EPC187-11
Version 1.1 Approved
Date issued: 21 July 2011

The EPC e-Operating Model for e-Mandates

Security Concept

(Approved by Plenary for publication on EPC Website)

Please note that this is an abridged version of document EPC159-08.

Document EPC 159-08 may be obtained under NDA from the EPC Secretariat.

Conseil Européen des Paiements AISBL– Cours Saint-Michel 30 – B 1040 Brussels
Tel: +32 2 733 35 33 Fax: +32 2 736 49 88
Enterprise N° 0873.268.927 www.epc-cep.eu secretariat@epc-cep.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]	EPC027-07	SEPA Scheme Management Internal Rules	EPC
[2]	EPC114-06	SEPA Direct Debit Scheme Implementation Guidelines	EPC
[3]	EPC306-07	e-Mandates Related to the SEPA Core Direct Debit Scheme – Service Description	EPC
[4]	EPC261-06	Risk Mitigation in the SEPA Direct Debit Scheme Version 2.3	EPC
[5]	EPC052-08	Customer-to-Bank Security Threat Assessment	EPC
[6]	SPTF-029/05	Impact of the EESSI Standards on the European Banking Community	EPC
[7]	SPTF-53/07	Customer-to-Bank Security Good Practices Guide (version 0.3.0)	EPC
[8]	EPC109-08	e-Mandates EPC e-Operating Model - High-level Definition (version 1.0, draft 0.2)	EPC
[9]	ISO 7498-2	Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture, 1989	ISO
[10]	ISO 9362	Bank Identifier Codes (BIC)	ISO
[11]	ISO 13616	Financial services - International bank account number (IBAN) -- Part 1: Structure of the IBAN	ISO
[12]	ISO 20022	Financial Services – Universal Financial Industry Message Scheme	ISO
[13]	ISO 27000	Information technology – Security techniques – Information security management systems – Fundamentals and vocabulary	ISO
[14]	ISO 27005	Information technology – Security techniques – Information security risk management	ISO
[15]	RFC 2560	Internet X.509 Public Key Infrastructure – Online Certificate Status Protocol – OCSP	IETF
[16]	RFC 2616	Hypertext Transfer Protocol – HTTP/1.1	IETF
[17]	RFC 3986	Uniform Resource Identifier (URI): Generic Syntax	IETF
[18]	RFC 5246	The Transport Layer Security (TLS) Protocol	IETF
[19]	RFC 5280	Internet X.509 Public Key Infrastructure – Certificate and Certificate Revocation List (CRL) Profile	IETF
[20]	XML	Extensible Markup Language (XML) 1.0	W3C
[21]	XMLDSIG	XML Signature Syntax and Processing	W3C
[22]	CWA 14167-1	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements, 2003	CEN
[23]	CWA 14170	Security requirements for signature creation applications, 2004	CEN

N.º	Document Number	Title	Issued by:
[24]	CWA 14365-1	Guide on the Use of Electronic Signatures – Part 1: Legal and Technical Aspects, 2004	CEN
[25]	TS 101 456	Policy requirements for certification authorities issuing qualified certificates, version 1.2.1	ETSI
[26]	TS 102 042	Policy requirements for certification authorities issuing public key certificates, version 1.3.4	ETSI
[27]	TS 101 903	XML Advanced Electronic Signatures (XAdES), version 1.3.2	ETSI
[28]	TS 102 904	Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES), version 1.1.1	ETSI
[29]	Dir.1999/93/EC	Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a community framework for electronic signatures	European Council

0.2 Defined Terms

This document refers to various defined terms which have a specific meaning in the context of this document. Chapter 6 includes a full list of defined terms used in this document.

0.3 Purpose of Document

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

1. The **High-level definition of the EPC e-Operating Model** presents a broad description of the e-Mandate EPC e-Operating Model, message flows, data model and general requirements for the solution and for the parties.
2. 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.
3. 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 EPC e-Operating Model.

This document defines the Security Concept of the EPC e-Operating Model. It takes as a basis the High-level Definition of the EPC e-Operating Model [30] and builds up a security platform defining security requirements to be adhered to by the detailed specification of the EPC e-Operating Model.

The Security Concept of the EPC e-Operating Model is detailed in the following chapters:

- **Vision and Objectives** – Introduces the Security Concept; the context in which it is being developed, the scope of applicability, its vision and objectives.
- **Risk Assessment -** Documents a risk assessment in order to have a perception of the level and types of risks that each component of the proposed model is exposed to.
- **Security Measures Evaluation** - Identifies and evaluates the security measures and how they contribute to the mitigation or elimination of the identified relevant risks.
- **Security Requirements** - Establishes the security requirements for each of the Parties and for the flow of information between them.

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 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-Mandate 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 ISO 20022 XML Standards messages and a technical standard (the EPC e-Operating Model).

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

The EPC e-Operating Model focuses on the way data is transported over the Internet between the Creditor websites and Validation Services, through a Routing Service. Furthermore, in order to ensure a secure communication between the Debtor and the Creditor, minimum security requirements are defined for Debtor browsers.

The EPC e-Operating Model includes a Security Concept, which 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, where the latter are evaluated through a risk assessment.

In order to have a complete justification of the security requirements identified in the High-level Description document, the risk assessment is built assuming that no security controls are in place on the model, however, that contractual agreements are considered to be in place.

For the components outside the scope of the EPC e-Operating Model, like the interaction between the Debtor and the Validation Service, infrastructure assets, etc, minimum industry best practices are considered to be in place.

The Security Concept described in this document is based on the ISO 27005 risk management process, which includes the following steps:

- *Context Establishment* – identification and delimitation of the scope and boundaries of the assessment;
- *Risk Assessment* – evaluation of the level and types of risks that the model is subject to;
- *Risk Treatment* – identification of the security measures for the Parties and flows;
- *Risk Acceptance* – acceptance of the security requirements based on the residual risk.

