EUROPEAN COMMISSION

DIGIT
Digital Europe Programme

eDelivery PKI Service

Service Offering Document

Version [1.20]

Date: 05/06/2023

Document Approver(s):

Approver Name	Role
Bogdan DUMITRIU	IT Project Manager – eDelivery

Document Reviewers:

Reviewer Name	Role
Bogdan DUMITRIU	IT Project Officer – eDelivery
Amar DEEP	Service Delivery Manager

Summary of Changes:

Version	Date	Created by	Short Description of Changes
V0.1	31/03/2022	Caroline AEBY	First draft
V0.2	28/04/2022	Thierry LEVY	Editorial review throughout document
V0.3	11/05/2022	Caroline AEBY	Support email address change
V0.4	31/05/2022	Caroline AEBY	No difference between DIGIT and eDelivery support + final review
V1.00	01/06/2022	Caroline AEBY	Final version
V1.10	24/10/2022	Caroline AEBY	Added privacy notice in new section
V1.20	05/06/2023	Caroline AEBY	Typos

Table of Contents

APPROACH AND PURPOSE OF THE DOCUMENT

The present document is the Service Offering Description (SOD) of the eDelivery PKI service. Key content includes an explanation of the roles and responsibilities and the process description of PKI service.

This document is intended for the eDelivery 'PKI domain owners' (i.e., organisations deciding which other organisations can be issued certificates to operate in a given message exchange network) and the organisations participating in the message exchange network by operating/benefiting from one or more eDelivery components, i.e., Access Points (AP) and Service Metadata Publishers (SMP).

Glossary

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

https://ec.europa.eu/cefdigital/wiki/x/TAfvB

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

https://ec.europa.eu/cefdigital/wiki/x/OgTvB

1. INTRODUCTION

Public Key Infrastructure (PKI) is a set of roles, policies, procedures, and systems needed to create, manage, distribute, store, and revoke digital certificates. The eDelivery PKI service enables issuance and management of the digital certificates used on the deployed eDelivery components, e.g., between eDelivery Access Points (AP) and Service Metadata Publishers (SMP), to ensure confidentiality, integrity and non-repudiation of the data moving across systems. This service is provided only to the European Union (EU) and European Economic Area (EEA) public administrations that wish to be established as PKI domain owners in the PKI service and that are interested in creating a circle of trust for information exchange using the technical specifications and components of eDelivery. The use of the eDelivery PKI is optional; policy domains may choose to use any other PKI service or mutual trust mechanism.

In its capacity as Solution Provider of the eDelivery Building Block, the Directorate-General for Informatics (DIGIT) makes available a PKI service (referred to as "eDelivery PKI service") to organisations participating in eDelivery-based projects operated by European Union (EU) and European Economic Area (EEA) public administrations. Such public administrations first have to establish themselves as "PKI domain owners" in relationship to the service. The organisations who are authorised by the PKI domain owner to be part of their domain can then use the eDelivery PKI service to obtain digital certificates.

The digital certificates can be used exclusively for the purpose of digital encryption and/or signing by eDelivery components, i.e., eDelivery APs and/or SMPs.

The eDelivery PKI service uses the CommisSign-2 PKI service of the European Commission[1] to issue digital certificates. In relationship to the CommisSign-2 PKI service DIGIT plays the role of Local Registration Authority (LRA) for all digital certificates issued via the eDelivery PKI service. As LRA, DIGIT ensures the segregation by PKI domain of the digital certificates it issues.

1.1. Purpose of the service

Every legal entity that acts as a service provider or uses one of the eDelivery components is denoted as "Organisation" in the rest of this document.

An Organisation that wants to make use of the PKI service needs to request the issuance of a digital certificate per eDelivery component it operates. The certificate usage is two-fold:

1. Signing a message: When an eDelivery component (AP or SMP) needs to send a signed message, the signing operation is performed using the private key associated to the certificate. The eDelivery component receiving the signed message uses information included in the certificate of the sender to check the signature of the message.

