SWIM Common PKI and policies & procedures for establishing a Trust Framework

D3.1 – Initial SWIM interfaces to Common PKI

Document information	
Project Title	SWIM Common PKI and policies & procedures for establishing a Trust Framework
Project Number	2017_084_AF5
Project Manager	EUROCONTROL
Deliverable Name	Initial SWIM interfaces to Common PKI
Deliverable ID	D3.1
Edition	1.0
Template Version	01
Task contributors	

Please complete the advanced properties of the document

Abstract

This document describes the initial PKI interfaces presented to the users of the European Aviation Common PKI (EACP) to access and manage different PKI services as presented in the EACP portfolio.

Authoring& Approval

Prepared By - *Authors of the document.*		
Name &Company	Position & Title	Date
Abdel YOUSSOUF EUROCONTROL	PKI expert	15/06/2021

Reviewed By - *Reviewers internal to the project.*		
Name & Company	Position & Title	Date
Patrick MANA EUROCONTROL	Project Manager	07/07/2021
Denis BUTIN DFS	Project Member	20/08/2021
Gregers INOUE NAVIAR	Project Member	20/08/2021

Reviewed By – *e.g. EDA, staff associations, other organisations.*		
Name & Company	Position & Title	Date

Approved for submission to the SDM By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date

Rejected By - *Representatives of the company involved in the project.*		
Name & Company	Position & Title	Date

Rational for rejection

Document History

Edition	Date	Status	Author	Justification
0.1	15/06/2019	Draft	A.YOUSSOUF	Initial draft
0.2	08/07/2021	Draft	P. MANA	Review draft
0.3	08/07/2021	Draft	A.YOUSSOUF	Updated draft
1.0	19/10/2021	Released Issue	A.YOUSSOUF/ P.MANA	Amended to take comments into account

Table of Contents

1 INTRODUCTION 7
1.1 Content 7
1.2 Objective of this Deliverable 7
1.3 Project description 7
1.4 Project scope 7
1.5 Project objectives 8
2 European Aviation Common PKI Hierarchy 9
3 European Aviation Common PKI Platform 9
4 European Aviation Common PKI Interfaces 11
4.1 Certification Authority Operator Interface 11
4.2 Registration Authority Operator Interface 12
4.3 Interface for End Entity Certificate provisioning 12
4.3.1 Web Interface 12
4.3.2 Certificate Enrolment Protocol 13
4.3.3 XKMS Protocol 14
4.3.4 ACME Protocol ..... Fejl! Bogmærke er ikke defineret.
4.4 Interface to access EACP repositories 14
4.5 Interface for Certificate Revocation Checking 15
4.5.1 Interface for CRL Distribution Point 15
4.5.2 Interface for Online Certificate Status Protocol 15
4.6 SCVP Interface 16
4.7 Interface for timestamping 16
4.8 Signing as a Service Interface 17
5 References 17

Table of Figures

Figure 1: European Aviation Common PKI Hierarchy 9
Figure 2: Typical PKI Architecture 10

1 INTRODUCTION

This document describes the users' interfaces for the future European Aviation Common PKI (Public Key Infrastructure), deliverable D3.1 - Initial SWIM interfaces to Common PKI of the "SWIM Common PKI and policies&procedures for establishing a Trust Framework" project.

1.1 Content

These users' interfaces of the future European Aviation Common PKI (EACP) describes the multiple interfaces that users will have to interact with to use the EACP services.

The scope of this document is limited to the description of the main PKI component interfaces. Interfaces of other components that make the PKI solution such as Network components (firewalls, routers, etc.), load balancers, backup tools and monitoring tools are not described in this document.

1.2 Objective of this Deliverable

The main objective of this Deliverable D3.1 is to describe the main PKI interfaces, used by a user to access the different PKI Services. The interfaces described here are rather generic ones. More precise interfaces will be described by the contractor that will provide the EACP solution infrastructure.

The different acronyms used in this document are defined in the document "Acronyms and Definition". See [1].

1.3 Project description

The "SWIM Common PKI and policies&procedures for establishing a Trust Framework" project aims at developing and preparing the deployment of a common framework for both integrating local PKI deployments in an interoperable manner as well as providing interoperable digital certificates to the users of SWIM and other services and systems supporting European aviation operations. The resulting PKI and its associated trust framework, which will be part of the cyber security infrastructure of aviation systems, are required to sign, emit and maintain digital certificates and revocation lists including as required in the Common Project 1 family 5.1 (EC IR 2021/116). The digital certificates will allow user authentication and encryption/decryption when and where needed in order to ensure that information can be securely transferred. All aviation Stakeholders (ANSPs, Airspace users, MIL, Airport, etc …) will benefit from the project.

