EUROPEAN PAYMENTS COUNCIL
Towards our Single Payment Area

e-Mandates e-Operating Model

High Level Definition

Abstract	This is the High-level Definition for the development of an e-Operating Model for the support of e-Mandates in the SEPA Direct Debit Scheme.
Document Reference	EPC109-08
Issue	Version 1.0
Date of Issue	30 May 2008
Reason for Issue	Banking Consultation
Reviewed by	EPC
Produced by	EPC
Authorised by	EPC Plenary
Circulation	EPC Plenary Members

EPC AISBL Secretariat – Avenue de Tervueren 12 – B 1040 Brussels · Tel: + 32 2 733 35 33 · Fax: + 32 2 736 49 88
Enterprise N.º 0873.268.927 www.europeanpaymentscouncil.eu secretariat@europeanpaymentscouncil.eu

TABLE OF CONTENTS

FIGURES

TABLES

0 DOCUMENT INFORMATION

0.1 References

This section lists external references mentioned in this document. Use of square brackets throughout this document is used to reference documents in this list.

N.º	Document Number	Title	Issued by:
[1]	EPC306-07	e-Mandates Related to the SEPA Core Direct Debit Scheme – Service Description (Version 1.0)	EPC
[2]		e-Mandates Message Standard	SWIFT
[3]	EPC016-06	SEPA Direct Debit - Scheme Rulebook	EPC
[4]	RFC 2560	Internet X.509 Public Key Infrastructure – Online Certificate Status Protocol - OCSP	IETF
[5]	RFC 2616	Hypertext Transfer Protocol – HTTP/1.1	IETF
[6]	RFC 3280	Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile	IETF
[7]	RFC 3986	Uniform Resource Identifier (URI): Generic Syntax	IETF
[8]	RFC 4346	The Transport Layer Security (TLS) Protocol	IETF
[9]	XML	Extensible Markup Language (XML) 1.0	W3C
[10]	XMLDSIG	XML-Signature Syntax and Processing	W3C

0.1.1 Defined Terms

This document refers to various defined terms, which have a specific meaning in the context of this document. Chapter 7 includes a full list of defined terms used in this document.

0.2 Change History

Issue number	Dated	Reason for revision
V1.0	May 2008	First document

0.3 Purpose of Document

The EPC e-Operating Model is defined across the following three documents:

- The **High-level definition of the EPC e-Operating Model** presents a broad description of the e-Mandate e-Operating model, message flows, data model and general requirements for the solution and for the parties.

- The **Security Concept of the EPC e-Operating Model** has the objective of establishing a security platform via the definition of security requirements that must be fulfilled by the detailed specification in order to mitigate risks evaluated through a risk assessment.

- The **Detailed Specification of the EPC e-Operating Model** has the objective to make a comprehensive description of each requirement allowing an unambiguous implementation. It will include the implementation guidelines and a complete XML schema for the e-Operating Model.

This document defines the High-level definition for the EPC e-Operating Model. It takes as a basis the e-Mandates Service Description [1] and builds up an operating model that will be detailed in the following chapters:

Vision and objectives – Introduces the e-Operating Model, the context in which it is being developed, the scope of applicability, its vision and objectives.

e-Operating Model - Documents the e-Operating Model, covering the description of the operating model (including the enrolment process), the description of the parties of the model, message flows and the data model.

General requirements - Identifies the general requirements of the e-Operating Model covering the security issues and the routing / interoperability issues.

Parties' requirements - Identifies the requirements for all the participants in the e-Operating Model.

Messaging Use-Cases - Presents a summary of common actions for issuing, amending, and cancelling an e-Mandate.

1 MANAGEMENT SUMMARY

The e-Mandate service is an optional feature complementing the Core SDD Scheme. The process of issuing an e-Mandate will allow Debtors and Creditors to exchange mandates in a fully electronic way, presenting advantages for Debtors, Creditors, Creditor Banks, and Debtor Banks.

The objective of the e-Mandates is to replace the paper flow in the Mandate Flow, allowing the Debtors to issue, to amend and to cancel a Direct Debit Mandate using an electronic way, while the collection process stays the same as in the existing Core SDD Scheme. A Bank involved in the e-Mandate service may choose to act as Debtor Bank and/or as Creditor Bank for offering the e-Mandate related services.

The Creditors may offer an optional functionality by allowing Debtors to amend and cancel paper based mandates in an electronic way.

The e-Mandate is based on the Four Corner Model of the Core SDD Scheme and it adds two new entities that play a key role in the e-Mandates flow: the Routing Service and the Validation Service.

To implement the e-Mandate solution, the e-Mandate service description needs to be completed by a set of UNIFI (ISO 20022) XML messages and a technical standard (the e-Operating Model).

The e-Operating Model covers aspects such as guaranteed delivery, non-repudiation of emission/reception, authentication of sender, data integrity, encryption, compression, and it will be aligned with the EPC business requirements (e-Mandates Service Description), rules and best practices.

The e-Operating Model focuses on applicational data transport over the Internet between the Creditor Websites and Validation Services, through a Routing Service. Furthermore, in order to assure a secure communication between the Debtor and the Creditor, minimum security requirements are defined for Debtor Browsers.

This model considers that the total transaction time to request an e-Mandate should be acceptable to the Debtor, providing a fluid and responsive user experience. The transport mechanisms support the transmission of account access data validation (BIC, IBAN, etc) and are prepared for future enhancements such as multiple signatures.

The general requirements and the application data transportation between Debtor and Validation Service are out of scope of this document, as well as the security and authentication mechanisms of the online banking services.

The e-Operating Model is designed to allow the issuance, amendment and cancellation of e-Mandates with a clear focus on reachability and interoperability between different Routing Service providers and Validation Service providers. In this model, it is necessary to have the support of a Directory Service and Certification Authorities, in order to offer a trusted connection between Routing Services and Validation Services.

Routing Service providers use Directory Services as enablers for reachability to all trusted participant Debtor Banks, while Certification Authorities (which must meet the defined requirements) are used to securely qualify legitimate Validation Service providers and Routing Service providers.

The essential steps of the e-Operating Model are as follows (for the issue of an e-Mandate):

- The Debtor using a browser initiates the creation of an e-Mandate on the Creditor's Website, by entering all the required elements (including the Operational BIC and IBAN).
- The Creditor Website creates the e-Mandate proposal and submits it to a Routing Service provider (provided by the Creditor Bank). In order to identify the Validation Service, the Routing Service queries a Directory Service using the Operational BIC.
- The Routing Service submits the e-Mandate proposal to the Validation Service of the Debtor Bank. Mutual authentication between the Routing Service and the Validation Service is achieved by using certificates issued according to EPC requirements.
- The Validation Service performs the validation of the BIC, IBAN and account access.
- The Debtor is routed from the Creditor's Website to the Validation Service for the validation of the Debtor's authenticity.
- The Debtor must identify and authenticate himself according to the instructions received from the Debtor Bank.
- After a successful authentication, the Debtor confirms the e-Mandate and is routed back to the Creditors Website. The e-Mandate itself is then delivered to the Creditor through the initial Routing Service.
- The Creditor Website acknowledges the reception of the e-Mandate and confirms this to the Debtor.

2 VISION AND OBJECTIVES

2.1 Vision

"*The e-Mandate process is an optional feature complementing the SEPA Core SDD Scheme, currently under development. The process will allow Debtors and Creditors to agree on mandates in a fully electronic way. Issuing, amendment and cancellation of e-Mandates must be possible in an electronic way. In addition, the Debtor Bank has an important role in validation. This will allow the complete avoidance of paper administration in the mandate flow, while the collection process stays the same as in the existing Core Scheme."[1 section 1.2]*

The e-Mandate service is built upon the e-Operating Model that has the objective of establishing a trusted platform for models with a similar structure (e.g. SEPA Online Payments) implemented over open networks, assuring adequate levels of security and interoperability.

The e-Operating Model will define a platform to guarantee secure and reliable transactions between parties communicating over the internet. This assurance is achieved through contractual relationships between the parties and their respective banks, and through an infrastructure that provides a trusted environment for the interactions between parties.

The e-Operating Model will cover aspects such as guaranteed delivery, non-repudiation, data integrity, encryption and compression of exchanged information as well as authentication of the involved parties and it will be aligned with the EPC business requirements (e-Mandates Service Description [1]), rules and best practices.

2.2 Objectives

This document is intended for the use of any party that requires a high-level view of the e-Operating Model. Although this model is being devised to support e-Mandates, the design has taken into account that it should also support other services based on the four corner model. In this sense, references to e-Mandate throughout this document can be seen in generic terms as an *authorization*. Thus, whenever an *authorization* is required, this e-Operating Model can be applied.

This document provides an understanding of the e-Operating Model through the description of the following issues:

- Message flows and data model;
- Security requirements;
- Routing / interoperability requirements;
- Parties' general requirements.

3 E-OPERATING MODEL

3.1 Overview

The e-Mandates conceptual model is based on the Four Corner Model of the SDD Core Scheme, which introduces two new entities: the Routing Service and the Validation Service.