Among the proposed security measures for the EPC e-Operating Model, the main ones are:

- Provision of secure communication channels between parties via TLS protocol with mutual authentication where the deployment of client certificates is considered to be adequate;
- Electronic signature of e-Mandates;
- Definition of a set of Certification Authorities approved by the EPC to provide PKI interoperability between the Parties.

After applying the security measures identified, most threats will have their risk level reduced to marginal values.

Although the Debtor authentication through the Validation Service is out of scope, the overall risk level of the EPC e-Operating Model still strongly depends on the security measures adopted in those interactions between the Validation Service and the Debtor. The adoption of authentication methods aligned with industry best practices, as found in the EPC document "Customer-to-Bank Security Good Practices Guide" complements the overall security model.

2 VISION AND OBJECTIVES

2.1 Vision

"*The e-Mandate process is an optional feature complementing the SEPA Core SDD Scheme. 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 SEPA Core SDD Scheme."* [3], section 1.2.

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

The EPC e-Operating Model defines a platform to guarantee secure and reliable transactions between parties communicating over the Internet. In order to support these features a Security Concept has been developed and documented here in.

2.2 Objectives

The objective of this Security Concept is to define requirements and recommend best practices in order to guarantee adequate levels of security for the EPC e-Operating Model.

This document is intended for use by specialists who require an understanding of the rationale that supports the security of the EPC e-Operating Model as well as the detailed security requirements and recommended best practices to be adopted by the Participants.

2.3 Approach

A risk-based approach is the basis for the conception of a sound security framework since it does not only identify the selected controls but it also demonstrates the relationship between the risks evaluated through the risk analysis process, and the controls selected by the risk treatment process.

Adopting standard risk methodologies[1] in order to conceive requirements for an EPC e-Operating Model, however, presents itself as a challenge given the fact that the context on which such a model is to be built is vastly heterogeneous. The wide set of e-commerce and e-banking implementations (aligned with different cultural and business interests) and subject to variable legislative and regulatory requirements are other variables to consider.

In order to have a complete justification for the security requirements to be adopted, the risk assessment starts from a basis where no security related controls are in place in the model. Therefore, the model is considered as being merely conceptually operative, running over a gross security concept which is just based on the contractual agreements identified on the Service Description [3]. Furthermore, for the components outside the scope of the EPC e-Operating Model, minimum industry best practices are considered to be in place so as to make the risk assessment feasible.

[1] The ISO 27000 "Information Security Management Systems" series

One especially important aspect on which the model depends is the Debtor Authentication towards the Validation Service. It is assumed that the authentication methods are aligned with industry best practices as can be found in the EPC document "Customer-to-Bank Security Good Practices Guide" [7], derived from the threat assessment included in the document "Customer to Bank Security Threat Assessment" [5].

The Security Concept described in this document is based on the risk management process of ISO 27005 [14] (Figure 1). The risk management process has the following steps:

- *Context Establishment* – necessary to identify and delimit the scope and boundaries of the assessment;
- *Risk Assessment* – evaluation of the level and types of risks that the model is subject to;
- *Risk Treatment* – identification of the security measures for each of the Parties and flows between them;
- *Risk Acceptance* – acceptance of the security requirements based on the residual risk of the model after applying the identified security measures.

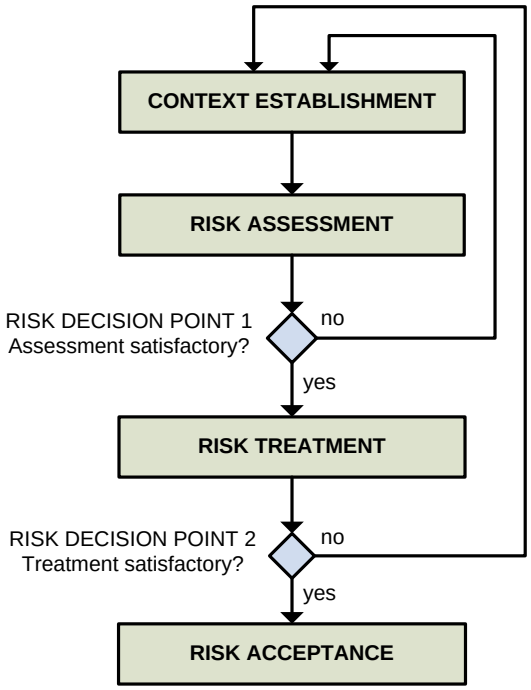

Figure 1: ISO 27005 risk management process

2.4 Principles

The e-Operating Model is based on the following principles, as stated in the e-Mandates EPC e-Operating Model - High-level Definition [8]:

- 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.
- The roles defined in the model can be provided by one or more entities, assuming that segregation measures are in place.
- Each party is allowed to create additional features on top of the model as long as the interoperability is not affected.
- The Validation Service electronically signs the e-Operating Model enveloped message[2], on behalf of the Debtor if the authentication / authorization means are correctly used.

For technical purposes, the following additional principles are considered:

- In order to participate, Creditors must enrol 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.

[2] For the sake of simplicity, the terms e-Mandate and e-Mandate request/proposal will be used throughout this document to refer to the "e-Operating Model messages enveloping the ISO 20022 XML e-Mandate messages".

3 RISK ASSESSMENT

This chapter presents the risk assessment process following the ISO 27005 approach [14]. The goal of the risk assessment is to have a perception of the level and types of risks that each component of the model is exposed to. Figure 2 illustrates the methodology adopted, in accordance to ISO 27005.