[1] http://commissign.pki.ec.europa.eu/index_en.htm

2. Encrypting a message: When an eDelivery component (AP or SMP) needs to encrypt a message, the encryption is performed using the public key included in the certificate of the receiving component. The receiving component is the only one able to decrypt the message, as it is the only one to know the private key corresponding to its certificate.

DIGIT plays the role of Local Registration Authority (LRA) for all digital certificates issued via the eDelivery PKI service. As LRA, DIGIT ensures the segregation by PKI domain of the digital certificates it issues.

Figure 1 shows the CA (Certification Authority) architecture[1] on which the eDelivery PKI service relies. The Root CA is the European Commission Root CA - 2. The Sub-CA is CommisSign - 2, which issues/signs the certificates for eDelivery APs and SMPs.

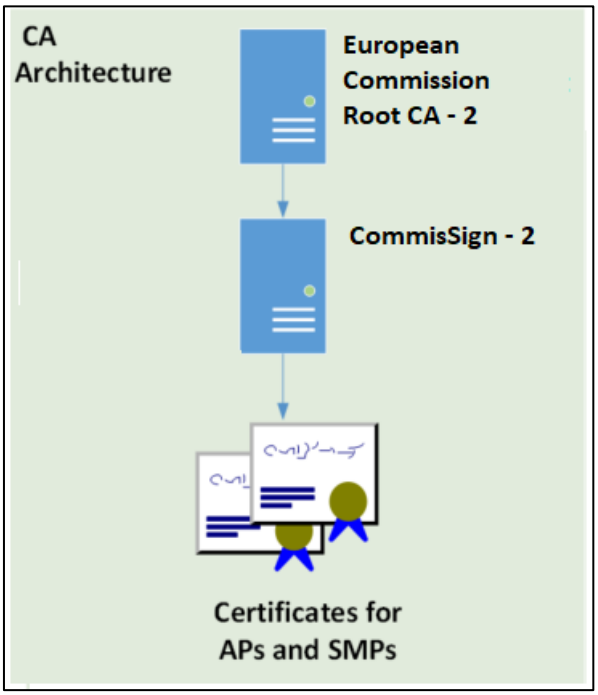

Figure 1. CA Architecture

The CA architecture information is important for the certificate validation process, to ensure that the certificates are issued by the trusted CA (European Commission Root CA - 2). The European Commission Root CA – 2 is not present in either the European Union Trusted Lists[2] or the trusted lists trusted by major operating systems, web browsers, or applications.

In addition to the CA, an important part of the eDelivery PKI service is the Local Registration Authority (LRA), which registers and approves the requests of issuance, revocation, and renewal of certificates. Figure 2 shows the architecture of the eDelivery Local Registration Authority.

The local registration authority serves to register and manage multiple domains, i.e., **organisation units (OU)**, each corresponding to a different eDelivery **PKI domain**, e.g., eHealth or e-Justice. The PKI domain owners are responsible to register and approve the requests of issuance, revocation and renewal of certificates performed by the operators of eDelivery

[2] See https://digital-strategy.ec.europa.eu/en/policies/eu-trusted-lists.

components (AP and SMP) that operate in the corresponding PKI domain. More details about the certificate validation process are provided in Annex 5.3.

Finally, the certificates for APs and SMPs that are issued to Organisations are separated using the "Organisation" ('O') field, which is part of the certificate metadata. Detailed information about the naming convention for the certificates is provided in Annex 5.2 of this document.

Note: It is important to note that the public keys included in the certificates and the corresponding private keys are generated by the requestors of certificate, i.e., the operators of eDelivery components (AP and SMP). The private keys need to be kept in a secure place by the requestors of the certificate. There is **no backup** of the keys provided by either the CommisSign-2 PKI service or the eDelivery PKI service.