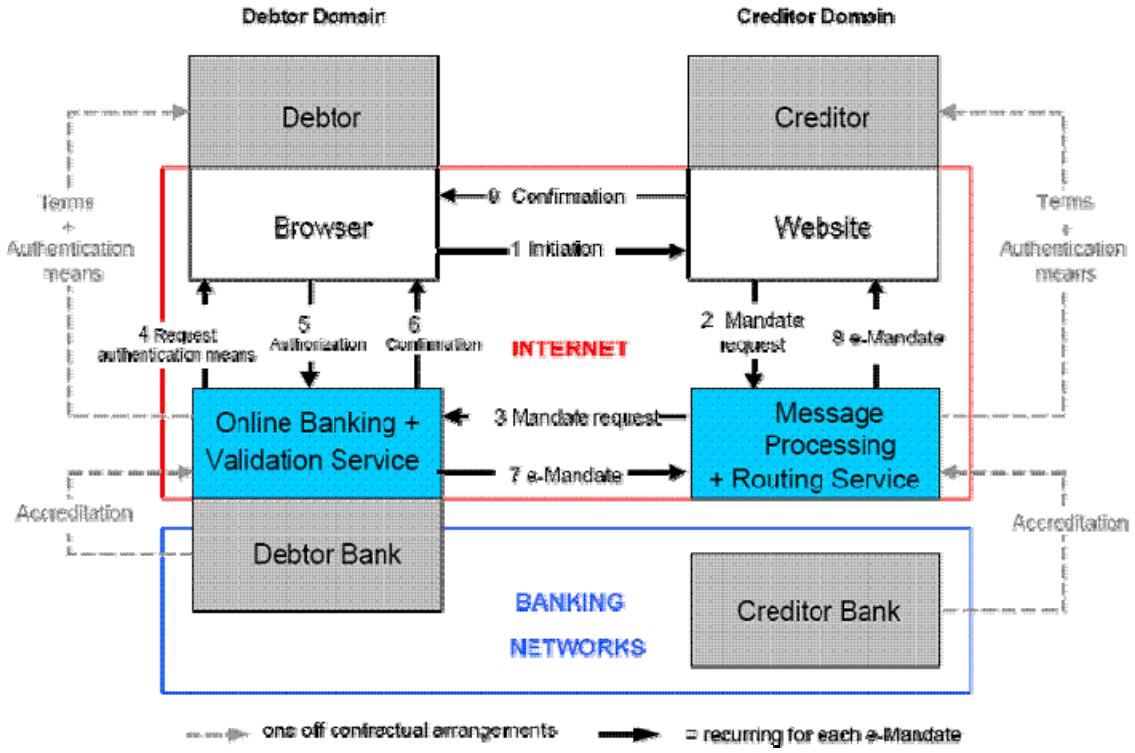

Figure 1: e-Mandate Conceptual Four Corner Model

To implement the e-Mandate conceptual model a technical standard was designed: the e-Operating Model.

3.2 Scope of the e-Operating Model

The e-Operating Model covers the application data transport over the Internet between the Creditor Websites and Validation Services making use of Routing Services.

The means of authentication between the Debtor and the Online Banking / Validation Service is out of scope.

The model was conceived to enable additional features such as extended account access validation, multiple debtor authentications and extended account validation.

This document only describes the process flow. The liabilities and responsibilities of each party are described in the e-Mandates Service Description [1].

3.3 e-Operating Model Parties

The execution of the e-Mandate service, complementing the SEPA Direct Debit Scheme, involves the following main parties:

- **The Debtor**: *"gives the Mandate to the Creditor to initiate Collections. The Debtor's bank account is debited in accordance with the Collections initiated by the Creditor. By definition, the Debtor is always the holder of the account to be debited"* [3], §3.1.

- **The Creditor**: *"receives the Mandate from the Debtor to initiate Collections, which are instructions to receive Funds from the Debtor Bank by debiting the account of the Debtor. On the basis of this Mandate, the Creditor collects the direct debits"* [3], §3.1

- **The Creditor Bank**: *"is the bank where the Creditor's account is held and which has concluded an agreement with the Creditor about the rules and conditions of a product based on the Scheme. On the basis of this agreement, it receives and executes instructions from the Creditor to initiate the Direct Debit Transaction by forwarding the Collection to the Debtor Bank in accordance with the Rulebook."* [3], §3.1.

- **The Debtor Bank**: *"is the bank where the account to be debited is held and which has concluded an agreement with the Debtor about the rules and conditions of a product based on the Scheme. On the basis of this agreement, it executes each Collection of the direct debit originated by the Creditor by debiting the Debtor's account, in accordance with the Rulebook."* [3], §3.1

- Providers of **Routing Services**: *"Providers offer this service, in agreement with and on behalf of Creditor Banks, for giving access, by Creditors, to validation services made available by Debtor Banks for the validation of e-Mandates initiated by Debtors through the electronic channels of Creditors. Creditor Banks may provide these routing services themselves."* [1], §1.5

- Providers of **Validation Services**: *"Providers offer this service in agreement with and on behalf of Debtor Banks for validation of e-Mandate proposals initiated by Debtors through the electronic channels of Creditors and the routing services offered by Creditor Banks. Debtor Banks may provide these validation services themselves."* [1] , §1.5

In order for the e-Operating Model to fulfil the reachability and security requirements, it is necessary to consider new parties: the Directory Service and the EPC Approved Certification Authority.

- Providers of **Directory Services**: Providers offer this service in agreement with a Routing Service Provider to provide for reachability to all participant Banks with the role of Debtor Bank. The directory must have an update list of all participant Debtor Banks' operational BICs and the correspondent Validation Service URLs.

- **EPC Approved Certification Authorities (CAs)**: PKI Certification Authorities that issue certificates for Validation Service providers and Routing Service providers, with extensions that qualify the entities as legitimate Validation Service providers or Routing Service providers. These CAs must present a "Declaration of Compliance" to the EPC.

In order to be authorised to offer the e-Mandate service, Participants must sign the appropriate Adherence Agreement (T.B.D.). In the enrolment process complementing the adherence process, Participants must provide the following information:

- Routing Service Name(s) / Address / etc (for Creditor Bank);
- Operational BIC of the bank (for Debtor Bank);
- Validation Service URL / Name / Address / etc (for Debtor Bank).

3.4 Principles

The e-Operating Model is based on the following principles, as stated in the e-Mandate Service Description [1]:

- It is not mandatory for Debtors to use this service, when offered by the Debtor Bank;
- The Debtor must have a commercial agreement with a Creditor and the Creditor must give access to his Website;
- The Debtor must have access to the Online Banking service provided by the Debtor Bank;
- The Debtor's Bank and the Debtor must have an agreement on the conditions for using the means of authentication;
- The Creditor and the Creditor's Bank must have an agreement on the conditions for using the Routing Service(s) providers;
- In order to participate, Routing Services must be accredited by Creditor Banks;
- The Creditor Bank must designate one or more Routing Service providers and must have an agreement with each one on the conditions of use;
- In order to participate, Validation Services must be accredited by Debtor Banks;
- The Validation Service will always respond to the Routing Service from which the enquiry was originated;

For technical purposes, the following additional principles are considered:

- In order to participate, Creditors must enroll with a Routing Service acting on-behalf of the Creditor Bank;
- All Routing Services must be able to connect with all e-Mandate Validation Services;
- A Routing Service must be able to connect at least to one Directory Service.

3.5 Model Description

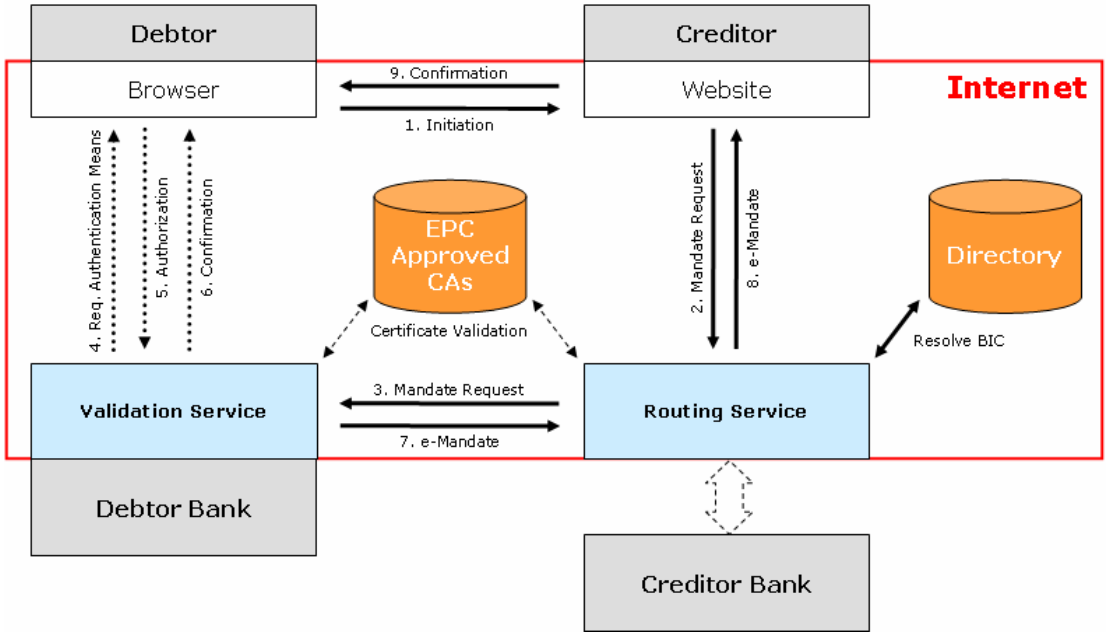

Figure 2: e-Operating Model

The Debtor accesses the Creditor's Website (flow 1, in Figure 2) using the browser for the completion of the Debtor Information by entering all the required elements (including the Operational BIC and IBAN).

Afterwards, the Creditor's Website creates the e-Mandate proposal by adding the Creditor Information to the Debtor Information and submits the e-Mandate proposal to a Routing Service (flow 2). In order to identify the Validation Service URL, the Routing Service queries a Directory Service using the provided Operational BIC.

Using the Validation Service URL of the Debtor Bank, the Routing Service submits the e-Mandate proposal (flow 3) to the Validation Service. The mutual authentication between the Routing Service and the Validation Service is achieved by using certificates issued by EPC Approved Certification Authorities. The Validation Service performs the validation of the BIC, IBAN and account access.

The Debtor is routed from the Creditor's Website to the Validation Service of the Debtor Bank (flow 4) for the authentication of the Debtor. The Debtor must identify and authenticate (flow 5) himself according to the instructions received from the Debtor Bank. The Debtor Bank defines and provides the authentication means that the Debtors should use.