1.4 Project scope

The scope of the "SWIM Common PKI and policies&procedures for establishing a Trust Framework" project includes the definition and development of a dedicated common PKI and its associated trust framework for the European aviation (so-called EACP), its integration and validation with some Stakeholders. It will ensure the interoperability of digital certificates within Europe and with other regions.

The future EACP solution will not be restricted to provide certificate only for SWIM purposes. Benefits of developing and deploying this solution have been taken to extend its scope as much as possible to:

- Increase the level of security of the European aviation network by allowing as many stakeholders, applications, services, systems using digital certificates as security enhancement means.
- Increase the cost-efficiency of the solution as the cost of developing and operating a PKI/Bridge is not linearly linked to the number of certificates (e.g. the cost of developing and operating a PKI/Bridge for few or half million certificates is nearly the same).

Therefore, the "SWIM Common PKI and policies&procedures for establishing a Trust Framework" project will develop the material to prepare the development and the operations of the future European Aviation Common PKI solution.

1.5 Project objectives

The "SWIM Common PKI and policies&procedures for establishing a Trust Framework" project also aims at preparing the development of the systems needed to operate a PKI and its associated trust framework in order to produce and manage digital certificates, e.g. Certification Authorities, validation services such as OCSP (Online Certificate Status Protocol) or CRL (Certificate Revocation List) or SCVP (Server Certificate Validation Protocol), user interfaces, systems supporting the Registration Authority and Policy Management Authority roles. These systems will be developed through procurement, for which the project will prepare a Call For Tenders (CFT).

Task3 is dedicated to define the users' interfaces.

2 European Aviation Common PKI Hierarchy

The different use cases discussed during the SWIM Common PKI Project has led out to the PKI hierarchy shown in Figure 2, which in turn induces different certificate profiles. As every digital certificate has its own purpose, its own policy and its own registration procedure, it has also its own interface used to manage this digital certificate.

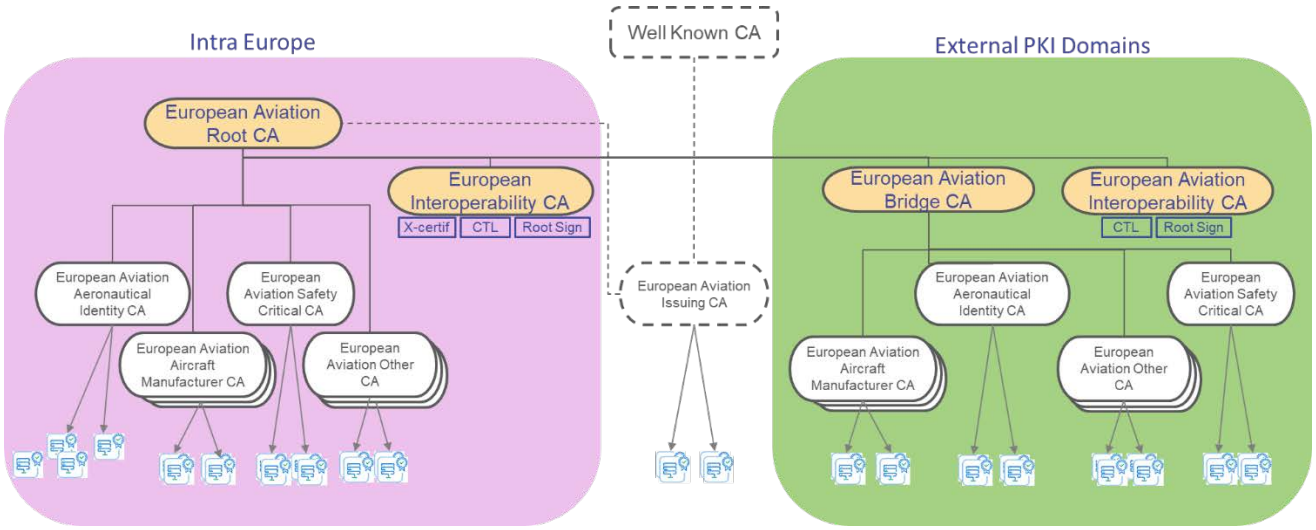

Figure 1: European Aviation Common PKI Hierarchy

3 European Aviation Common PKI Platform

A PKI by definition is a set of hardware, software, policies and procedures that enable digital certificate lifecycle management. Hence, a typical PKI architecture is made of set of hardware hosting different software that are installed and configured in two data centres so that they can work in high availability mode and then fulfil the Service Level Agreement (SLA). Figure 2 gives a typical PKI architecture.