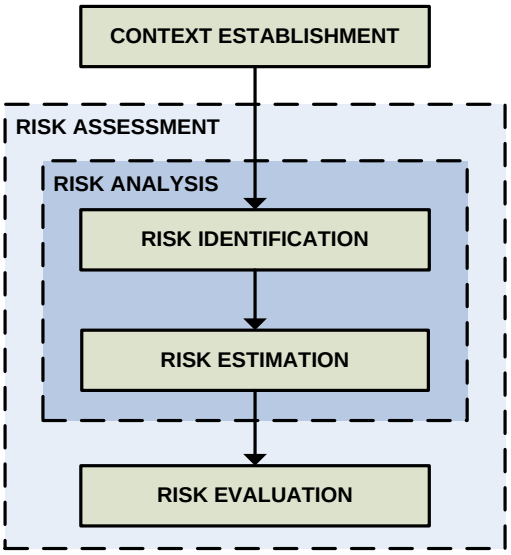

Figure 2: ISO 27005 risk assessment process

As a first step, a *context establishment* is defined in order to identify and delimit the scope and boundaries of the assessment.

After defining the context, the next step is the *risk assessment*, which is composed of:

- A *risk analysis* based on:
  - *Risk identification* - an enumeration and definition of the assets, threats and vulnerabilities.
  - *Risk estimation* - the subjacent risks are characterized and a corresponding estimation of the risk level is performed.
- A *risk evaluation*, with a prioritization of the risks estimated on the risk analysis.

The risk estimation adopts a qualitative methodology, using a range of three levels - low, medium and high – and is expressed in terms of:

- Likelihood – The probability of occurrence of an identified risk. Several factors affect the likelihood, such as:
  - Effort needed to deploy an exploiting attack;
  - Benefits obtained from a successful attack;
  - Motivations (ego, espionage, revenge, fanaticism, terrorism, etc.);
  - Risk of being detected;
  - Exploitable vulnerabilities;

- Number of potential attackers.

- Impact – The amount of value that an asset (or set of assets) may lose if an attack is successful. Impacts can be of diverse natures, namely:
  - Financial;
  - Reputational;
  - Operational;
  - Legal and regulatory.

3.1 Scope and Boundaries

The risk assessment presented in this document is focused exclusively on the EPC e-Operating Model functionality and, therefore, the context establishment is restricted to this environment. All players and flows between players are considered in this analysis with the exception of:

- The interaction between the Debtor and the Creditor, except where strictly indispensable;
- The interaction between the Debtor and the Validation Service.

As a starting point for this technical analysis, it is considered that contracts and accreditations have been established between relating parties as defined in the Service Description [3].

The risks of a particular implementation, architecture or infrastructure (system, in general) are outside the scope of this assessment. For those systems, the respective providers are expected to apply the best known practices and elaborate a specific risk assessment.

3.2 Assets

In the context of this analysis, assets are anything that has value for the correct and expected operation of the model and the services supported by the model, and which therefore require protection [13] [14].

The assets[3] considered in this risk assessment are identified in Table 1.

Table 1: Assets description list

Asset	Description
Personal data	Personal data that characterizes the Debtor in his individuality must not be disclosed to external parties other than that explicitly permitted.
Business data	Data related or supporting the business of a party whose disclosure could constitute an advantage to its competitors or violate privacy requirements.
Reputation	Intangible and subjective global evaluation about a party as being a trustful, reliable and credible organization.
Service	Continuous availability and reliability of a service.
e-Mandate	Authorization to be granted by the Debtor to the Creditor to enable future Collections over the Direct Debit Scheme.
Funds	Debtor's monetary values deposited on an account at the Debtor Bank.

This rest of this section is intentionally left blank. The complete version is contained in EPC 159-08.

[3] For a detailed list of the assets included in the risk assessment please check Annex A: Assets

4 SECURITY MEASURES EVALUATION

This chapter identifies and evaluates a set of commonly used security measures and how they contribute to the mitigation or elimination of the identified relevant risks. The evaluation will identify the security features that each measure can contribute. The different options available in these protocols will be identified and evaluated so that its application on the entities and flows can be best suited.

4.1 Transport Level Security

The first step towards a secure model is to protect the exchanged data on a host-to-host connection by creating a secure networking channel. This can be achieved by using the TLS protocol [18], which has standard built-in mechanisms to provide:

- *Authentication* of parties, based on X.509 certificates. The server is always authenticated whereas the client may optionally be authenticated (mutual authentication);
- *Confidentiality* of data, by performing a symmetric key agreement at session initiation and using that key to cipher the exchanged data. The risk of eavesdropping is mitigated;
- *Data Integrity*, based on cryptographic hash functions. The risk of tampering is mitigated.

The EPC e-Operating Model enforces the use of TLS on all connections between Debtors and Creditors, Creditors and Routing Services, Routing Services and Directory Services and Routing Services and Validation Services. The connections between Debtors and Validation Services/Online Banking of Debtor Banks are outside the scope of the EPC e-Operating Model.

The mutual authentication feature of TLS is required between the Routing Services and Validation Services, in order to allow only legitimate Routing Services to access legitimate Validation Services. Due to the absence of a direct contractual relationship between those parties, it is expectable that Routing Services and Validation Services may not know each other prior to the first connection establishment. Therefore, a secure and interoperable mechanism is necessary to allow Routing Services to be able to recognize Validation Services as being SEPA enrolled and legitimate and, reversely, Validation Services to be able to recognize Routing Services as being SEPA enrolled and legitimate.

This objective is accomplished by using specific certificate extensions that qualify the entitled entities as being legitimate participants (Routing Services or Validation Services). The issuing Certification Authority is responsible to comply with the full set of procedures defined in the EPC e-Operating Model which are required for the enrolment of Routing Service and Validation Service providers.