After a successful authentication, the Debtor Bank confirms (flow 6) the result to the Debtor and returns the e-Mandate to the Creditor through the intermediary of the initial Routing Service (flows 7 and 8). The mutual authentication between the Routing Service and the Validation Service is achieved by using certificates issued by EPC Approved Certification Authorities.

The Debtor is routed back to the Creditor's Website which acknowledges the receipt of the e-Mandate and confirms this to the Debtor (flow 9).

3.6 Message flow

In order to implement the e-Operating Model, it is necessary to describe the message flow between the four parties: the Debtor's Browser (used by the Debtor), the Creditor's Website, the Routing Service and the Validation Service. The several interactions are illustrated in Figure 3.

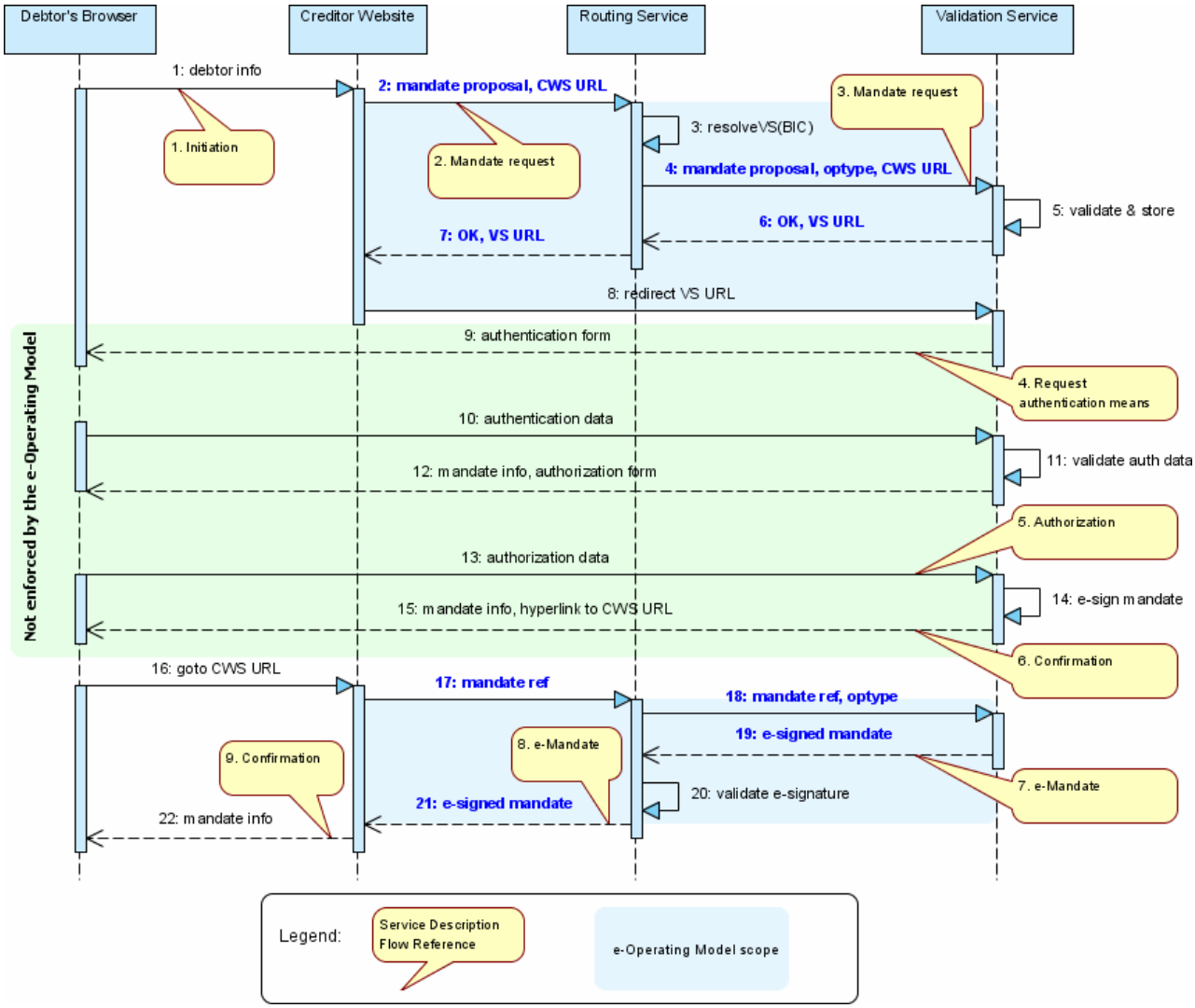

Figure 3: Message Flow

The message flow is described on Table 1 and applies to all available e-Mandate operations (issuing, amendment and cancellation).

Table 1: Message Flow description

Step	Action	Service Description flow Reference	Data
1	The Debtor using an Internet Browser accesses the Creditor's Website. The Debtor must validate that the presented Creditor Information is correct (Creditor Name, Address, etc) and mandatory legal advertisements are shown. The Debtor selects the transaction (issuing, amendment and cancellation) and the Creditor's Website presents a form to collect the Debtor's information required for the transaction (e.g. BIC and IBAN for an e-Mandate issuance). The Website may already have some Debtor information stored and pre-fill some of the fields.	1. Initiation	Debtor Info
2	Using the information provided by the Debtor, the Creditor's Website merges the Debtor data with the required Creditor information to generate the e-Mandate proposal message. Regardless of the information that is transported for the e-Mandate service, the BIC and IBAN will be mandatory fields for the routing of the message and the identification of the Debtor. The Creditor's Website (CWS URL) must also be included so as to redirect the Debtor back to Creditor at a later stage (step 15). The message, along with the CWS URL, is submitted to the Routing Service using the URL and credentials provided by the Creditor Bank (issued by the Routing Service Provider) or directly by the Routing Service Provider. The credentials may include a certificate, username/password or other secure means.	2. Mandate Request	e-mandate proposal, CWS URL
3	After verifying the Creditor's credentials, the Routing Service receives the e-Mandate proposal message and validates that all the required fields are filled-in. The Routing Service then looks up the Directory Service (either an online request or a cached mapping) to resolve the Operational BIC into the Validation Service URL. This operation is further detailed in **section 3.6.1**. The access to the Directory Service must be performed using the credentials provided by the Directory Service Provider. The Directory Service returns the Validation Service URL for the provided Operational BIC.		BIC (input), Validation Service URL

Step	Action	Service Description flow Reference	Data
4	The Routing Service dispatches the request received to the Validation Service URL indicating that this is an e-Mandate enrolment request (optype). The Routing Service must present a client certificate issued by an EPC approved CA qualifying it as legitimate Routing Service and the Validation Service must present a server certificate issued by an EPC approved CA qualifying it as a legitimate Validation Service (see section 4.2).	3. Mandate Request	e-mandate proposal, optype, CWS URL
5	The Validation Service validates the e-Mandate proposal (BIC, IBAN, user account access, etc) and stores the information.		e-mandate proposal, optype, CWS URL
6	The Validation Service returns a status code (OK) and a URL specific to this transaction (VS URL), which will be used on step 8 to redirect the Debtor's browser.		OK, VS URL
7	The Validation Service response is returned to the Creditor's Website.		OK, VS URL
8	The Creditor, which is still holding the control of the Debtor's browser, performs a redirect to the given Validation Service URL.		VS URL
9	The Debtor is redirected from the Creditor's Website to an authentication screen offered by the Validation Service to the Debtor, in order to authenticate the Debtor.	4. Request authentication means	authentication form
10	The Debtor enters the authentication credentials agreed with the Debtor Bank The authentication credentials may be composed of personalised device(s) and/or a set of procedures, including its personalized security features ([1] PT-07.03).		authentication data
11	The Validation Service verifies the correctness of the authentication credentials provided.		authentication data
12	If the authentication credentials provided are correct and valid, the Validation Service presents an authorization form along with all the mandate data.		mandate info, authorization form
13	The Debtor is asked to verify the mandate data (e.g., the accuracy of the Creditor information, for example, name and address) and proceeds with the authorization. The authorization is defined here as the set of procedures agreed between the Debtor and the Debtor Bank to assure the clear consent of the Debtor for the issuing, amendment and cancellation of an e-Mandate.	5. Authorization	authorization data
14	The Validation Service verifies the authorization and performs an electronic signature of the e-Mandate data.		e-mandate (input), electronically signed e-mandate (output)

Step	Action	Service Description flow Reference	Data
15	The Validation Service presents a confirmation message to the Debtor along with the e-Mandate data and a link to the Creditor's Website (URL provided on step 4)	6. Confirmation	mandate info, CWS URL
16	The Debtor follows the link to the Creditor's Website.		CWS URL
17	The Creditor's Website recovers the e-Mandate transaction data and sends a request with the e-Mandate reference (e-Mandate ref) to the arranged Routing Service in order to retrieve the issued e-Mandate. The Creditor must present the credentials previously arranged with the Routing Service provider (similar to step 2).		e-mandate reference
18	The Routing Service dispatches the e-Mandate retrieving request to the same Validation Service URL resolved in step 3, indicating that this is a retrieval operation (optype). The Routing Service must present a client certificate issued by an EPC approved CA qualifying it as legitimate Routing Service and the Validation Service must present a server certificate issued by an EPC approved CA qualifying it as a legitimate Validation Service (see section 4.2).		e-mandate reference, optype
19	If the authentication credentials are correctly validated, the Validation Service returns the electronically signed e-Mandate to the Routing Service.	7. e-Mandate	e-signed mandate
20	The Routing Service performs a validation of the e-Mandate electronic signature received. This operation is further detailed in **section 3.6.2.**		e-signed mandate
21	The Routing Service returns the electronically signed e-Mandate to the Creditor's Website.	8. e-Mandate	e-signed mandate
22	The Creditor's Website presents a confirmation message along with the e-Mandate data to the Debtor. The Creditor stores the electronically signed e-Mandate XML file according to national legal requirements.	9. Confirmation	mandate info

The data sets exchanged in each of the steps are the same for all the operations defined for e-Mandates: issuance, amendment and cancellation. However, some of the optional fields defined in the e-Mandate request message (DS-12, [1]; [2]) and the e-Mandate validation message (DS-13, [1]; [2]) may be required for some of the operations.