At the time of drafting this document, the EACP architecture has not been yet selected because the Call For Tenders has not been published. What is presented is therefore an anticipated EACP architecture, which is based on most common (typical) PKI architecture.

Typical PKI hardware are:

- Ordinary servers hosting the different software listed below
- HSM
- Servers with Storage Area Network
- Firewalls
- Routers
- Load balancers
- Backup servers

- Monitoring servers

Typical PKI software are:

- Operating system
- Certificate Management software
- Database software
- LDAP software
- Timestamp software
- OCSP software
- SCVP software
- HSM software

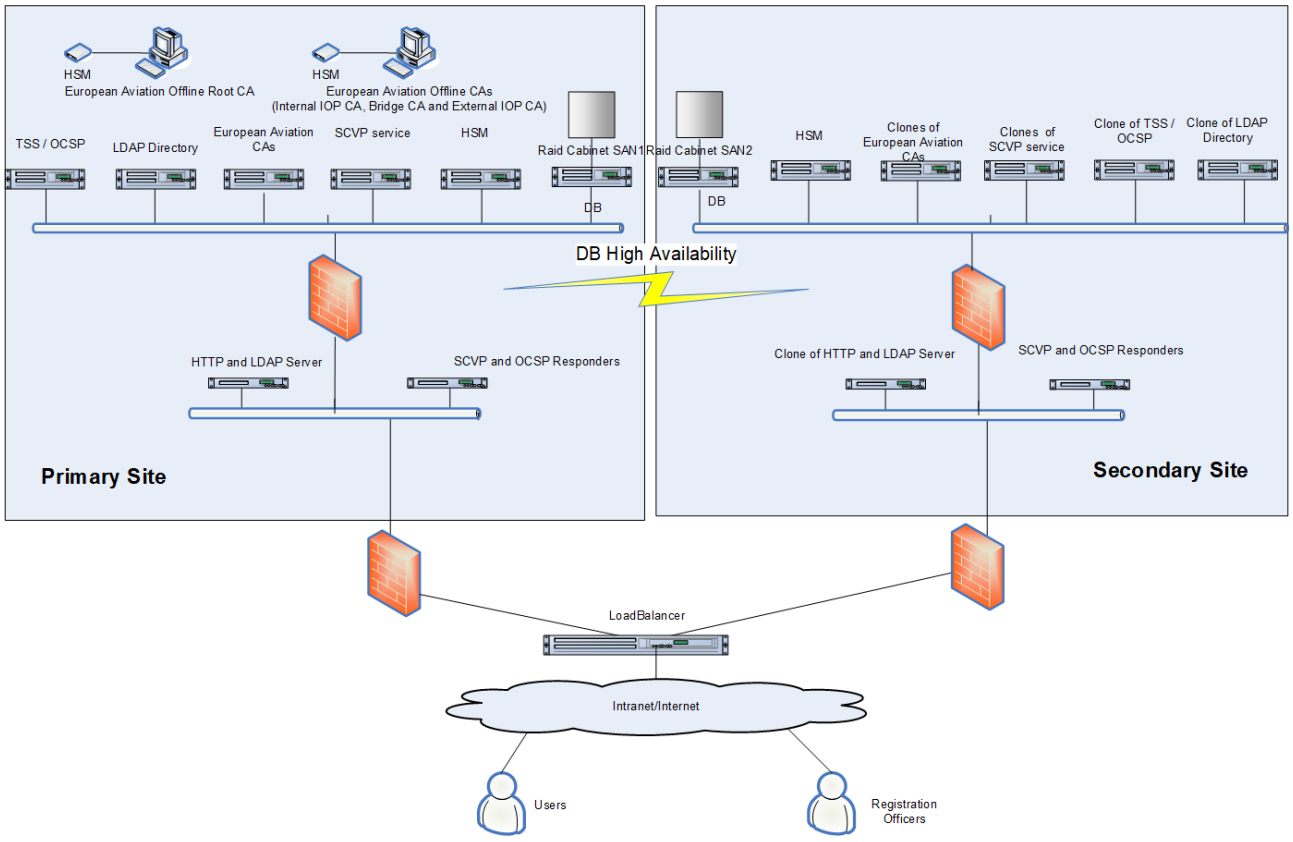

Figure 2: Typical PKI Architecture

The main interfaces that are presented to an end entity user can be summarised as follows:

- Certification Authority interface
- Registration Authority and Local Registration Authority interface
- Certificate lifecycle management:

  - User interface: set of web interfaces that allows subscribers to enrol themselves to request certificates, to renew or to revoke an existing certificate.
  - PKI Portal (Web Interface): This is an interface that PKI Operators use to request certificates and revocation on behalf of subscribers.
  - SCEP (Single Certificate Enrolment protocol): this is a protocol that is used to support the enrolment of devices
  - XKMS (XML Key Management Specification) protocol: this is a protocol that allows for handling certificate request and certificates delivery in bulk based on an xml standards
  - ACME (Automatic Certificate Management Environment) protocol: This protocol allows automation of certificate provisioning to system administrators.
- PKI Publication: EACP uses its repositories to disseminate some PKI certificates, CRLs and documentation. The repositories can be either LDAP servers, HTTP servers or even folders accessed via secure file transfer protocols. .
  - Certificate and CRLs publication using LDAP protocol, this covers end entity certificates (if applicable), as well as CA certificates and associated CRLs
  - Certificates (only CA certificates) and associated CRLs publication using http protocol
  - PKI Certificate Policy (CP), Certification Practices Statement (CPS), Subscriber Agreement and relying party agreement and other documentation as deemed necessary.
  - Certificate Trust List (CTL), bridge and cross-certificate publication
- Interface for Online Certificate Status Protocol
- Interface for Online Certificate Validation
- Interface for timestamping
- Interface for Signing as a Service

4 European Aviation Common PKI Interfaces

4.1 Certification Authority Operator Interface

The Certification Authority Operator (CAO) is the administrator responsible for configuring and maintaining on a daily basis the Certification Authority Module. The CAO controls all of the administration functions and grant privileges to other operators using a set of interfaces. The first CAO is created during the bootstrap of the CA. There can be multiple CAOs with the same rights (for back up reasons) or with different rights if distributed control is required. The CAO credentials can be stored on software or on hardware tokens, protected by access control means.

Responsibilities of the CAO include the following:

- Creation of other Operators: the CAO can create other PKI entities such as other CAOs, or CA Auditors, or Registration Authorities and Local Registration Authorities.
- Registration policy creation: the CAO can create and maintain registration policies for the creation of certificates and configure the CRL generation profile, as set forth by the EACP Certificate Policy document.
- Audit functions: The CAO can view the certificates and the CRLs that have been issued,
- Certification and Revocation: the CAO can directly create or revoke any certificate

- Export and import CA audit logs.

4.2 Registration Authority Operator Interface

The Registration Authority (RA) service acts as a router between RA Operators (RAO) and the CA. The main role of the RAOs is to vet the certificate requestors as per the registration procedures, and to approve, differ or deny certificate requests and revocation requests.

RAO is an authorized entity who can only process requests associated with specific registration policies that have been assigned to him by the CAO. The role of the RAOs may be segregated per domain, i.e. assigned different roles to manage different certificate types, e.g. RAO1 manage the lifecycle of SSL certificate, Client Certificate and Personal Certificate, while RAO2 manages SSL Certificate and Object Signing Certificate, etc.

Every RAO obeys to its own operational policy, which is maintained centrally by the CAOs.

Responsibilities of the RAO include the following tasks:

- The RAO can only approve certificate requests using Registration Policies that have been assigned to him by the CAOs.
- Under the control of the registration Policies, the RAO can enforce face-to-face registration, certification request, including optionally generating and storing user keys on a token or in software.
- Under the control of Registration policies, the RAO can authorise or reject a certification or revocation request from Subscriber or PKI Operators.
- Depending on the approval level, the RAO can provide additional authorisation for certification requests received from other RAOs, e.g a certificate request approval may request two RAO approvals (principle of 4 eyes)
- The RAO can authorise revocation of a certificate issued against registration policies that have been assigned by the CAOs.