When establishing a TLS session, the authentication is performed during the “handshake”. When the parties present to each other their certificates, a verification of the presented certificates must be performed. The certificate verification must follow the general rules described on the RFC 3280 [19], and, if applicable to the certificates presented, it should take an additional step to verify the existence of the SEPA specific extension. The most significant steps of the process are illustrated on Figure 3.

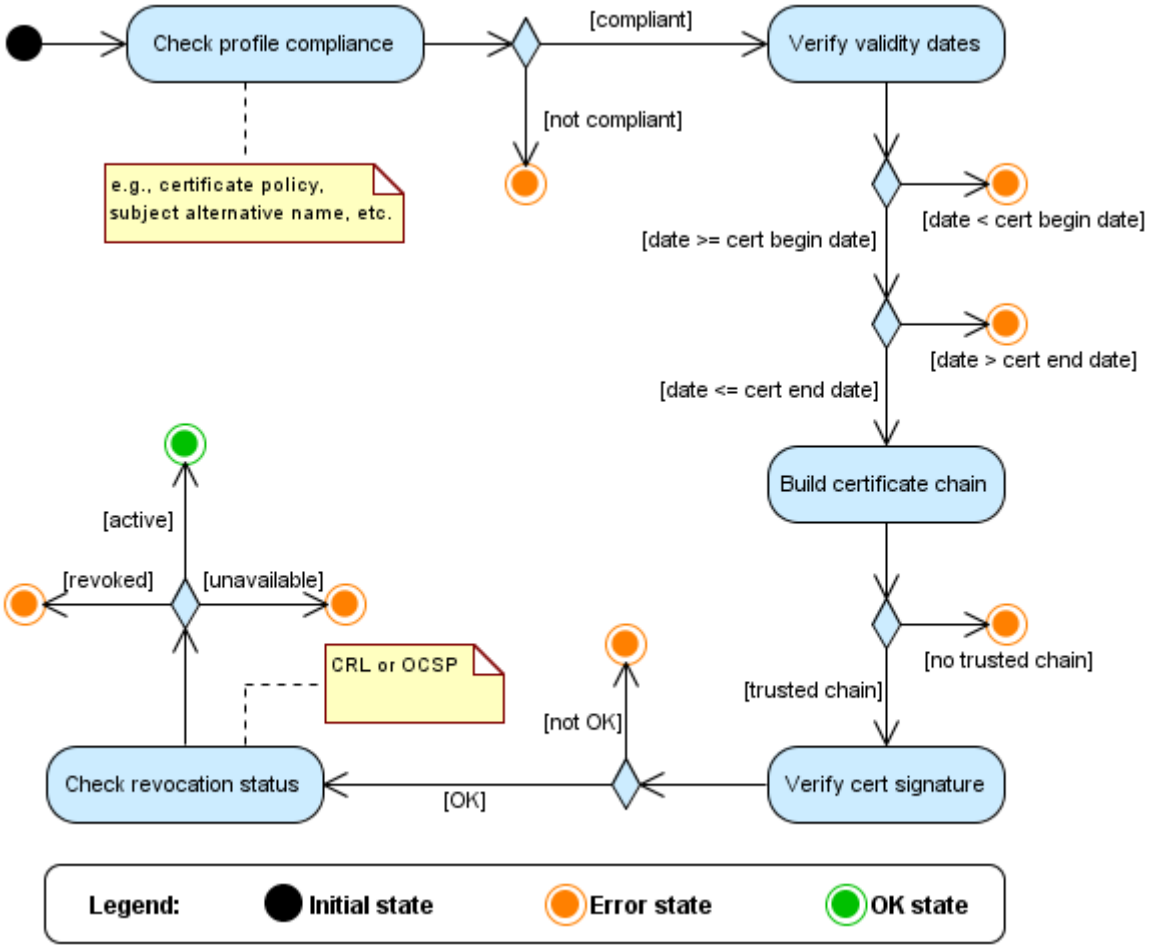

Figure 3: Significant steps of the certificate verification

The minimum version of TLS to be supported is 1.0, but all parties are recommended to migrate to TLS v1.2 as soon as possible (for interoperability purposes, all versions of TLS have mechanisms to provide both forward and backward compatibility).

4.2 Application level security

The security measures discussed in Section 4.1 are focused on the transport level, providing network security on a host-to-host basis. Additional complementary measures must be addressed to further increase the overall security of the EPC e-Operating Model. Those measures are targeted to the application level and include:

- Electronic signatures, described in Section 4.2.1;
- Time accuracy and synchronization, described in Section 4.2.2;
- Audit trails, described in Section 4.2.3;
- Error reporting, described in Section 4.2.4;
- Timeouts, described in Section 4.2.5;
- Caching of BIC resolutions, described in Section 4.2.6.

4.2.1 Electronic signatures

The most important security measure at the application level is the binding of electronic signatures[4] to e-Mandates by Validation Services. Electronic signatures are based on common cryptographic techniques and are efficient and highly secure mechanisms that provide the following security properties [13] at the application level:

- *Authenticity* – a party receiving an electronically signed e-Mandate is able to positively confirm the identity claimed by the source of the e-Mandate.
- *Integrity* – verification of the completeness and accuracy of an e-Mandate.
- *Non-Repudiation* – ability to prove that the issuance of an e-Mandate has taken place, so that it can not be repudiated later in support of a dispute resolution.

Since the e-Mandate is a XML electronic document, the format of the electronic signature will be in accordance with XML Advanced Electronic Signatures (XAdES) [27], in the form of Basic Electronic Signatures (XAdES-BES).

The profiles defined for XAdES-BES [28] are compliant with the requirements of the European Directive 1999/93/EC [29] for Advanced Electronic Signatures[5], while being also fully compatible and interoperable with legacy implementations of the plain W3C specification XML Signature [21] (from which XAdES derives).