The data exchanged in the scope of this e-Operating Model is described on Table 2.

Table 2: Description of data exchanged

Step	Data	Description
2	e-mandate proposal	e-Mandate proposal message data, as defined in DS-12 ([1]; [2])
	CWS URL	Creditor's Website return URL, including enough data to restore the transaction processing at a later stage, on step 16
4	e-mandate proposal	As received in step 2
	Operation type	Type of operation: request
	CWS URL	As received in step 2
6	OK	Status data: • Processing timestamp • Status code • Status message, in case of error • e-Mandate proposal message, in case of error
	VS URL	Validation Service URL to redirect Debtor, including key data to be able to retrieve Debtor's information and the e-Mandate proposal message received on step 8
7	OK	Status data: • Processing timestamp • Status code • Status message, in case of error • e-Mandate proposal message, in case of error
	VS URL	As received on step 6
17	e-Mandate ref	Creditor e-Mandate Reference (field AT-01 [1];[2])
18	e-Mandate ref	As received in step 17
	Operation type	Type of operation: retrieval
19	e-signed e-Mandate	e-Mandate validation message as defined in DS-13 ([1]; [2]), enveloped on a XML Signature [10]
21	e-signed e-Mandate	As received in step 19

3.6.1 BIC Resolution

In order to contact the corresponding Validation Services, the Routing Service providers must be able to resolve BICs into Validation Service URLs (**Step 3** in the message flow). This is achieved by using Directory Services that maps the Debtor's Bank Operational BICs into the designated Validation Service URLs.

The BIC Resolution process can be performed in two ways:

1. An online query, where the Routing Service provides the Operational BIC and the Directory Service (DS) returns the corresponding Validation Service URL. For faster processing and improved service availability, it is recommended that Routing Service providers implement a cache strategy to avoid repeated requests on frequent BICs. This is illustrated in Figure 4.

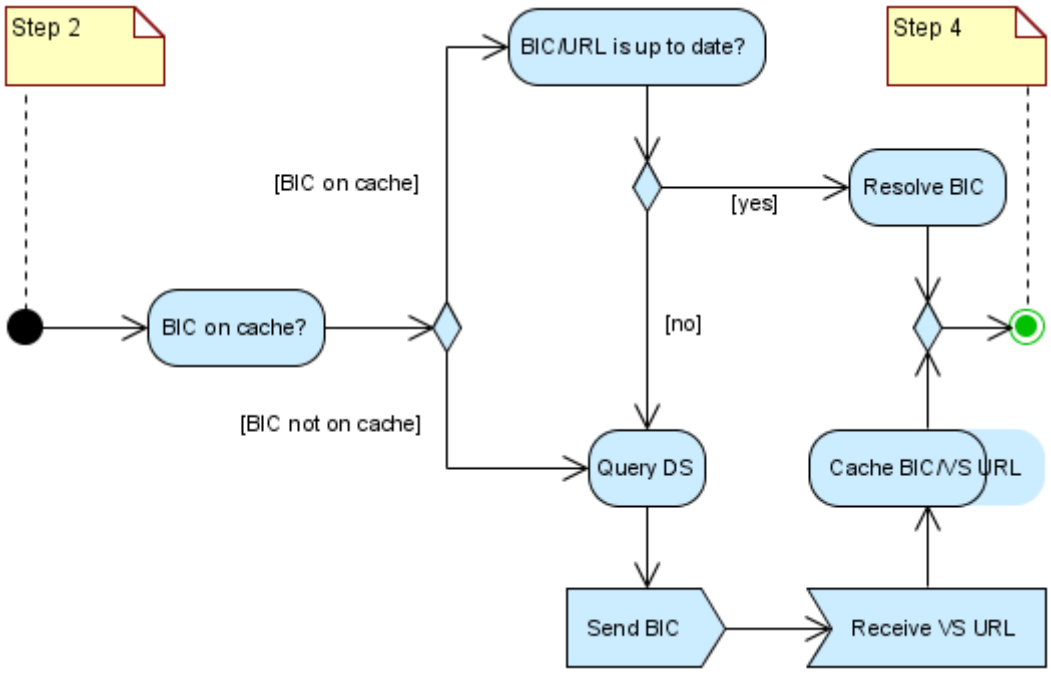

Figure 4: Online Validation Service resolution

2. An offline cache-based resolution, where the Directory Service publishes the full list of Operational BIC/Validation Service URL mapping data and also the next expiry date. Subscribing Routing Services download the mapping file at the announced periodic updating dates and cache it (see Figure 5). The resolution can then be performed internally (Figure 6).

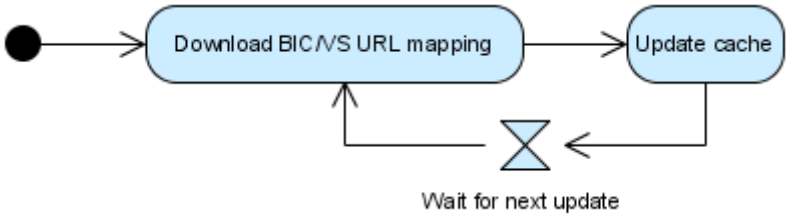

Figure 5: Caching of full Validation Service resolution tables

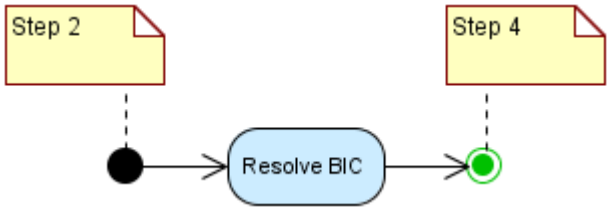

Figure 6: Offline Validation Service resolution

3.6.2 Validation of e-Mandate electronic signature

The validation of an e-Mandate electronic signature is performed in **Step 20** on the message flow by the Routing Services after receiving the e-Mandate.

An e-Mandate is considered to be valid if and only if all of the following verifications are met (Figure 7):

1. The cryptographic verification of the electronic signature value succeeds, according to the defined algorithms;

2. The signing certificate was valid at the signing date (see section 3.6.3).

If any of the conditions above fail, the signature must be considered invalid and the e-Mandate discarded.

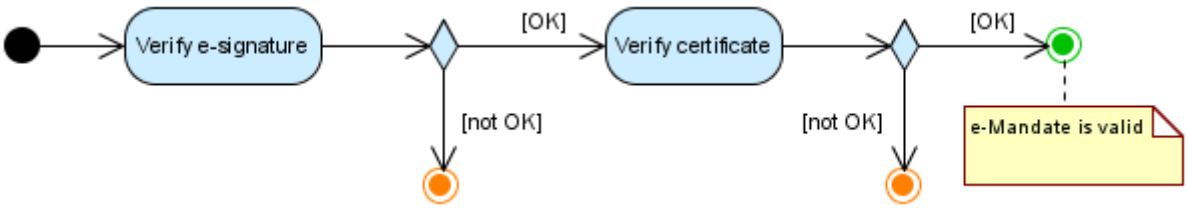

Figure 7: e-Mandate electronic signature validation

3.6.3 Validation of certificate

A X.509 certificate [6] is considered to be valid at a given date if and only if (Figure 8) all the following conditions are met:

1. The certificate has the specific e-Operating Model extension;
2. The given date is within the certificate begin and end validity dates;
3. A certification path ([6] §6.1) can be built up to any of the trusted EPC approved Certification Authorities;
4. The certificate is correctly signed by the issuing Certification Authority;
5. The certificate was not revoked at the given date.