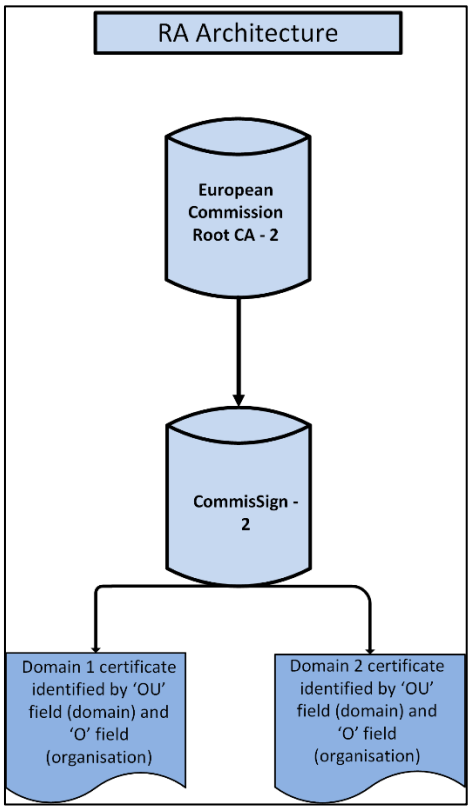

Figure 2 - Example of RA Architecture

A list of key terminology related to the eDelivery PKI service, is defined in the table below.

Terminology	Definition
Organisation	Every legal entity that acts as a service provider or uses one of the eDelivery components.

eDelivery PKI domain (organisation unit)	A policy domain in which eDelivery is used, e.g., e-Justice, BRIS, or eProcurement.
Domain owner	Entity established to request the eDelivery PKI service, register and approve the requests of issuance, revocation and renewal of certificates performed by the Organisations that participate in the corresponding domain.
LRA	Local Registration Authorities (LRAs) are entities responsible for the End Entity (i.e., Organisation) administration on behalf of the Commission CA. DIGIT D3 plays the role of Local Registration Authority (LRA) for all digital certificates issued via the eDelivery PKI service. As LRA, DIGIT D3 ensures the segregation by PKI domain of the digital certificates it issues.

Table 1 – eDelivery PKI Service Key Terminology

1.2. Users

The eDelivery PKI service is intended for the following types of users:

- **Organisations:** organisations that act as service providers or benefit from the eDelivery AP/SMP (denoted as "Organisation" in the rest of the document) which can include public and private organisations.
- **eDelivery PKI Domain Owners:** the owners of the eDelivery PKI domains, such as BRIS. They are typically a Directorate-General (DG) of the European Commission, e.g., DG JUST. Only European Union (EU) and European Economic Area (EEA) public administrations can become PKI domain owners in the context of this PKI service. Private businesses cannot become domain owners.

1.3. Scope

The table below represent the scope of the eDelivery PKI service.

Type of certificate	Description
Message Signing/Encryption Certificate	A certificate that supports signing and encryption of messages exchanged between eDelivery components, i.e. AP and SMP (see § 1.1 - Purpose of the service.)

1.4. Benefits

The eDelivery PKI service has been designed to generate a list of benefits to the users of the service:

- Well-established processes and procedures supported by the eDelivery Support.
- Digital certificates issued by a trusted PKI service provider – CommisSign-2 PKI service.
- Free-of-charge PKI service for a limited number of certificates.

2. Roles and Responsibilities

This section describes the main roles in the eDelivery PKI service and the responsible entities that are taking them up.

The following table summarises the split of roles and responsibilities between the different actors in the eDelivery PKI Service processes in the form of a RACI matrix where:

- **Responsible (R):** indicates the entities that perform the process step. Every process step has at least one responsible entity. Responsibilities can also be shared.
- **Accountable (A):** indicates the entity that is ultimately accountable for the process step. Every process step has only one accountable entity.
- **Consulted (C):** indicates the entities that give feedback or are consulted during the process step. This is a two-way process. Not every process step has an entity that is being consulted.
- **Informed (I):** indicates the entities that needs to be informed on the results of the process step. This is a one-way process. Not every process step has an entity that is being informed.