The electronic signature will be applied as an enveloping signature, meaning that the original XML content of the e-Mandate remains unchanged and is encapsulated into a secure XML case (see Figure 4).

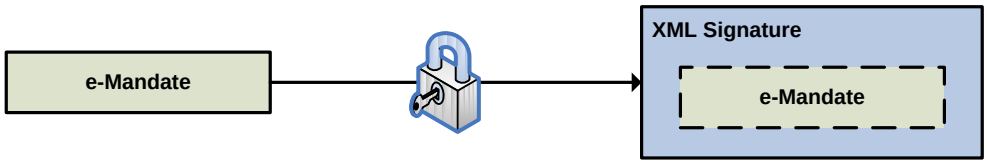

Figure 4: Enveloping XML signature

The electronic signature verification (see Figure 5) is composed of a verification of the signing certificate followed by a cryptographic verification of the electronic signature (see Figure 3).

[4] *Electronic Signature* is a concept introduced by the European Directive 1999/93/EC [29]. It is also commonly referred as *Digital Signature*, as defined in ISO 7498-2:1989.

[5] See also document "*Impact of the EESSI Standards on the European Banking Community*" (SPTF-029/05) [6].

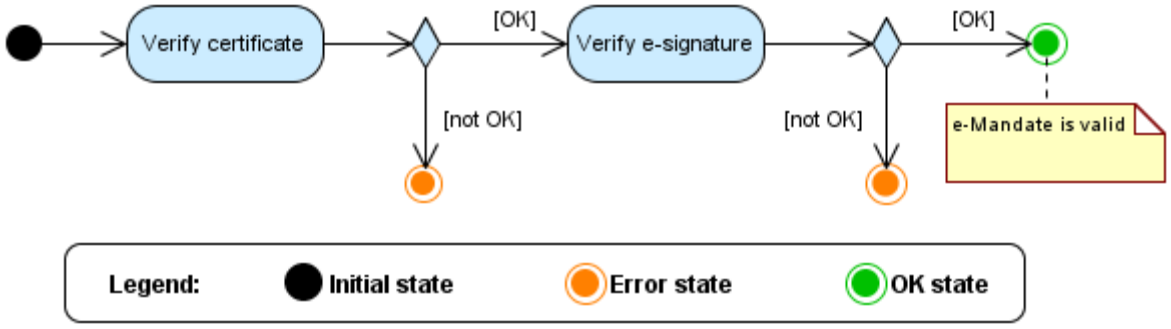

Figure 5: Electronic signature verification

The electronic signature verification of e-Mandates must be performed by Creditors and Routing Services. However, due to the complexity of the verification process and given the contractual nature of the relationship between Creditors and Routing Services, Creditors may delegate the responsibility of the verification to the relying Routing Service provider.

4.2.2 Time accuracy and synchronization

Each party of the model should have its system clocks synchronized with a trusted time source of its choice. This guarantees a reasonable timeliness of data and operations between several different parties and the accuracy of exchanged times and dates (e.g., field 25 of DS-13 [3]).

4.2.3 Audit trails

In addition to the electronic signatures, Routing Service and Validation Service providers must produce audit trails on their systems for all relevant operations, including the issuance, amendment and cancellation of e-Mandates, configuration changes, access attempts, exceptions and key management functions critical to the security of the reliance being placed on PKI processes and operations.

The audit trails can be application based logs or other equivalent means of evidence, as long they contain sufficient information to trace back the complete details of an operation and can be searched or queried in an automated way.

The audit trails must also be stored in a long-term support and a tamper evident format, such that illicit addition, modification or deletion of any audit trail can be detected.

The dates and times registered in the audit trails must be obtained from a trusted time source to ensure accuracy and a reasonable clock synchronization of the different parties (see section 4.2.2).

The Annex C of CWA 14170 [23] presents guidelines for the implementation of a Signature Logging Component.

4.2.4 Error reporting

Another relevant security measure is error reporting. To avoid unpredictable and/or *ad-hoc* operation results on abnormal situations, error messages are defined to report incidents. Having well-known error messages has the following advantages:

- Handling of errors can be improved since all possible cases are known in advance.
- The strict formatting of error messages avoids accidental disclosure of sensitive details (e.g., infrastructure details).

4.2.5 Timeouts

The services running over the EPC e-Operating Model are usually composed of several steps. In each of them, the requests may be in a holding state, waiting for some event, be it input or the occurrence of a given action. During this time, resources are consumed to maintain the context of the state. If the event does not occur, the systems may end up with too many exhausted resources resulting from aborted requests.

Therefore, adequate timeout mechanisms must be implemented to invalidate endless requests and free up the committed resources.

4.2.6 Caching of BIC resolutions

In order to contact the corresponding Validation Services, the Routing Service providers must be able to resolve BICs into Validation Service URLs. This is achieved by using a Directory Service that maps the Debtor's Bank Operational BICs into the designated Validation Service URLs.

If the Directory Service is queried for each incoming transaction and the Routing Service provider is fully dependent on the response to proceed with the transaction, the Directory Service would be a single point of failure. This means that an interruption (either accidental or deliberate) of the Directory Service can make the whole system unavailable, since Routing Services will not be able to route the requests.

One important mechanism to mitigate this risk is to cache the BIC resolutions. Routing Services are recommended to maintain an internal mapping of the BICs and respective Validation Service URLs.

The EPC e-Operating Model suggests three approaches to build the cache:

1. Request the Directory Service for the full mapping table and store it locally;
2. Request the changes occurring between a previous version and the current table;
3. Collect and cache the queries as they are being processed.

A maximum time for cache update must be adopted so as to assure that mapping changes and new additions or deletions are reflected.