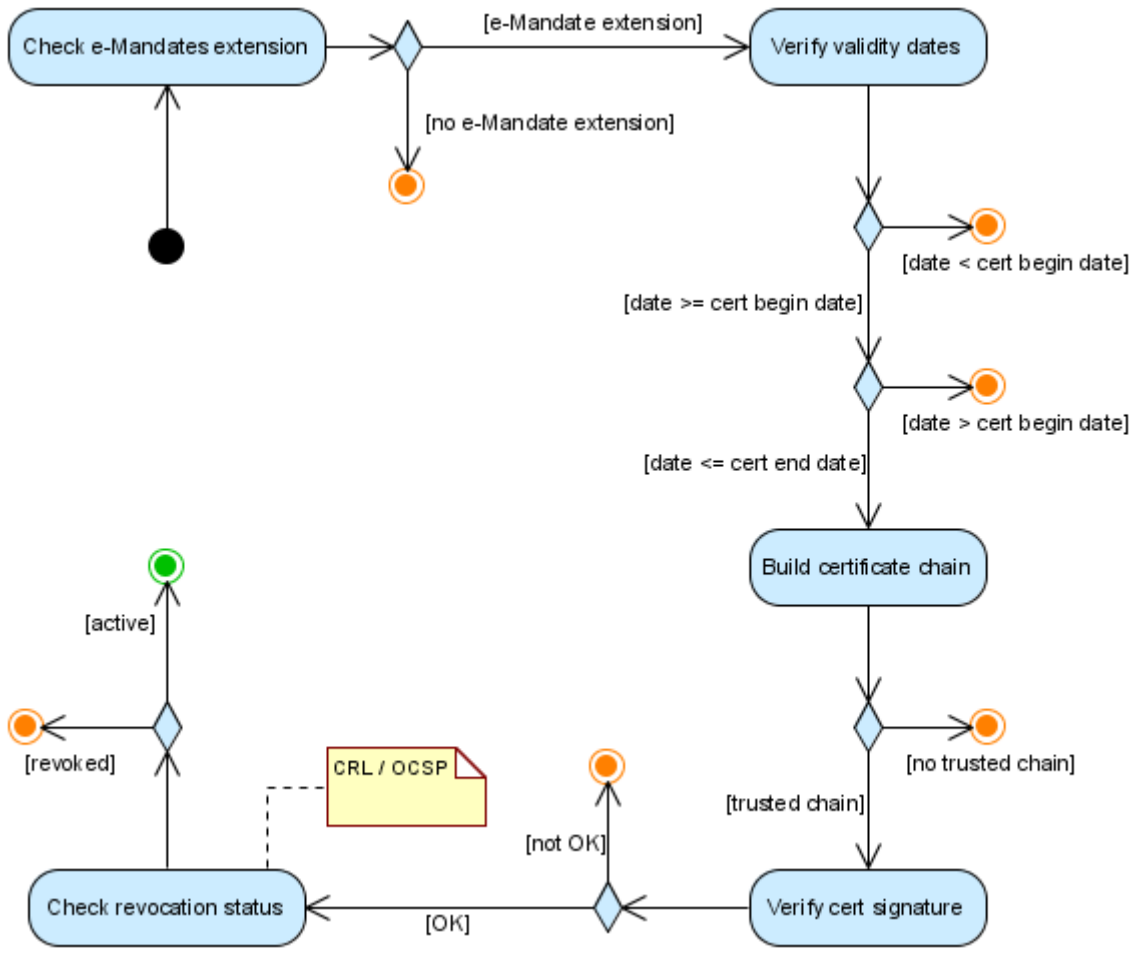

Figure 8: Certificate validation

If any of the conditions above fail, the certificate must be considered invalid and discarded.

3.7 State transitions

On the course of a transaction, each party advances progressively from one state to the next one until its participation in the process is not further required. In this context, a state is considered to be a waiting period in which the party is idle and awaiting for input or a response from another party. When such an input/response is received, some sort of activity is performed and the system advances to the next waiting state.

The figures below illustrate all the possible states for Creditor Websites, Routing Services and Validation Services. The indicated *steps* refer to the steps of the message flow (described in section 3.6).

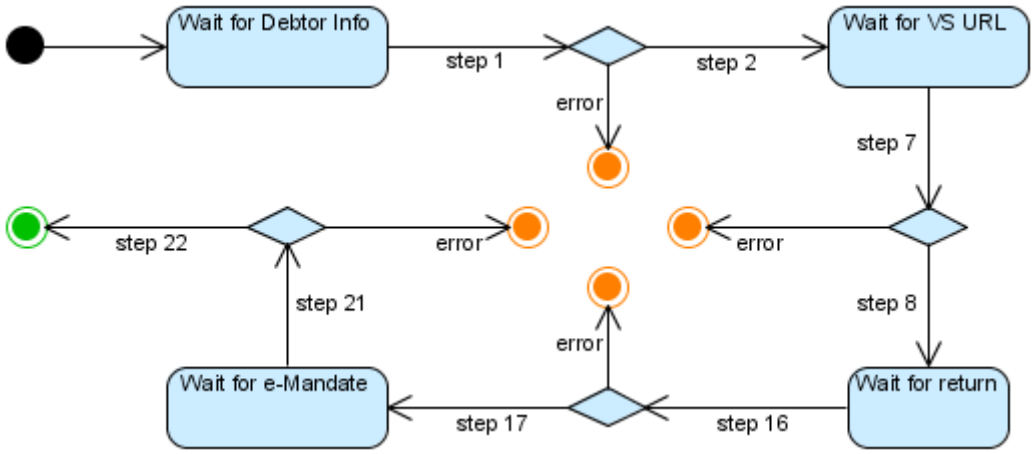

Figure 9: State diagram for Creditor Websites

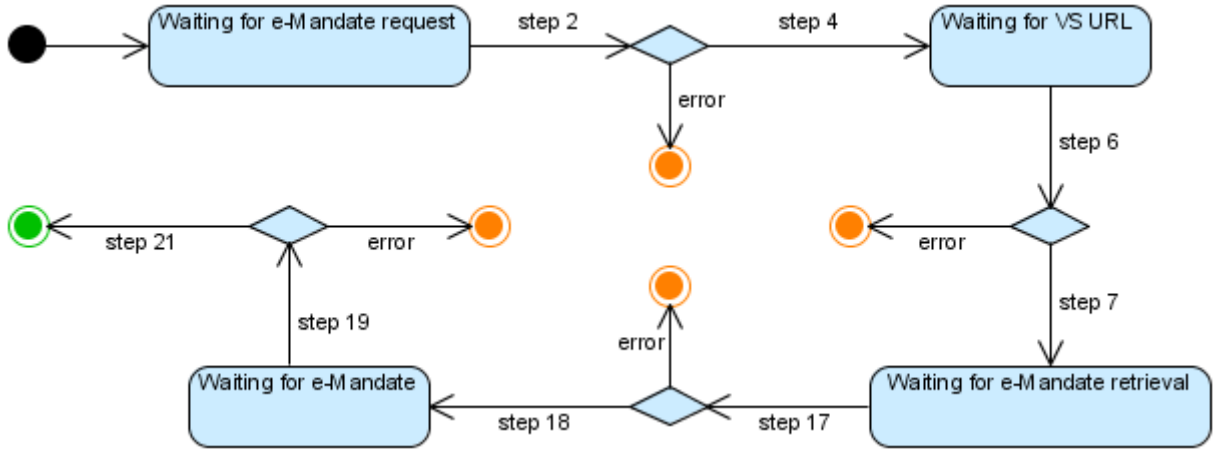

Figure 10: State diagram for Routing Services

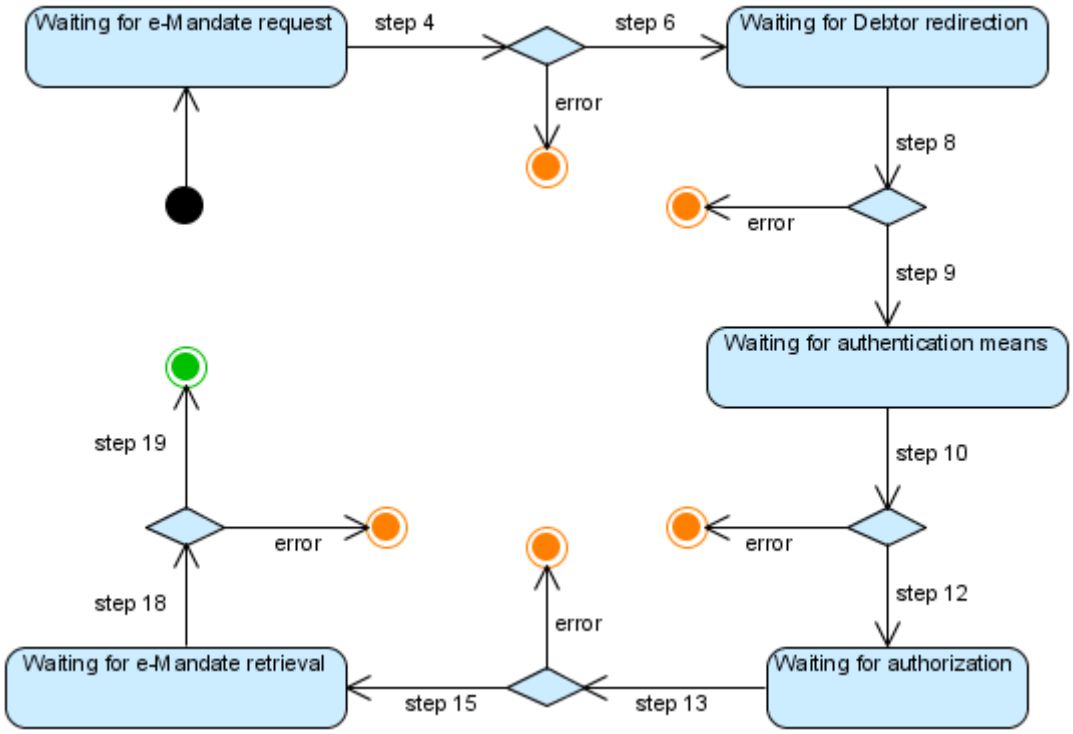

Figure 11: State diagram for Validation Services

3.8 Error handling

The message flow described on section 3.6 corresponds to a successful transaction. Nonetheless, errors may occur during the whole process and the e-Operating Model supports them.

Each of the state diagrams on section 3.7 illustrates the possible transitions to errors, which may be classified as:

- **Business errors** – resulting from data validation of business messages (e.g., e-Mandate proposal);
- **Protocol errors** – resulting from transport, interoperability and security failures.

Protocol errors will be fully detailed in subsequent e-Operating Model documents and the description of how each involved party must handle them.

Although business errors are not described by the e-Operating Model, the transport of these errors between the different parties is supported.

4 GENERAL REQUIREMENTS

4.1 Security

4.1.1 Introduction

The e-Operating Model design is intended for Internet use, meaning that the interactions between the different parties take place across interlinked public networks. These networks have been subject to a great number and variety of threats during the past years. Banking and e-commerce services provided on the Internet have been specially targeted in recent years given the potential financial benefits that can be gained by the perpetrators. Entities providing these services have been able to adapt and counter these attacks at some expense.

The e-Operating Model interconnects a vast number and variety of parties and therefore the capability to respond to threats are unavoidably cumbersome. Thus, the security requirements for this model are raised to a level as to minimize the need for change when confronted with new threats.

Although liability issues are out of scope of this document, security mechanisms are integrated in this model to support them.