The following table summarises the split of roles and responsibilities between DIGIT, the eDelivery PKI domain owner and the Organisation that operates the eDelivery AP/SMP. The processes are described in detail below in the document.

Processes/Service	eDelivery Support Team	eDelivery PKI Domain Owner	Organization
Step 1: Request of a new eDelivery sub-domain	**R**	**A**	
Step 2: Notification about new eDelivery PKI domain	**A/R**	**I**	
Step 3: Certificate issuance			
Step 3.1: Certificate request	**I**	**A**	**R**
Step 3.2: Certificate approval	**R**	**A**	**I**
Step 3.3: Certificate creation	**R/A**	**I**	
Step 3.4: Certificate import			**R/A**
Step 4: Certificate renewal	**I**		**R/A**
Step 5: Certificate revocation	**C/R**	**R/A**	**I**

Table 2 – eDelivery PKI service RACI

2.1. eDelivery Support (Local Registration Authority or LRA)

Role: Local Registration authority (LRA)

Responsibilities:

- Identifying and authenticating the identity of Organisations applying for certificates.
- Verifying the authenticity of the request for a certificate.
- Verifying the applicant's data in Subject field.
- Technical implementation of certificate issuance, revocation, and renewal processes.
- Requesting the approval of the PKI Domain Owner for any certificate requests in their domain.
- Request of certificate issuance, renewal, and revocation within the appropriate eDelivery PKI domains.
- Handling new certificate issuance, renewal, and revocation requests for each specific operator of APs and SMPs

2.2. eDelivery PKI Domain Owner

Role: Governance of the eDelivery PKI domain

Responsibilities:

- Initiating the process of creating the PKI domain under the eDelivery PKI domain.
- Approval of the certificate issuance requests submitted by the eDelivery AP/SMP Operators in its domain.

2.3. Organisation (eDelivery AP/SMP Operator)

Role: Operate eDelivery AP/SMP within the eDelivery PKI domain

Responsibilities:

- Request and retrieve the certificates for the eDelivery AP/SMP it operates.
- Securely store and use the private keys associated to the certificates.

3. How to use the service step by step

This section describes the processes that are part of the eDelivery PKI service.

3.1. Process Overview

The figure below presents the main steps of the eDelivery PKI service process. Each of the process steps is described in more detail in the next sections.