4.3 Public Key Infrastructure

Some of the identified mechanisms in the above sections make use of certificates, either for TLS or for XML Signatures. Therefore, a Public Key Infrastructure (PKI) is needed not only to issue the certificates, but to manage their lifecycle (suspensions, revocations and reactivations) and provide additional services (e.g., CRL, OCSP, etc.) as well.

Since the EPC e-Operating Model is to be run by heterogeneous entities, both in nature and interests, it is desirable to allow some flexibility in the choice of the Certification Authority (CA) from which to request the certificates. Nonetheless, it is fundamental to create mutual trust and recognition between players operating cross border in the SEPA environment. This trustable set of CAs should be defined by the EPC by accepting candidate CAs that declare strict compliance with the rules of enrolment and certification practices defined in the EPC e-Operating Model and are sponsored by a Routing Service or Validation Service provider.

Applicant CAs may be already established in the market, private internal CAs already in use by the parties or special purpose CAs specifically targeted to the EPC e-Operating Model. In either of the cases, the conditions for application to the EPC are a sponsorship of a Routing Service or Validation Service provider and full compliance with the defined rules for CAs.

The adoption of the required certification practices minimizes the risk of compromise of a CA, while the enrolment rules guarantees the univocal identity and legitimacy of the end entity.

Once a CA is approved by the EPC, it becomes part of the *EPC Approved CAs* set and must be trusted by all participating parties that need SEPA certificates (i.e., Routing Service and Validation Service providers). This common set of trust anchors is the basis for the interoperability between Routing Services and Validation Services, which may not know each other prior to a transaction.

The full set of certificates necessary for the EPC e-Operating Model is illustrated in Figure 6.

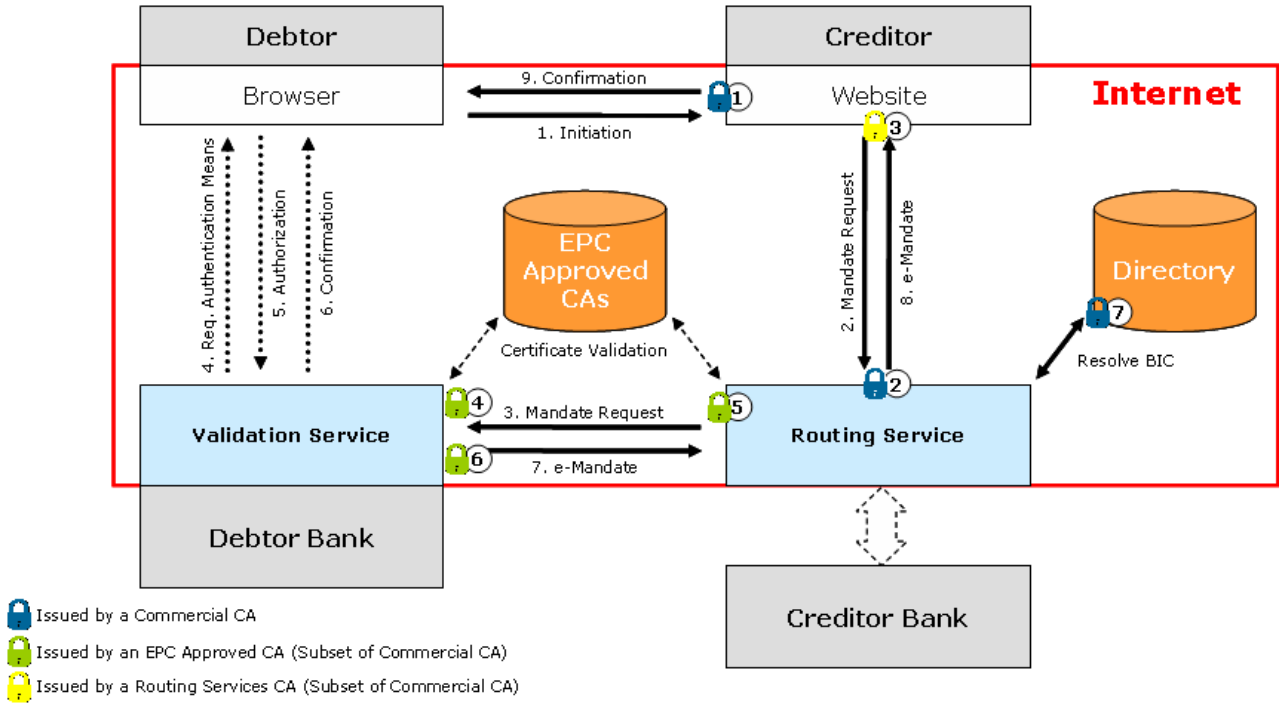

Figure 6: PKI and certificates for the EPC e-Operating Model

Table 2 presents a description of the certificates depicted in Figure 6.

Table 2: Description of the EPC 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 / Commercial	Creditor	Routing Service	(Optional) Authenticates the Creditor to the Routing Service.

Ref	Certificate Type	CA	Authenticated Object	Verifying Party	Description
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 EPC e-Operating Model. Protects the communication between these two parties.
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 EPC e-Operating Model.
6	Signing	EPC approved	Validation Service e-mandate	Creditor, Routing Service	Signs messages in the EPC 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 profile specified on the EPC e-Operating Model for certificate 5 (Routing Service TLS Client) allows Routing Services to use it simultaneously as certificate 2 as it will also be ready for server-side usage.

5 SECURITY REQUIREMENTS

This chapter establishes security requirements based on the analysis performed in the previous sections by enumerating for each participating entity the measures to be implemented. Requirements will be enumerated for the setup process as well as for the common actions of issuance, amendment and cancellation of the e-Mandates.

5.1 Debtor security requirements

In order to establish secure connections between the Debtor and the Creditor Website, the Debtor's Browser must support TLSv1 / SSLv3 (or higher) with strong security cipher suites and have the security options enabled.

