI operates under this model providing organisations with a simplified configuration and limited maintenance.

Key attributes of every trust model	**Specific characteristics of this model**
Trust Anchor	Single anchor ***Note:*** The certificate verification and validation process happens via the digital certificate path chain (hierarchical direct relation) to the shared issuing CA.
Number of supported domains	Multiple domains ***Note:*** The issuing CA is shared among multiple domains and users operating CEF eDelivery components. This increases the flexibility and interoperability of communications with other domains and components by using the shared CA.
Use of local trust stores	Can be circumvented ***Note:*** If combined with dynamic discovery, there is no need to maintain a local trust store as all certificates issued by the anchor can be trusted. ***Note:*** Typically, the use of a local trust store is needed. However, in specific cases, an additional check could be implemented at application layer to ensure that the certificate is issued in the relevant domain (based on the requirement to update the certificate policy to add a domain specific value in the certificates themselves). This option is only feasible if all implementations of all the components in the network support this specific check.
Example	The CEF eDelivery PKI operates under this model by using a known issuing CA from for all the digital certificates used by eDelivery components. The CEF eDelivery provides an optional PKI service offering from a well-known TSP containing the required provisions to support a shared PKI model [5]. The use of the CEF eDelivery PKI service offering reduces the complexity and cost of organisations during setup, readiness and operational effort. CEF eDelivery defines the policies in a certificate policy document. The CEF eDelivery PKI service offering provides organisations the access to a Registration Authority (RA) service for the issuing, renewal and revocation of digital certificates for the different organisations and domains under the shared CA, i.e. Shared Business CA (hereafter referred as 'SBCA'). The CEF eDelivery team manages both the RA and PKI Factory, and organisations operating CEF eDelivery components can establish specific sub-CAs.

The table below summarises the main strengths and weaknesses of this model.

Table 4. Shared domain PKI model main strengths and weaknesses

Requirements	Model strengths	Model weaknesses
Setup	This model simplifies the process of acquiring digital certificates by relying on already available and existing CAs under well-established policies and the possible use of multiple RAs.	Additional technical and administrative workload to setup a RA.
Operational effort	Low setup and operational effort, much lower than the dedicated domain PKI. Organisations can use any shared issuing CA or RA, improving the readiness.	
Scalability	This model allows to issue certificates directly for new components and organisations under the same shared CA.	
Flexibility & interoperability	The shared domain CA provides digital certificates that are cross-domain, reusable and interoperable with other domains with the same CA.	
Readiness	The readiness of this model depends on the level of maturity of organisations and the type of TSP used.	
Trustworthiness	Trust is dependent on the used TSP and shared CA.	
Cost		Costs can increase with the number digital certificates and levels of assurance required (i.e. qualified vs. non-qualified).

4.7. Mutual exchange

This model relies on digital certificates from different trust anchors. As there is no single trust anchor, this allows organisations to choose their preferred trust anchor. The eJustice domain operates under this model.

Key attributes of every trust model	**Specific characteristics of this model**
Trust Anchor	Multiple trust anchors ***Note:*** This model requires the mutual exchange of digital certificates between all eDelivery components communicating with each other. Each organisation is responsible for defining and agreeing on the policies with other organisations, and distributing the digital certificates for all the operated and managed components. As the exchanged digital certificates represent the trust anchor, the validation and verification of trust is reflected by the existence of the digital certificate in the local trust store. The certificate distribution should follow a secure protocol, whereas the authenticity verification should be performed according to the documented policy requirements. A secure portal or third party services could be used to facilitate the distribution of digital certificates between organisations.
Number of supported domains	Not applicable
Use of local trust stores	Cannot be circumvented ***Note:*** Each component maintains a local trust store containing a repository of exchanged and trusted digital certificates. These certificates represent the trust anchors in this model.
Example	This model is widely used to support business data exchange by different organisations employing different types of trust models. For instance, the eJustice domain uses this model to allow different CAs in a small fixed topology. Two components each use a different CA. Mutually exchanged certificates are stored in a local trust store. This offers flexible interaction between different trust anchors without the need to manage different trust models.

The table below summarises the strengths and weaknesses of this model to be considered by organisations.

Table 5. Mutual exchange model main strengths and weaknesses

Requirements	Model strengths	Model weaknesses
Setup	The creation, operation and maintenance of local trust stores provide a simplified way for establishing common trust anchors among different parties without the need for additional cross certification.	• Technical and administrative workload to setup a local trust store. • The PKI factories could be reused from the TSPs. However a party can chose to setup its own PKI factory, which implies technical and administrative workload.
Operational effort		Increased operational effort and cost with the increase of communication parties, as trust stores need to be updated accordingly.
Scalability		Requires extra operational processes and mechanisms for exchanging certificates whenever the topology and the number of users changes.
Flexibility & interoperability	Digital certificates are re-usable between different models, allowing organisations to freely choose the issuing CAs. Trust is attained via the exchanged certificate and its availability on the local trust store. This model is ideal for topologies with a low number of users.	
Readiness	The readiness of this model depends on the level of maturity of domain owners.	
Trustworthiness	Direct trust on the digital certificate exchanged after exchange process.	
Cost		Costs for setting up the infrastructure to support the certificate exchange, storage and management.

4.8. Domain trusted list

This model relies on a list containing the trusted certificates and/or trust anchors complying with a common domain policy. For example, the Noble project[11] aims to use this model.