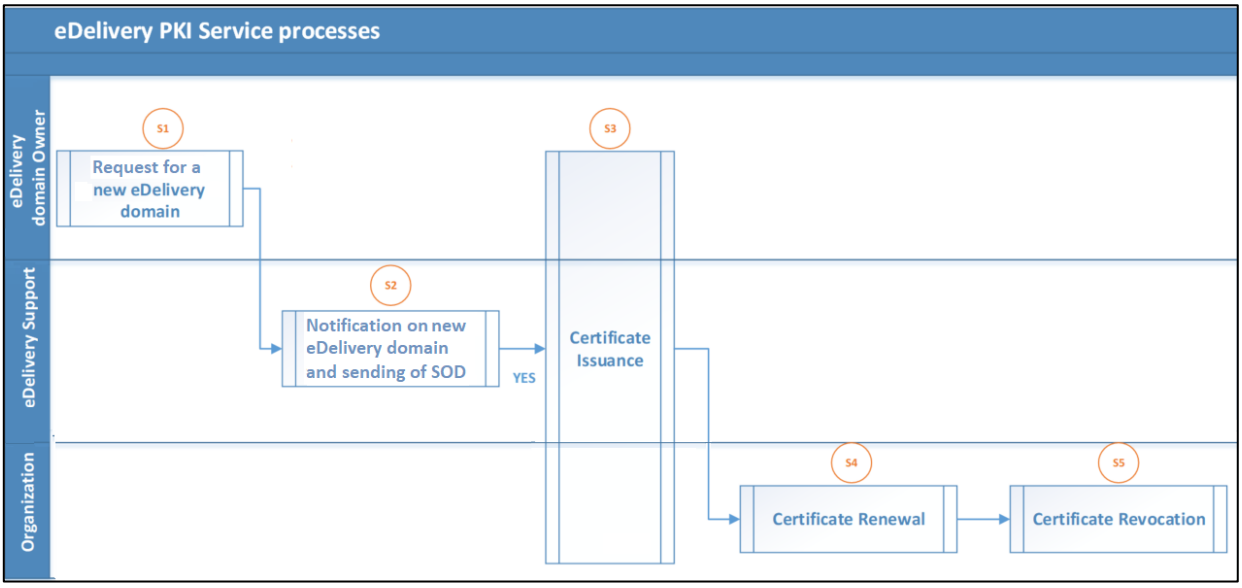

Figure 3 - eDelivery PKI Service processes

3.2. Step 1: Request for a new eDelivery PKI domain

Purpose: Submit an application for a PKI domain within the eDelivery PKI service.

Actors:

- PKI Domain owner (a policy domain owner who wants to use the eDelivery PKI service to establish trust in the domain)
- eDelivery Support

Process:

A domain owner sends the email to the eDelivery Support (EC-EDELIVERY-SUPPORT@ec.europa.eu) with the request for the PKI service. This email needs to include the contact details of the domain owner, including its email address and fixed phone number.

3.3. Step 2: Notification that new eDelivery PKI domain is ready

Purpose: Notify the PKI domain owner that the PKI domain is ready and provide him with the certificate issuance description document (Service Offering Description).

Actors

- PKI Domain owner
- eDelivery Support

Process:

eDelivery Support notifies the domain owner once the PKI domain for its service is ready. The notification includes the supporting material on how to interact with the service. Among others, the eDelivery Support must provide the following to the domain owner:

- The Service Offering Description document (SOD) for the specific PKI domain.

3.4. Step 3: Certificate issuance process

Purpose: Obtain certificates for the purpose of operating eDelivery APs /SMPs.

Actors

- Organisation operating the eDelivery AP/SMP
- PKI Domain owner
- eDelivery Support

Process:

1. Complete and sign the application form for eDelivery PKI certificate.
2. Generate the key pair and the CSR (Certificate Signing Request).
3. Send the CSR to eDelivery Support Team.
4. Import the CA Reply sent by eDelivery Support Team into the keystore.

The overview of the certificate issuance process is shown in the diagram below:

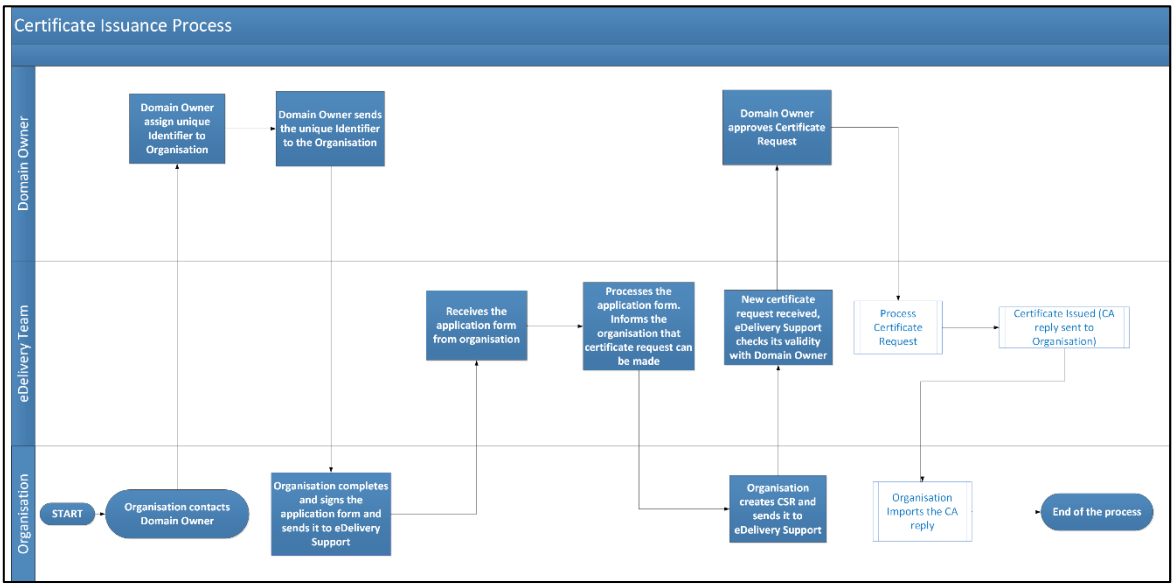

Figure 4. Certificate Issuance

3.5. Step 4: Certificate renewal

Purpose: Renew a certificate for the eDelivery AP.

Actors:

- Organisation
- PKI Domain owner
- eDelivery Support

Process:

1. eDelivery Support informs one month in advance the organisation that its certificate is about to expire.
2. The organisation is invited to renew its existing certificate.

eDelivery Support will advise on the renewal process.

3.6. Step 5: Certificate revocation

Purpose: Revoke a certificate for the eDelivery AP.

Actors:

- Organisation
- PKI Domain owner
- eDelivery Support

Process:

1. An Organisation or a PKI Domain owner submits a revocation request by emailing eDelivery Support.
2. eDelivery Support implements the certificate revocation after checking the organisation representative is valid (contacting the PKI Domain Owner).

4. TERMS AND CONDITIONS

4.1. Global Terms and Conditions (GTC) of the eDelivery PKI Service

Each PKI domain must sign the Global Terms and Conditions (GTC) of the eDelivery PKI service.

The PKI service GTC document describes the permitted and the prohibited usage of certificates as well as additional obligations of the certificate owner.

4.2. General terms and conditions of the Building blocks

The general terms and conditions of the Digital Building Blocks can be consulted in the Master Service Arrangement, available on the Digital Single Web Portal:

https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Master+Service+Arrangement

The terms and conditions specific to the eDelivery PKI service are described on the Digital site: https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Terms+and+Conditions+for+eDelivery+PKI+Service .

5. ANNEX

This annex contains the information that supports the proper understanding and execution of the processes described in Section “3 - How to use the service step by step “.

How to use the service step by step”.

5.1. Creation of organisation units - Separation between the eDelivery PKI domains

One of the security requirements for the eDelivery PKI is to create separated areas of responsibilities that correspond to different eDelivery PKI domains, e.g., e-Justice, BRIS, etc. This means that all the eDelivery components (APs and SMPs) that belong to the same PKI domain trust each other. On the other hand, a component/participant from one PKI domain, e.g., e-Justice, should not be considered trusted in a different PKI domain, e.g., BRIS.

There are different ways to implement the trust architecture that supports the creation of areas of responsibilities. The simplest one is to use a dedicated domain-specific Sub-CA that issues end-entity certificates to all the components/participants in a given eDelivery domain. By setting the domain-specific Sub-CA as trust anchor for the eDelivery components, it is ensured that only the components within the domain are trusted.

In the eDelivery CA architecture (Figure 1), the end-entity certificates for all PKI domains are issued by the same Sub-CA: CommisSign - 2. Therefore, it is not possible to create isolated trust domains by relying on the Sub-CA information in the end-entity certificates. To overcome this, a different mechanism is put in place to create areas of responsibilities and provide separation between the eDelivery domains. This is explained in more details in the following section.

5.2. Certificate Naming Convention

To achieve separation per area of responsibility, the eDelivery PKI service uses the naming convention in the certificate metadata.