4.1.2 Security Principles

The security principles that have been set to support this model are the following:

- **Confidentiality and Data Privacy**
  - All data transmitted between parties that cross unprotected areas must be protected from eavesdropping by adopting appropriate encryption mechanisms;
  - Confidentiality-wise critical data must be stored in adequate means to limit the possibility of disclosure to unauthorized parties;
  - Data must be conveyed between parties in such a fashion as to follow a need-to-know principle.
- **Integrity**
  - All data transmitted between parties that cross unprotected areas must be protected against tampering through the adoption of integrity mechanisms;
  - Integrity-wise critical data must be stored in adequate means to limit the possibility of unauthorized or unintentional modification.
- **Authentication**
  - Wherever appropriate, parties must be mutually authenticated.
- **Non-repudiation**
  - All critical data in support to liability issues must be electronically signed.

4.1.3 Security Mechanisms

Various security mechanisms are publicly available to fulfil the enumerated security principles. The criteria for the selection of the mechanisms are to adopt technologies and protocols that have proven to withstand time and the scrutiny of implementations subject to trial.

The mechanisms hereby presented are at two levels: the transport level and the application level. The Certification Authorities are the key enablers for those mechanisms.

4.1.3.1 Transport Level

TLS[8] is a cryptographic protocol that provides secure communications over the Internet.

TLS incorporates, as a basis, a variety of security features, most importantly:

- Exchanged data is ciphered, thus protected from eavesdropping and guaranteeing confidentiality;
- Integrity of exchanged data is guaranteed through the use of Message Authentication Codes, thus protecting data tampering;
- Authentication of the server to which a party is connecting is attested through the use of electronic signatures (server certificates).

Optionally TLS supports authentication of the party initiating the session via the usage of client certificates. Adopting this option guarantees a mutual authentication between participants.

4.1.3.2 Application Level

Electronic signatures are a form of providing integrity, repudiation of fraudulent messages and non-repudiation of legitimate messages. If an electronic signature is successfully verified, it is guaranteed that the contents of the corresponding message are known and confirmed by the signing party and that no changes have occurred since it was electronically signed.

The e-Operating model applies electronic signatures to XML messages by using the XML Signature standard [10].

4.1.3.3 Certification Authorities

A Certification Authority is a trusted third party guaranteeing that a specific certificate belongs to a named entity. Trusting a Certification Authority provides that all certificates issued and not revoked by that Certification Authority can be trusted and correctly authenticated.

4.1.4 Certificate infrastructure

The identified mechanisms make use of certificates, either for TLS or for XML Signatures. This section describes the type of certificates that each party uses and describes the involved Certification Authorities that will guarantee the chain of trust between parties.

The full set of certificates necessary for this e-Operating Model is illustrated in Figure 12.

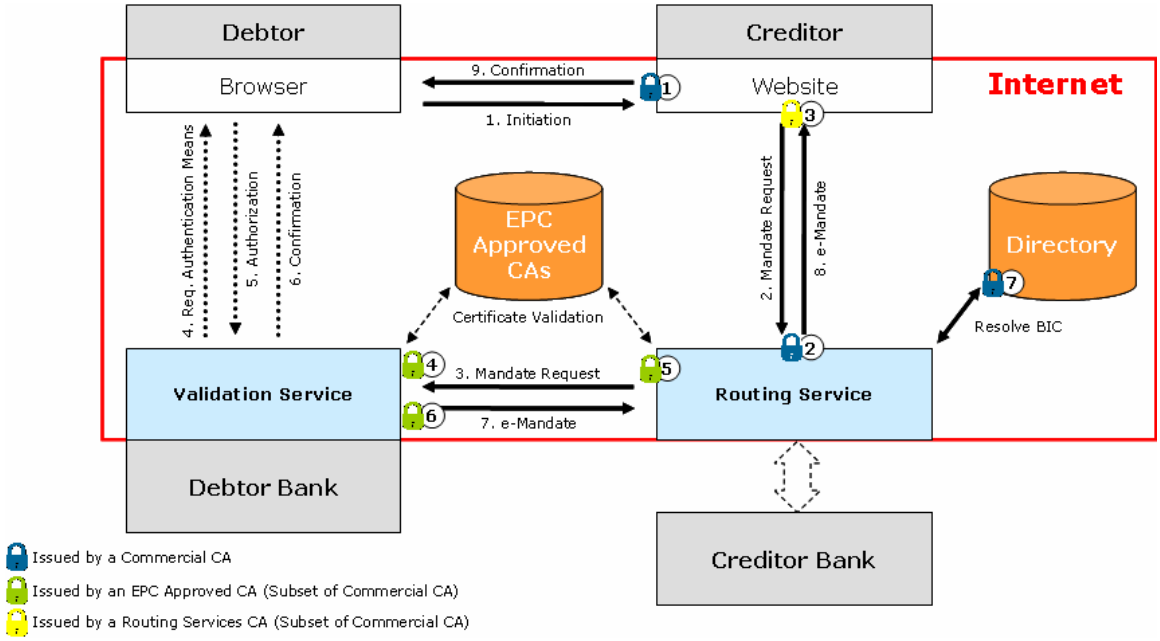

Figure 12: PKI and certificates for the e-Operating model.

Table 3 presents a description of the certificates depicted in Figure 12.

Table 3: Description of the e-Operating Model certificates.

Ref	Certificate Type	CA	Authenticated Object	Verifying Party	Description
1	TLS Server	Commercial	Creditor	Debtor	Authenticates the Creditor to the Debtor. Protects the communication between these two parties.
2	TLS Server	Commercial	Routing Service	Creditor	Authenticates the Routing Service to the Creditor. Protects the communication between these two parties.
3	TLS Client	Routing Service CA	Creditor	Routing Service	(Optional) Authenticates the Creditor to the Routing Service.
4	TLS Server	EPC approved	Validation Service	Routing Service	Authenticates the Validation Service to the Routing Service. This certificate is specific for the Validation Services of the e-Operating Model. Protects the communication between these two parties.

Ref	Certificate Type	CA	Authenticated Object	Verifying Party	Description
5	TLS Client	EPC approved	Routing Service	Validation Service	Authenticates the Routing Service to the Validation Service. This certificate is specific for the Routing Service of the e-Operating Model.
6	Signing	EPC approved	Validation Service e-mandate	Routing Service	Signs messages in the e-Operating Model through the use of a specific certificate for this purpose.
7	TLS Server	Commercial	Directory Service	Routing Service	Authenticates the Directory Service to the Routing Service. Protects the communication between these two parties.

The certificates described on Table 3 must be issued by Certification Authorities (CA). In order to guarantee full interoperability between the different Routing Service and Validation Service providers, it is necessary that all of them share the same "trust anchors". This means that a well known set of root Certification Authorities approved by the EPC must be trusted by all Routing Service and Validation Service providers.

The Certification Authorities allowed in the e-Operating Model can be classified in the following categories:

- **Commercial Certification Authorities** are current market established CAs, generally trusted by browsers and server frameworks. Interoperability of certificates issued by these CAs is out of the scope of this e-Operating model;

- **EPC approved Certification Authority** is a CA that issues certificates according to the e-Operating defined certificate profiles and complies with the defined enrolment terms for applying entities (Routing Services and Validation Services). An applying CA must present a "Declaration of Compliance" to the EPC in order to be accepted and must be listed on the EPC portal as an Approved CA. Appropriate enrolment terms for applying entities assure that only legitimate Validation Services and Routing Services are issued with these certificates dedicated to provide mutual authentication between parties;

- **Routing Service CA** is a CA that issues TLS client certificates for Creditors by request of the Routing Service. This provides stronger authentication of Creditors for the Routing Service. The Routing Service CA can be a commercial available CA for which the Routing Service settles an agreement or a self-owned specific purpose CA.

4.2 Routing and interoperability

According to the message flow described on section 3.6, Routing Service providers are responsible for delivering the messages exchanged between Creditors and Validation Service providers. Therefore, Routing Service providers must "be able to connect" to every Validation Service provider available. In order to do so, the following conditions must be met by the Routing Service:

1. The URL address of the target Validation Service must be known;
2. The Validation Service must be authenticated as a legitimate one;
3. Must provide credentials so that the Validation Service can be guaranteed that it is a legitimate Routing Service provider.

Condition 1 is achieved by resolving the BIC into the Validation Service provider URL using the Directory Service as defined on section 3.6.1.

Condition 2 is achieved by using "SEPA Validation Service" certificates and condition 3 is achieved by using "SEPA Routing Service" certificates. These two types of certificates, described on section 4.1.4, are used to establish secure HTTP connections over TLS. Both parties taking place on such a session must validate the presented certificates similarly as described in section 3.6.3.

4.3 Processing time

The total transaction time to request an e-Mandate should be acceptable to the Debtor, providing a fluid and responsive user experience. Parties must be aware that the Debtor will be guided through several different screens and, at the Validation Service/Online Banking, will be authenticated through specific means that can greatly extend the total transaction time.

5 PARTIES' REQUIREMENTS

5.1 Debtor browser requirements

The Debtor must use a web browser compliant with the Creditor's Website.

In the context of this e-Operating model, the strict requirements for the web browser are:

- HTTP 1.1 support;
- Ability to perform HTTP redirects.

In addition to the above general requirements, security requirements must be fulfilled. In order to establish secure connections between the Debtor Browser and the Creditor's Website, the browser must support TLS with strong cipher suites and have the security options enabled.

5.2 Creditor's website requirements

Creditors willing to implement the e-Mandate service of the SDD scheme must comply with the following general requirements:

- Provide to Debtors access to a management area where e-Mandates can be queried, issued, amended and cancelled;
- SEPA branding material and mandatory wording must be displayed during the whole e-Mandate transaction to provide Debtors with a coherent, consistent and recognizable experience across multiple Creditors;
- The electronically signed e-Mandate must be stored intact by the Creditor as long as the e-Mandate exists, according to national legal requirements;
- After cancellation, the e-Mandate must be stored by the Creditor for a period according to the applicable national legal requirements.