Key attributes of every trust model	**Specific characteristics of this model**
Trust Anchor	A domain trusted list containing the trust anchors and/or trusted issuing CAs. This list acts as a central point of trust. ***Note:*** Trust is obtained as the digital certificates are issued under a CA in the domain trusted list. Domain trusted lists serve as a tool for materialising mutual recognition of digital certificates from different issuing CAs.
Number of supported domains	Multiple domains ***Note:*** Domain trusted lists are specific lists available to eDelivery components, these can belong to different business domains that rely on a single domain policy. The list is shared among all the components and updated for each certificate issuance and revocation.
Use of local trust stores	Not required ***Note:*** Organisations do not need to maintain a local trusted store as trust is directly attained via the CAs available in the trusted list. Organisations are free to choose their preferred trust from the trust list.
Example	The Noble project relies on this model to establish trust in order to minimise the barriers of eDelivery services.

[11] Noble project: http://www.mju.gov.si/si/delovna_podrocja/informatika/mednarodni_projekti/noble/

The table below highlights the benefits for organisations of using a domain trusted list model.

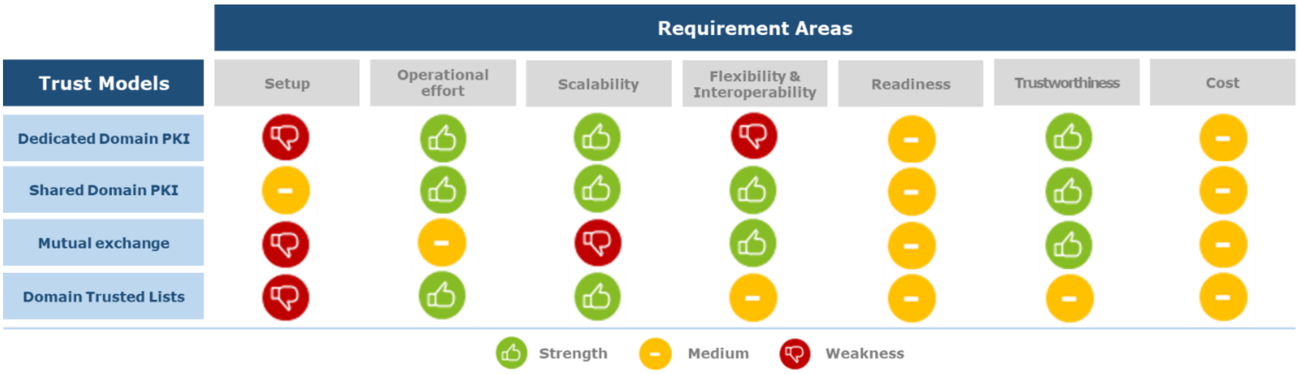
Table 6. Domain trusted lists model main strengths and weaknesses

Requirements	Model strengths	Model weaknesses
Setup		Trusted lists must be integrity protected with an electronic seal by the policy domain owner reflecting each content change, such as addition and deletion of digital certificates. The CA of the digital certificate of the domain owner is required to be available to the domain participants for verification and validation of the list integrity. The domain owner is responsible for the integrity protection and distribution of the domain trusted list upon each update.
Operational effort	Organisations do not need to maintain a local trust store as trust is directly attained via the CAs available in the trusted list.	
Scalability	The decentralised issuance of certificates allows organisations to freely choose their own TSP from the list of represented TSPs in the domain trusted list. This model can also be extended to a multiple trusted lists model, by using a master trusted list that concentrates the multiple trusted lists trust anchors in a single place.	
Flexibility & interoperability		
Readiness	The readiness of this model depends on the level of maturity of domain owners. Most solutions available in the market currently do not support trusted lists, which increases the effort for becoming ready and setup.	
Trustworthiness		Managing the different levels of assurance and levels of trust from the issuing CAs in the domain trusted list is complex. Trust is dependent on the levels of assurance defined by the domain owner responsible to manage the domain trusted list.
Cost		This model is currently not widely supported by solutions available in the market, which may lead to higher costs.

7. SUMMARY

This document describes different trust models that can be used for the trust establishment between CEF eDelivery components, and the different efforts to be borne by organisations. The evaluation of the different models follows the list of defined requirements aiming to help organisations operating and using CEF eDelivery components to understand and select the trust model best tailored to their business requirements.

The table below summarises the strengths and weaknesses of the different trust models.



	Requirement Areas						
Trust Models	Setup	Operational effort	Scalability	Flexibility & Interoperability	Readiness	Trustworthiness	Cost
Dedicated Domain PKI	👎	👍	👍	👎	−	👍	−
Shared Domain PKI	−	👍	👍	👍	−	👍	−
Mutual exchange	👎	−	👎	👍	−	👍	−
Domain Trusted Lists	👎	👍	👍	−	−	−	−

👍 Strength − Medium 👎 Weakness

Figure 4. Trust model lifecycle and business requirements effort per trust model

It is important to note that organisations may opt for different sourcing models and outsource the infrastructure, maintenance and support to an external party to facilitate and reduce the setup and operational efforts. These options change the effort for most requirement areas for the implementation of trust models in cases where the in-house skills, IT maturity and infrastructure levels are considerably low. Additionally, extra configurations and the use of automated services and cross-certification between trust models reduces the effort and improves interoperability.