4.3 Interface for End Entity Certificate provisioning

4.3.1 Web Interface

4.3.1.1 PKI Operator Portal

The PKI Operator portal interface allows PKI operators to manage a subset of EACP certificate classes and offers auditing and reporting functionalities. It is accessed from the web via HTTPS by different PKI operators that are designated by European Aviation stakeholders.

Before having access to the portal, PKI Operators need to be registered and enrolled for specific certificate types. Once registered, PKI operators are authorised to access the **PKI Operator Portal** and perform a set of functions such as submit a certificate request, retrieve a certificate, search for a certificate, revoke a certificate, etc.

If needed, PKI Operator interface may be configured to support the case where the PKI Operators can create key pairs on software or hardware on behalf of subscribers, and then submit associated certificate request for the certification purpose.

Information related to the certificate management status will be in a specific Database, which stores among others, certificate request, associated certificate, the certificate's issuer, the certificate serial number, the certificate status, the certificate signature, the certificate validity period, notification sent by the CA to the PKI Operator, audit etc... This audit and reporting function can also be exportable and be available to specific authorised users.

4.3.1.2 Web Interfaces presented to EACP end users

A set of web pages are presented to the end users to allow them managing a specific certificate class, i.e. requesting, revoking, or renewing it.

The web pages are designed to implement the certificate policies (including options specifying key pair created on software or on hardware) and associated registration procedures (automatic generation, or interaction with the RA). The link to the different web pages are presented in the EACP website.

4.3.2 Certificate Enrolment Protocol

4.3.2.1 SCEP Registration process

Simple Certificate Enrolment Protocol, or **SCEP**, is a protocol that allows devices to easily enrol for a certificate by using a URL and a shared secret to communicate with a PKI. This protocol has the main benefit of improving scalability and limiting operational overhead. SCEP enables an endpoint to request a certificate or other certificate-related functions (revocation checking, renewal and so on) remotely.

In fact, when dealing with large number of networked devices such as routers, firewalls, MDMs (Mobile Device Management), going through the steps to manage digital certificates for each of those devices can be painful task for the network engineers and PKI operators. Often, engineers and PKI operators prefer to have an automated way of acquiring and renewing digital certificates.

When network connections are possible between an endpoint device and a PKI platform, a network-based approach might be the preferred option for the digital certificate provisioning because it provides the opportunity to template the configuration that can be setup one time enabling automation for subsequent certificates upon certificate expiration. This approach is easier to implement and save engineers and PKI operators a lot of time and effort.

This automatic way of provisioning devices with digital certificate can be implemented with Simple Certificate Enrolment Protocol (SCEP) Protocol. It is drafted in Request For Comment (**RFC 8894**).

When an end device has a key pair, it can make a request to a designated EACP certificate authority using SCEP. That certificate request includes the public key. EACP responds with the new certificate, which is encrypted with the requestor's public key. This way, only the entity making the request can decrypt it.

4.3.2.2 ACME Protocol

The Automated Certificate Management Environment protocol (**ACME**) is a protocol for automating certificate lifecycle management communications between Certificate Authorities (CAs) and end entities.

ACME protocol can apply for different digital certificates such as SSL certificates, email certificates, device certificates, etc.

ACME protocol is open standard and can be easily integrated at both back end (EACP side) and the end entity side. It is an Internet Standard, described in **RFC 8555** by its own-chartered IETF working group. ACME v2 is the current version of the protocol.

CAs provide mechanisms to ensure that certificate users legitimately represent the identities and domain name(s) associated with the certificates. The process for exchanging information necessary for EACP to perform that authentication and issue certificates, and for the user to then deploys the issued certificates, is automated using the ACME protocol, rather than communicating this information manually. In addition to the certificate issuance process, the protocol also enables other certificate lifecycle management use cases like certificate revocation and renewal.

4.3.3 XKMS Protocol

XKMS interface features both a W3C's XML Key Management Specification (XKMS) and a W3C's XML Key Management Specification Bulk Operation (X-BULK) compliant responder. Both represent the most open and interoperable PKI interface known today.

XKMS and its extension X-BULK utilize the XML Schema Language to define the necessary structures, integrating the XML Signature for authentication and authorization while the Simple Object Access Protocol (SOAP) and the Web Services Definition Language (WSDL) defines the interfacing and the relation between the XML messages.

XKMS offers both Certificate request (XKRS) and Certificate information/validation (XKISS) functionality. The X-BULK extends the Certificate request function for bulk registrations necessary for interfacing with such systems as smart card management systems.