In addition to the above general requirements, Creditor Websites must comply with the following security requirements:

- In order to establish secure connections between the Debtor Browser and the Creditor's Website, the server must use HTTP over TLS (HTTPS). The Creditor's Website must provide access to the e-Mandates functionalities to Debtors only through appropriately secure authentication means;
- A client certificate must be assigned by the Routing Service provider to the Creditor's Website. On each HTTPS connection, the certificate must be presented for authentication and the Creditor must also authenticate the server certificate presented by the Routing Service provider;
- TLS must be performed using only strong cipher suites; weak cipher suites must be disabled on the web server.

5.3 Routing Service Provider requirements

Routing Service providers must observe the following general requirements:

- Routing Service providers must use a Directory Service containing all the operational BICs of the Participant Banks and has well defined and secure procedures to update the BICs and Validation Service URLs;

- For faster processing, Routing Service providers should cache the directory service data and implement mechanisms to update it periodically and whenever required;

- For privacy concerns, Routing Service providers must not store any Debtor private information related with e-Mandates, but must log all significant events about the transactions and keep their state on transaction life-cycle. The log should register information for complete traceability / audit of the e-Mandates (URL, destination BIC, e-mandate unique ID, state, error code, timestamp, etc). The log must be protected against tampering.

Besides the above general requirements, Routing Service providers must comply with the following security requirements:

- In order to establish secure connections between the Creditor's Website and the Routing Service provider, HTTP over TLS (HTTPS) must be used;

- A TLS client certificate must be assigned by the Routing Service provider to the Creditor's Website. On each HTTPS connection, the certificate will be presented by the Creditor for authentication. For mutual authentication, the Routing Service provider must also present a TLS server certificate;

- Must trust all EPC approved Certification Authorities;

- In order to establish secure and interoperable connections between the Routing Service provider and all the Validation Service providers, the Routing Service must use a TLS client certificate issued by an approved EPC Certification Authority with the specific "SEPA Routing Service" extension. For mutual authentication, Validation Service providers will present a TLS server certificate issued by an approved EPC Certification Authority with the specific "SEPA Validation Service" extension;

- All certificates must be validated in accordance with the process described on section 4.2;

- All electronic signatures must be validated in accordance with the process described on section 3.6.2;

- TLS must be performed using only strong cipher suites; weak cipher suites must be disabled on the web server.

5.4 Validation Service Provider requirements

Validation Service providers must observe the following general requirements:

- Validation Service providers must be able to access the respective Online Banking Service in order to perform initial validations like the debtor's rights to access the account, IBAN validation, etc;
- Validation service must log all significant events about the transactions and keep their state on transaction life-cycle. The log should register information for complete traceability / audit of the e-Mandates (URL, destination BIC, e-mandate unique ID, state, error code, timestamp, etc). The log must be protected against tampering.

In addition to the above general requirements, Validation Service providers must comply with the following security requirements:

- Sensitive data must be stored in ciphered form;
- All systems supporting the service must be protected against unauthorized access;
- All e-Mandates must be electronically signed using a dedicated security equipment such as a Hardware Security Module with an electronic signing certificate (X.509);
- Must trust all EPC approved Certification Authorities;
- In order to establish secure and interoperable connections between all the Routing Service providers and the Validation Service provider, the Validation Service must use a TLS server certificate issued by an approved EPC Certification Authority with the specific "SEPA Validation Service" extension. For mutual authentication, Validation Service providers will present a TLS client certificate issued by an approved EPC Certification Authority with the specific "SEPA Routing Service" extension;
- All certificates must be validated in accordance with the process described on section 4.2;
- TLS must be performed using only strong cipher suites; weak cipher suites must be disabled on the web server.

5.5 Directory Service

Directory Service providers must observe the following general requirements:

- The Directory Service must have all the operational BIC of the Participant Banks with the role of Debtor Banks and the corresponding Validation Service URL;
- The directory service must update the information of routing tables on a regular basis;
- The directory can have only one Validation Service URL per BIC, but can have more than one BIC per Validation Service URL.

In addition to the above general requirements, Directory Service providers must comply with the following security requirements:

- In order to establish secure connections between the Directory Service and the Routing Service providers, HTTP over TLS (HTTPS) must be used;
- TLS must be performed using only strong cipher suites; weak cipher suites must be disabled on the web server;
- Information must be protected against unauthorized modification;
- Must perform automatic regular data base integrity checks.

5.6 Certification Authority

In order to be accepted and listed on the EPC portal as an EPC approved Certification Authority (CA), an applying CA must comply with the following requirements:

- Be able to issue certificates in accordance with the customized certificate profiles defined in this e-Operating model;
- Strictly follow the defined enrolment steps for applying Routing Service and Validation Service providers;
- Offer access for Certificate Revocation List (CRL) status validation and, optionally, an Online Certificate Status Protocol (OCSP) service.

6 MESSAGING USE-CASES

This chapter presents a summary of the main e-Mandate use cases, both from the Debtor perspective (see Figure 13) and from other parties' perspective (automated systems).

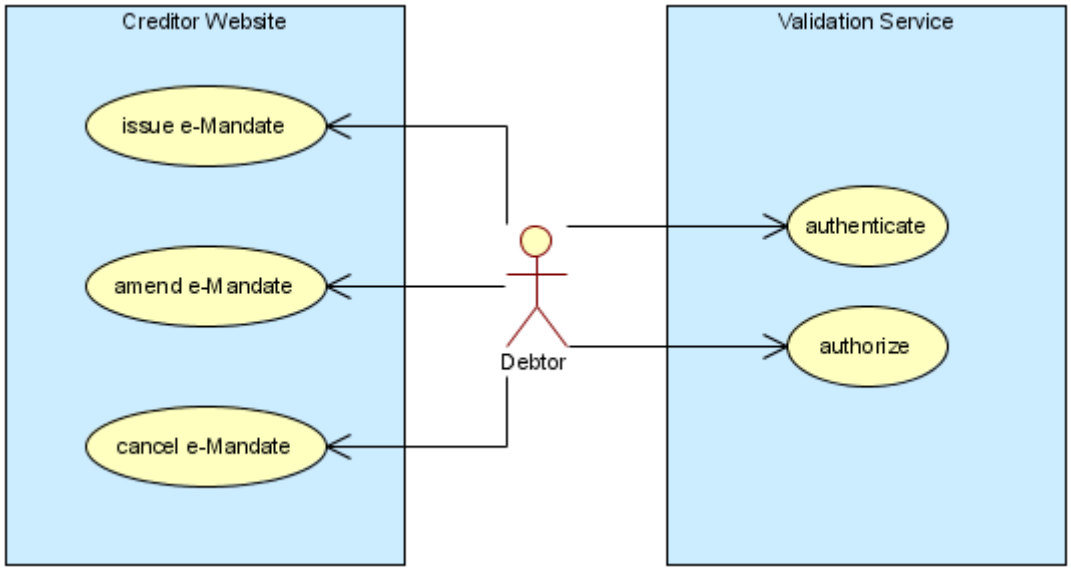

Figure 13: Debtor's use cases

From the point of view of the Debtor, five operations are available:

1. *Issue e-Mandate*, offered by the Creditor's Website, relates to the issuance of a new e-Mandate and corresponds to PR-07 [1];

2. *Amend e-Mandate*, offered by the Creditor's Website, which relates to the amendment of an existing e-Mandate and corresponds to PR-08 [1];

3. *Cancel e-Mandate*, offered by the Creditor's Website, which relates to the cancellation of an existing e-Mandate and corresponds to PR-09 [1];

4. *Authenticate*, offered by the Validation Service, which relates to the authentication requested by the Debtor Bank;

5. *Authorize*, offered by the Validation Service, which relates to the authorization needed for proceeding with the e-Mandate process.

Figure 14 illustrates the detailed use cases from the parties' perspective (automated systems).