Given the importance of security aware users, entities with direct relationships with Debtors (namely Banks, Validation Services and Creditors) should promote security awareness, training and education wherever possible. Debtors should be encouraged to adopt security measures advised by the parties such as firewalls, antivirus, antispyware, etc.

5.2 Creditor security requirements

In order to mitigate or lower the risk levels identified on the risk assessment (Chapter 3), Creditor websites must comply with the following security requirements:

M.1 To establish secure connections between the Debtor browser and the Creditor website, the server must use HTTP over TLS. The Creditor Website must provide access to the e-Mandates functionalities to Debtors only through secure authentication means.

M.2 To establish secure connections between the Creditor website and the Routing Service provider, HTTP over TLS must be used.

M.3 A TLS client certificate (or any other equivalent strong authentication mechanism) must be assigned by the Routing Service provider to the Creditor Website. On each HTTPS connection, the certificate must be presented for authentication.

M.4 TLS must be performed using only strong cipher suites; weak cipher suites must be disabled on the web server. This measure is complementary to the previous ones and further reduces the likelihood of an attack.

M.5 A trusted time source is recommended to be used to ensure reasonable time accuracy on exchanged timestamps and audit trails. This measure is complementary to the previous ones and further reduces the likelihood of an attack.

M.6 All stored personal information about Debtors and the e-Mandates they hold must be protected in strict accordance with the legal and regulatory requirements and used solely for the purposes explicitly allowed by the respective Debtors.

5.3 Routing Service provider security requirements

In order to mitigate or lower the risk levels identified on the risk assessment (Chapter 3), Routing Service providers must comply with the following security requirements:

M.7 To establish secure connections between the Creditor Website and the Routing Service provider, HTTP over TLS must be used.

M.8 A TLS client certificate (or any other equivalent strong authentication mechanism) must be assigned by the Routing Service provider to the Creditor 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.

M.9 Routing Service providers must establish contractual agreements and the terms of usage with Creditors through Creditor Banks. This measure is complementary to M.8 and further reduces the likelihood of an attack.

M.10 Trust on all EPC approved Certification Authorities must be guaranteed in order to have an interoperable Public Key Infrastructure. This is an enabling measure for requirement M.11.

M.11 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.

M.12 TLS must be performed using only strong cipher suites; weak cipher suites must be disabled on the web server. This measure is complementary to M.8 and M.11 and further reduces the likelihood of an attack.

M.13 All certificates must be validated in accordance with the process illustrated on Figure 3.

M.14 All cryptographic electronic signatures must be validated in accordance with the process illustrated in Figure 5.

M.15 Routing Services are recommended to cache BIC resolutions obtained from the Directory Service.

M.16 Audit trails must be generated for all relevant operations. They must include sufficient information to fully trace back a given operation and stored in a secure way such that addition, tampering or deletion of trails is detectable.

M.17 Timeouts to invalidate requests and discard state data must be set according to the defined rules.

M.18 A trusted time source must be used to ensure reasonable time accuracy on exchanged timestamps and audit trails. This measure is complementary to the previous ones and further reduces the likelihood of an attack.

5.4 Validation Service provider requirements

In order to mitigate or lower the risk levels identified on the risk assessment (Chapter 3), Validation Service providers must comply with the following security requirements:

M.19 Debtors must be able to easily confirm the authenticity of the Validation Service for which they are redirected. The document SPTF-053/07 "*Customer-to-Bank Security Good Practices Guides*" [7] presents guidelines on this issue.

M.20 All e-Mandates must be electronically signed by a signature creation application compliant with CWA 14170 [23] [6] using a certificate issued by an approved EPC Certification Authority.

M.21 Since Validation Services perform electronic signatures of e-Mandates on behalf of Debtors (requirement M.20), every data field of e-Mandate requests must be shown to the Debtor when requesting authorization.

M.22 Trust on all EPC approved Certification Authorities must be guaranteed in order to have an interoperable Public Key Infrastructure. This is an enabling measure for requirement M.23.

M.23 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.

M.24 TLS must be performed using only strong cipher suites; weak cipher suites must be disabled on the web server. This measure is complementary to M.23 and further reduces the likelihood of an attack.

M.25 All certificates must be validated in accordance with the process illustrated in Figure 3.

M.26 Audit trails must be generated for all relevant operations. They must include sufficient information to fully trace back a given operation and stored in a secure way such that addition, tampering or deletion of trails is detectable.

M.27 Timeouts to invalidate requests and discard state data must be set according to the defined rules.

M.28 A trusted time source must be used to ensure reasonable time accuracy on exchanged timestamps and audit trails. This measure is complementary to the previous ones and further reduces the likelihood of an attack.

5.5 Directory Service provider security requirements

In order to mitigate or lower the risk levels identified on the risk assessment (Chapter 3), Directory Service providers must comply with the following security requirements:

M.29 To establish secure connections between the Directory Service and the Routing Service providers, HTTP over TLS must be used.

M.30 TLS must be performed using only strong cipher suites; weak cipher suites must be disabled on the web server. This measure is complementary to the previous ones and further reduces the likelihood of an attack.

M.31 A trusted time source must be used to ensure reasonable time accuracy on exchanged timestamps and audit trails. This measure is complementary to the previous ones and further reduces the likelihood of an attack.

[6] Typically, signature creation applications in compliant with CWA 14710 require secure signature creation devices, such as Hardware Security Modules with certification FIPS 140-1/2 Level 2 or higher, or Common Criteria EAL 3 or higher.

5.6 Certification Authority security requirements

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

M.32 Have a sponsorship of a Routing Service provider or a Validation Service provider.

M.33 Be able to issue certificates in accordance with the customized certificate profiles defined in the EPC e-Operating Model.