In addition, it is possible to use the flexibility of the standards to introduce more functionality than the standard strictly offers. First of all, even when using XKMS requests (deviating from a standard PKCS#10 request), one can create a fully compliant x509 Certificate with a complete subject distinguished name making it backwards compatible. In addition, one can introduce the notion of suspension and reactivation of certificates. Finally, it is possible to support certificate generation according multiple certificate types (profiles), even mixed in a large X-BULK request.

EACP will implement XKMS protocol via client-server mode. The server mode will be running at the DMZ part of PKI and will be linked to back end part of the EACP via a specific gateway.

4.4 Interface to access EACP repositories

A repository is a generic term used to describe a storing location of certificates and revocation information (CRLs), PKI Policy documents and other related document and files so that they can be retrieved by subscribers or relying parties.

EACP uses its repositories to publish CA certificates, CRLs and some EACP PKI documentation including the Certificate Policy document and some agreements and Terms of Use. EACP may also publish end entity certificates if an evolving use case may require so. EACP repositories will be made of **LDAP directories** and **HTTP servers**.

The EACP repositories will be configured such that the offline CA Certificates and CRLs can be pushed manually to the repositories, while the online CAs, end entity Certificates and CRLs can be configured to be pushed automatically to the repositories whenever a new end entity certificate and/or new CRL has been created.

The LDAP directory can be accessed users and relying parties via any LDAP client.

4.5 Interface for Certificate Revocation Checking

4.5.1 Interface for CRL Distribution Point

CRLs and sometimes delta CRLs are used by subscribers and relying parties to determine if a certificate has been revoked or if it is still considered valid. Some applications may fail if they cannot determine the revocation status of a certificate, unless revocation checking has been disabled, which is a very poor practice, especially for aviation use cases, where availability is paramount. Just like certificates, CRLs have a time period during which they are valid. Once the CRL expires, the CA generates a new one and push it to its repository.

In every certificate, there is an extension named CRL Distribution Point (CDP), which is pointing to the location of the repositories used by the CA to publish its CRLs. As indicated in section 4.4, EACP will use both **LDAP directories** and **HTTP servers** to host the CRL files. CRL profile is defined in **RFC 5280**).

4.5.2 Interface for Online Certificate Status Protocol

Online Certificate Status Protocol (OCSP) is an Internet-based protocol that has been created as a real-time way to check the status of a certificate. It complements the classical revocation checking which is based on the revocation list (CRL). OCSP becomes the preferred way of revocation checking when the CRL files are large. In fact, downloading and processing very large CRL files can slow down and hamper many applications from checking the status of the certificates.

OCSP is implemented with the client-server mode. OCSP responses can be obtained for individual certificates via OCSP instead of downloading the entire CRL list or a portion of the CRL list. The "request then response" nature of OCSP queries led to OCSP servers being called OCSP responders.

An OCSP responder is typically a server that is connected to a CA server or use the CRL files and is configured to return an OCSP response indicating if a certificate specified in the request is "good", "revoked" or "unknown".

Both OCSP requests and OCSP responses are formatted according to the **RFC 6960** standard and RFC 8954, which is an update to this RFC . All OCSP responses are digitally signed; therefore, OCSP responders are configured to use digital certificates and associated key pairs. Following the configuration at the OCSP server side, OCSP requests may be signed, in such case, only signed request will be processed. Unsigned request will be rejected.

EACP will configure an OCSP responder so that to offer Online Status Checking. The location of the OCSP responder will be described in a certificate extension and more precisely in "Authority Information Access" where access to the responders is implemented with an **HTTP protocol**.

As the use of OCSP requires a connection to an OCSP server with an HTTP protocol, OCSP may not be used in the framework of use cases where high real-time performance is needed or where interaction with Internet should be limited, (no caching of OCSP responses can be implemented as for CRL).

As for CRL, some applications may fail if they cannot determine the revocation status of a certificate.

4.6 SCVP Interface

For business applications relying on PKIs, the process of trusting digital certificates is rather complex. It requires the ability to locate certificates (which can be stored locally, sent in the validation request or to be loaded from online resources) in order to construct a valid certificate path to one or more trust anchors. Once a certificate path is successfully constructed, it then needs to be subjected to a multi-step validation process where many fields and extensions inside each certificate in the path are reviewed and validated according to a complex set of PKI rules.