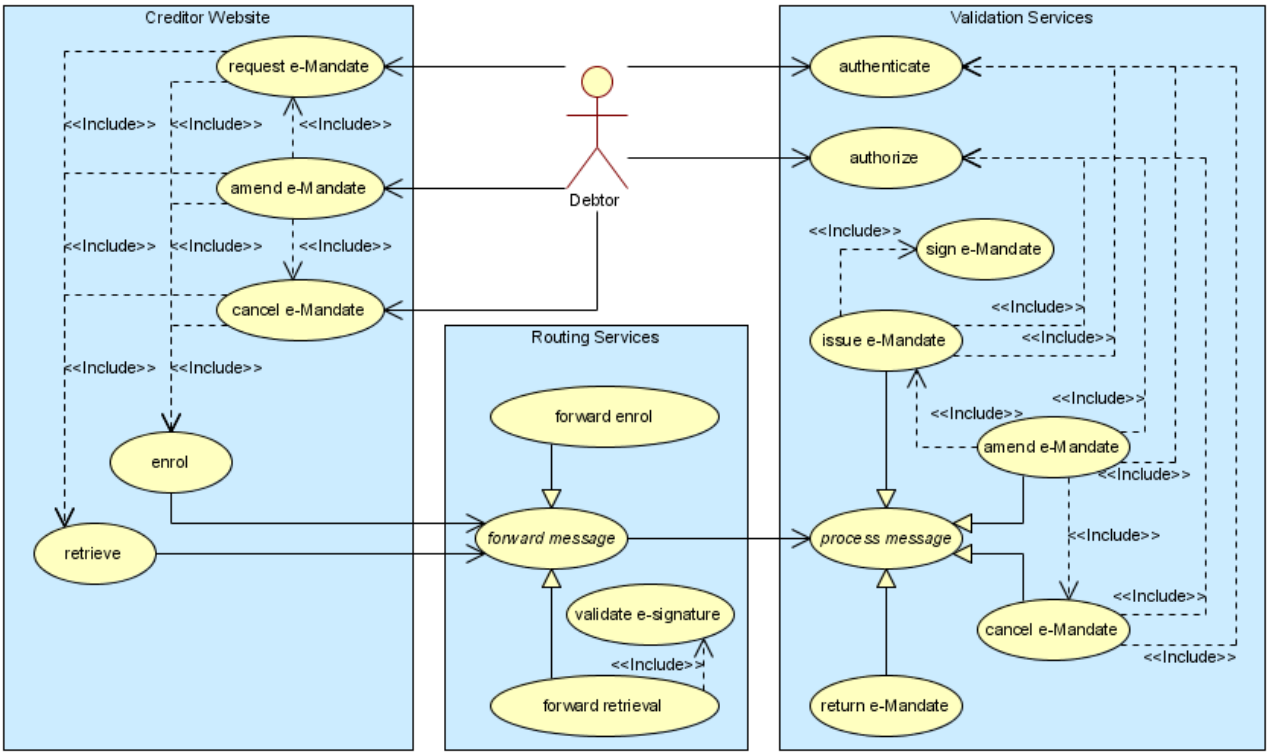

Figure 14: Entities use cases

From the Creditor perspective, the three main operations offered to the Debtor may build up on the same base operations: *enrol* at a first stage and *retrieve* at a later stage. Enrol includes building the e-Mandate enrolling message and calling the specified method on the Routing Service. Retrieve includes requesting the retrieval of the e-Mandate.

Notice that, according to [1], the amendment of an e-Mandate may be composed of a cancellation and an issuance of a new e-Mandate. Therefore, Creditors may build the amendment operation based on the cancellation and issuance operations.

From the Routing Service perspective, operations resume to forwarding requesting messages (either enrol or retrieval) and returning their respective responses. The retrieval operation includes the validation of the e-Mandate electronic signature.

From the Validation Services perspective, *authenticate* and *authorize* are operations offered to the Debtor and are used by the *issuance*, *amendment* and *cancellation* operations invoked by the Routing Service. The issuance operation includes an electronic signature over the e-Mandate. Validation Services must also provide a retrieval operation to *return* issued e-Mandates to the respective Creditors through the Routing Services.

The automated online operations available on Validation Services to Routing Services (*issue*, *amend*, *cancel* and *return*) must be extensions to the same base operation (*process message*) to allow a single entry point. Having the same entry point for all operations allows just one URL to be registered on the Directory Services.

For simplicity, the use cases for Directory Services and Certification Authorities are omitted from Figure 14. Figure 15 illustrates the use cases for Directory Services and Figure 16 the use cases for EPC Approved Certification Authorities.

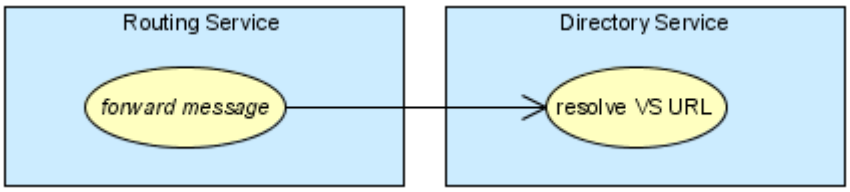

Figure 15: Directory Service use cases

When forwarding messages, Routing Services may use Directory Services to resolve BICs into the corresponding Validation Service URLs. That is the only operation performed by Directory Services in the scope of this e-Operation Model.

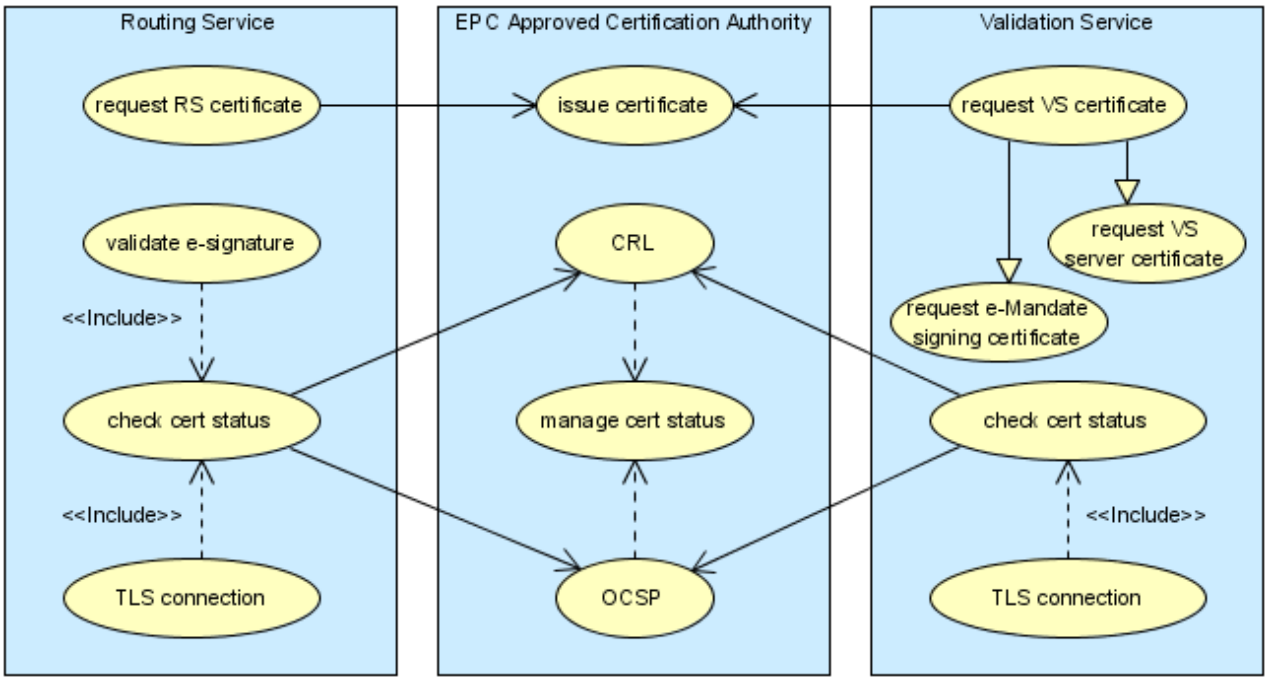

Figure 16: Certification Authorities use cases

Participant Routing Services and Validation Services must *request certificates* from EPC Approved Certification Authorities. Besides issuing certificates, Certification Authorities must also *manage certificate status* (revocations, suspensions, reactivations) and provide certificate status enquiry services, such as *Certificate Revocation Lists* (CRL) and *Online Certificate Status Protocol* (OCSP).

When establishing HTTPS connections, Routing Services and Validation Services make use of such mechanisms to verify the certificate status. If a certificate is not valid (i.e., is revoked or suspended), the connection is aborted. In addition, Routing Services perform certificate status checks when validating electronic signatures on e-Mandates.

7 TERMS USED IN THE DOCUMENT

Term	Definition
Additional Optional Services	*Complementary features and services based on the Scheme, as described in section 2.4 of the Direct Debits Rulebook.*
Adherence Agreement	*The agreement to be completed as part of the process by which an entity applies to become a Participant.*
AOS	*See 'Additional Optional Services'.*
Bank Identifier Code (BIC)	*An 8 or 11 character ISO code assigned by SWIFT and used to identify a financial institution in financial transactions (ISO 9362).*
BIC	*See 'Bank Identifier Code'.*
Certificate Revocation List	*A list of revoked certificates periodically issued by a Certification Authority.*
Certification Authority	*Defined is section 4.1.3.3.*
Creditor	*Defined in section 3.3.*
Creditor Bank	*Defined in section 3.3.*
CRL	*See 'Certificate Revocation List'.*
Debtor	*Defined in section 3.3.*
Debtor Bank	*Defined in section 3.3.*
Debtor Info	*Debtor information of the Mandate, as described in Service Description of the e-Mandates [1].*
Directory Service	*Defined in section 3.3.*
EPC	*The European Payments Council.*
EPC Approved Certification Authority	*Defined in section 3.3.*
HTTP	*Hypertext Transfer Protocol.*
HTTPS	*Hypertext Transfer Protocol over TLS.*
IBAN	*An expanded version of the basic bank account number (BBAN) intended for use internationally that uniquely identifies an individual account at a specific financial institution in a particular country (ISO 13616, EBS 204).* *As of late-2005, ISO is in the process of aligning the ISO 13616 Standard with the European Standard EBS 204. In due course the ISO Standard will replace the EBS standard.*

Term	Definition
Mandate Info	*Mandate Information, as described in Service Description of the e-Mandates [1].*
OCSP	*See 'Online Certificate Status Protocol'.*
Online Certificate Status Protocol	*A protocol designed to verify the current status of a given certificate.*
Operational BIC	*Is the BIC that the Debtor receives from the Debtor Bank.*
PKI	*Public Key Infrastructure.*
Routing Service	*Defined in section 3.3. For the sake of simplicity, the terms "Routing Service" and "Routing Service Provider" may be used interchangeably throughout this document.*
Routing Service Providers	*See 'Routing Service'.*
SDD	*See 'SEPA Direct Debit Scheme'.*
SEPA Direct Debit Scheme	*The SEPA Direct Debit Scheme is the payments scheme for making direct debits across SEPA, as set out in the SEPA Direct Debit Scheme Rulebook.*
SEPA Direct Debit Scheme Rulebook	*The Rulebook setting out rules and business standards for the SEPA Direct Debit Scheme.*
TLS	*Transport Layer Security.*
URL	*Uniform Resource Locator.*
Validation Service	*Defined in section 3.3. For the sake of simplicity, the terms "Validation Service" and "Validation Service Provider" may be used interchangeably throughout this document.*
Validation Service Providers	*See 'Validation Service'.*
XML	*Extensible Markup Language.*