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

1. **Common name (CN)**: <PKI domain>_<TYPE>_<ENV>_<COUNTRY CODE>_<UNIQUE ID>
   Where:
   <PKI domain> = name of the PKI Domain predefined with the PKI Domain owner
   <TYPE> = purpose of the certificate: **AP** or **SMP**
   <ENV> = environment where the certificate will be used: **TEST**, **ACC** as Acceptance, **PROD** as Production
   <COUNTRY CODE> = same as the **C** (Country) field (see below)
   <UNIQUE ID> = unique identifier defined by the Domain owner
   Examples:
   DOMAIN_AP_ACC_LU_001

2. **Organisation Name (O)**: name of the requester Organisation: it should match the Organisation name in the PKI application form created as a prerequisite of the certificate request. E.g.: ACME Corporation
3. **Organisational Unit Name (OU)**: This is the pre-defined domain name: e.g., CIxP.
4. **Country (C)**: The 2-letter code belongs to the country of the requester Organisation defined in ISO 3166-1 alpha-2. E.g.: BE

The **Subject** of the final certificate contains the following attributes:

Fields	Values	Fixed/Variable	Populated by
CN	Supplied by the domain owner. Format: <PKI_DOMAIN>_<TYPE>_<ENV>_<COUNTRY CODE>_<UNIQUE ID> e.g. DOMAIN_AP_ACC_LU_001	Variable	Organisation
OU(1)	<PKI DOMAIN>	Fixed	Organisation
OU(2)	<TYPE>_<ENV>-GTC_OID-1.3.130.0.2022.1704569 e.g.: AP_PROD-GTC_OID-1.3.130.0.2022.1704569	Variable	eDelivery Support
OU(3)	EC_eDelivery.europa.eu	Fixed	CommisSign-2 PKI
O	Organisation name	Variable	Organisation
C	Country code	Variable	Organisation

5.3. The certificate validation process

The certificate validation is implemented by each eDelivery component and is part of the eDelivery source code. More ample details about this process are present in the Guidance on Digital Certificates:
https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Guidance+on+Digital+Certificates.

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

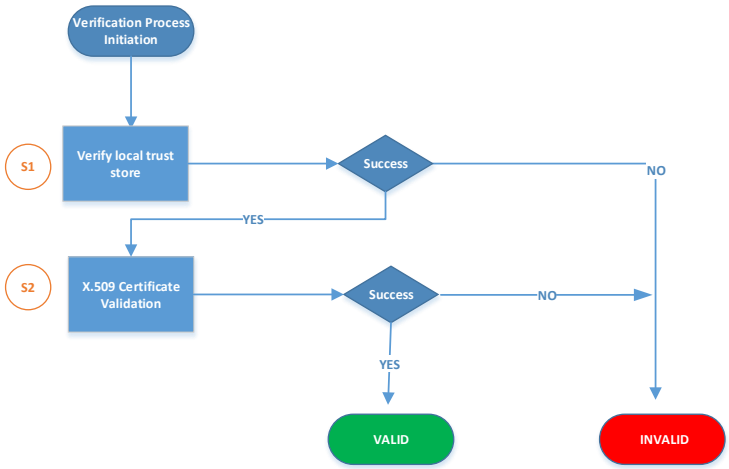

Figure 5 Certificate Validation in the eDelivery PKI

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

S1: Verify local trust store	**The verifying component first checks if the certificate is in its local trust store.**
S2: X.509 Certificate Validation	The standard certificate validation in accordance to the ETSI standard[3] that includes the verification of the expiration date, revocation status, and intermediate CA signature on the certificate.

Table 3 Certificate Validation Steps

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

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

6. PRIVACY NOTICE

The way European Commission is processing personal data belonging to the users of PKI service can be consulted in the eDelivery privacy statement for PKI Service.

7. CONTACT INFORMATION

eDelivery Support

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

Standard Service: 8am to 6pm (Normal EC working Days)