Server-based Certificate Validation Protocol (SCVP) is a validation service that implements the **RFC 5055**, it allows applications to delegate the validation tasks to a trusted Validation Authority. SCVP is a protocol for determining the path between an X.509 digital certificate and a trusted root; and the validation of that path according to a particular validation policy. An SCVP service supports two modes of operation that may be used in combination or separately:

- Delegated Path Discovery (DPD) - used to discover the path between an end entity certificate and a trusted root, and
- Delegated Path Validation (DPV) - to validate the path according to a pre-defined validation policy in SCVP Server.

EACP will offer SCVP based Validation in its ValidSuite. ValidSuite will offer many validation profiles so that to allow users and relying parties to select adequately the profile that fit in their business case. EACP will make available a set of API that allows users and relying parties to integrate these API with their application workflow and to connect seamlessly to the EACP Validation server to obtain the validation responses. EACP Validation server is implemented with the client-server mode, and access will be provided by an HTTP interface.

Users and relying parties need to develop validation client in order to be able to use the validation service. To that end, users and relying parties may address request for the validation API as well as for the validation documentation to the EACP PMA using the PMA address provided in the EACP CP document.

4.7 Interface for timestamping

Time Stamp Authority (TSA) Server provides independent and irrefutable proof of time for transactions, documents and digital signatures. It can be used to create legal weight evidence that business transactions occurred at a defined moment in time, that e-documents existed at a particular time and that they have not been subsequently altered. It can also independently prove when a digital signature

was applied by the signer so that its validity can be verified in the long-term, even after expiry or revocation of signer's digital credentials.

The EACP platform will provide the Time Stamp service that must be compliant with **RFC 3161** and its update referenced in **RFC 5816**. Creating one or more time stamping policy profiles identified by a specific Object Identifiers (OID) derived from the EACP OID arc. The timestamp interface is an http-based interface, which is configurable to enforce authentication and authorization through client-server authenticated by the TLS protocol.

Users may address request for EACP time stamping documentation to the EACP PMA using the PMA address provided in the EACP CP document.

4.8 Signing as a Service Interface

The EACP SignSuite is a platform allowing EACP users to seamlessly sign their documents, codes and other objects with minimum installation and configuration.

This platform will be hosted centrally by EACP and provide the service as a managed service. EACP SignSuite is suited for high volume activity for either detached digital signatures CMS/PKCS#7 (as described in **IETF RFC 5652 and in RFC 8933**), or embedded digital signatures for PDF, XML, as well as CAdES, XAdES and PAdES.

The EACP SignSuite interface can be provided as set of web services or as a set of API to be integrated with user's existing applications and platforms, so that to connect to the Signing as a Service Server hosted centrally by EACP. Optionally, a time-stamp from EACP Time-Stamp Authority can be embedded or used separately.

Users may address request for EACP SignSuite documentation to the EACP PMA using the PMA address provided in the EACP CP document

5 References

1. EACP Acronyms and Definitions
2. RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework
3. RFC 5280: Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List Profile.
4. RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
5. RFC 8954: Online Certificate Status Protocol (OCSP) Nonce Extension
6. RFC 5652 : Cryptographic Message Syntax (CMS)
7. RFC 8933 : Update to the Cryptographic Message Syntax (CMS) for Algorithm Identifier Protection
8. RFC 5055: Server-Based Certificate Validation Protocol – SCVP

9. RFC 8894: Simple Certificate Enrolment Protocol

10. RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

11. RFC 5816: ESSCertIDv2 Update for RFC 3161

12. RFC 8555: Automatic Certificate Management Environment (ACME)

13. RFC 3739: Internet X.509 Public Key Infrastructure - Qualified Certificates Profile.

14. RFC 4210: Internet X.509 Public Key Infrastructure - Certificate Management Protocol (CMP)

15. ETSI TS 102 042 V1.1.1 (2002-04): Electronic Signatures and Infrastructures (ESI) - Policy requirements for certification authorities issuing public key certificates

16. ETSI TS 101 456 v1.4.3 (2007-05): Electronic Signatures and Infrastructures (ESI) - Policy requirements for certification authorities issuing qualified certificates

17. REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

18. Trust Service Principles and Criteria for Certification Authorities – Version 2.

19. European Aviation – Common PKI Governance Model

20. RFC 8017: PKCS #1: RSA Cryptography Specifications - Version 2.2

21. RFC 2986: PKCS #10: Certification Request Syntax Specification - Version 1.7