M.34 Strictly follow the defined enrolment steps for applying Routing Service and Validation Service providers.

M.35 Offer an accessible Certificate Revocation List (CRL) for certificate status validation and an Online Certificate Status Protocol (OCSP) service.

M.36 Strictly follow CWA 14167-1 (for Non-Qualified Certificates) [24] and TS 102 042 (for Normalized Certificate Policy) [26].

The measures presented above minimize the risks of a CA compromise and the issuance of a certificate to a fraudulent party. In this sense, these measures are enablers of the preceding measures targeted to the other parties.

6 TERMS USED IN THE DOCUMENT

Term	Definition
Adherence Agreement	*The agreement to be completed as part of the process by which an entity applies to become a Participant.*
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	*Public key of a user, together with some other information, rendered un-forgeable by encipherment with the private key of the certification authority which issued it [26].*
Certificate Revocation List	*A signed list of revoked certificates periodically issued by a Certification Authority.*
Certification Authority	*Entity trusted by one or more users to create and assign certificates.*
Creditor	*Defined in [3].*
Creditor Bank	*Defined in [3].*
CRL	*See 'Certificate Revocation List'.*
Debtor	*Defined in [3].*
Debtor Bank	*Defined in section [3].*
Denial of Service	*An attack in which an attacker is able to degrade a service by consuming computing resources to such an extent that the service is considered unusable.*
Directory Service	*Defined in section [3].*
Disclosure	*Disclosure occurs when sensitive data is retrieved by persons which are not supposed to have access to it.*
EPC	*The European Payments Council (http://www.europeanpaymentscouncil.eu).*
EPC Approved Certification Authority	*A Certification Authority compliant with the requirements defined by the EPC.*
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
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.*
Repudiation	*Repudiation occurs when someone claims to have not performed a disputed operation that he actually performed. Reversely, repudiation is also about being able to refute the validity of forged operations.*
Routing Service	*Defined [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.*
Spoofing	*An attack in which one malicious person or program successfully appears to another.*
Tampering	*An attack in which data is modified or corrupted while in transit between two parties.*
TLS	*Transport Layer Security.*
URL	*Uniform Resource Locator.*
Validation Service	*Defined in [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'.*
W3C	*World Wide Web Consortium (http://www.w3c.org)*
XML	*Extensible Markup Language.*

ANNEX A ASSETS

In Section 3, the main assets considered in the risk assessment for the EPC e-Operating Model were presented. In this annex, the referenced assets are further detailed into their constituent items in Table 3.

For each identified asset, one or more stakeholders are assigned. An asset stakeholder may not have property rights to the asset but is responsible for its production, development, maintenance, use and security as appropriate.

Table 3: Detailed assets list

ID	Assets	Items	Description	Stakeholder[7]
A.1	Personal Data	Debtor data	Personal data that characterizes the Debtor in his individuality must not be disclosed to external parties other than the ones explicitly permitted.	Debtor, Creditor, RS, VS
A.2	Business Data	Creditor business data	Data related or supporting the Creditor's business (e.g., Creditor clients database)	Creditor, RS
A.3	Business Data	Routing Service business data	Data related or supporting the Routing Service provider business (e.g., Database of contracts with Creditors)	RS, VS
A.4	Business Data	Validation Service business data	Data related or supporting the Validation Service provider / Debtor Bank (e.g., Debtors database)	VS, RS
A.5	Reputation	SEPA DD reputation	Intangible and subjective global evaluation of the targeted groups exclusively about the SEPA Direct Debits as being a trustful and reliable service.	EPC
A.6	Reputation	SEPA e-Mandates reputation	Intangible and subjective global evaluation of the targeted groups exclusively about the SEPA e-Mandates as being a trustful and reliable service.	EPC
A.7	Reputation	Debtor Bank reputation	Intangible and subjective global evaluation of the targeted groups about the Debtor Bank as being a trustful, reliable and credible organization.	Debtor Bank, VS
A.8	Reputation	Creditor Bank reputation	Intangible and subjective global evaluation of the targeted groups about the Creditor Bank as being a trustful, reliable and credible organization.	Creditor Bank, RS
A.9	Reputation	Routing Service reputation	Intangible and subjective global evaluation of the targeted groups about the Routing Service provider as being a trustful, reliable and credible organization.	RS
A.10	Reputation	Validation Service reputation	Intangible and subjective global evaluation of the targeted groups about the Validation Service provider as being a trustful, reliable and credible organization.	VS
A.11	Reputation	Creditor reputation	Intangible and subjective global evaluation of the targeted groups about the Creditor as being a trustful, reliable and credible organization.	Creditor
A.12	Service	SEPA Direct Debits service	Continuous service availability and reliability of the whole current deployed infrastructure supporting SEPA.	EPC

[7] DS – Directory Service provider; EPC – European Payments Council; RS – Routing Service provider; VS – Validation Service provider

ID	Assets	Items	Description	Stakeholder[7]
A.13	Service	SEPA e-Mandates service	Continuous service availability and reliability of the whole infrastructure to be deployed in order to support SEPA e-Mandates.	EPC
A.14	Service	Creditor's website service	Continuous service availability and reliability of a Creditor's website.	Creditor
A.15	Service	Routing Service	Continuous service availability and reliability of a Routing Service provider.	RS
A.16	Service	Validation Service	Continuous service availability and reliability of a Validation Service provider.	VS
A.17	Service	Directory Service	Continuous service availability and reliability of a Directory Service provider.	DS
A.18	e-Mandate	e-Mandate	Authorization to be granted by the Debtor to the Creditor to enable future Collections over the Direct Debit Scheme.	Debtor Bank, Creditor
A.19	Funds	Funds	Debtor's monetary values deposited on an account at the Debtor Bank.	Debtor Bank