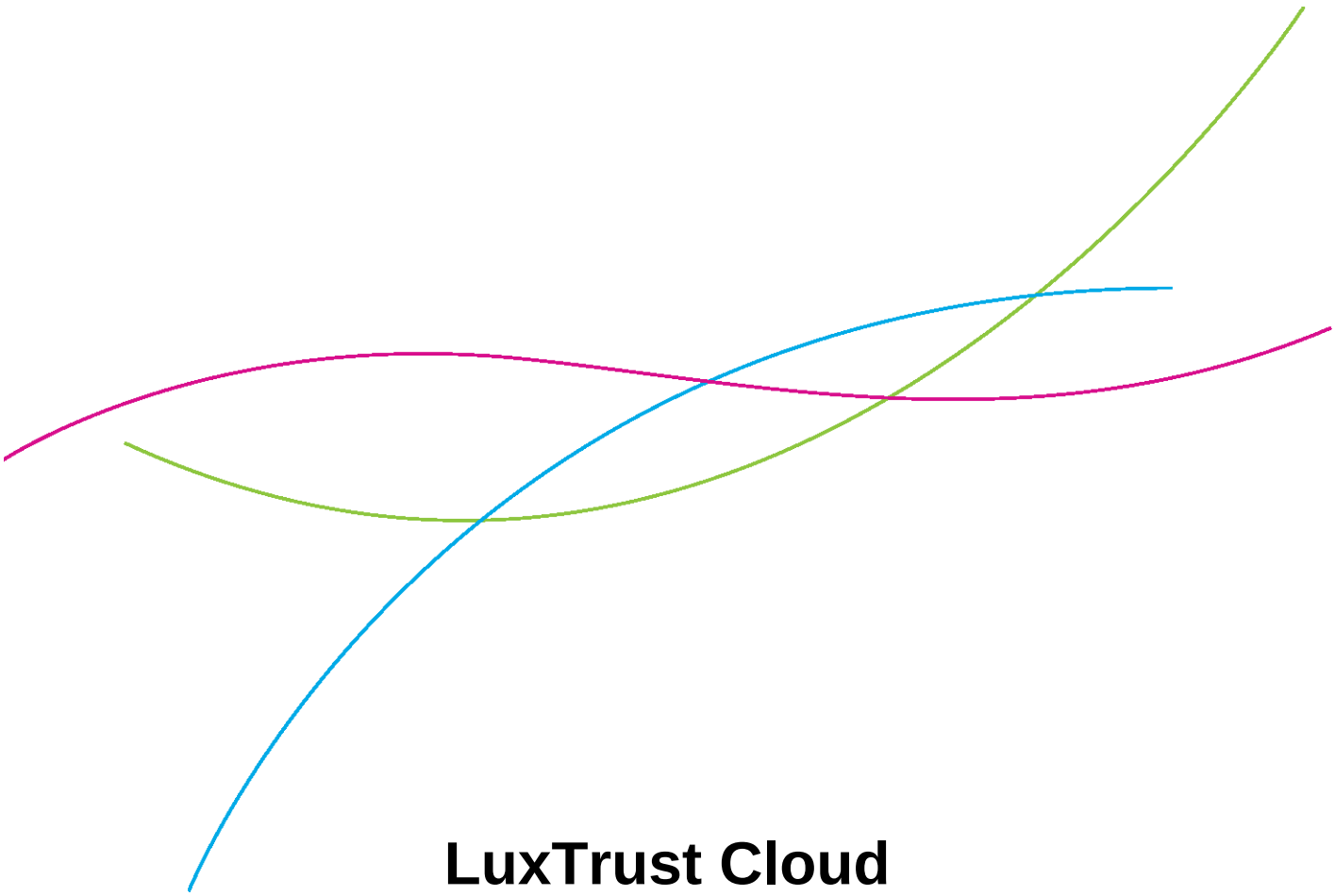

LuxTrust Cloud Validation Policies

Document reference:
LT-2020-01-06-01-R-E

Date issued:
2021-01-20

Version: 1. 2

LuxTrust S.A
IVY Building | 13-15, Parc d'activités | L-8308 Capellen
Luxembourg | VAT LU 20976985 | RCS B112233
Business Number N°00135240/0
Phone: +352 26 68 15 – 1
Fax: +352 26 68 15 – 789

Revision History

Version	Date	Description of Change
1.0.0	03/2020	Initial Draft
1.0.1	03/2020	Minor editorial corrections
1.2	01/2021	Clarifications triggered by the service audit

Intellectual Property Rights

Disclaimer

In case of discrepancy in interpretation concerning a given linguistic version with respect to the English reference version, the English version shall prevail.

References

[1] Regulation 910/2014/EU – Electronic identification and trust services for the electronic market, August 2014
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910&from=EN

[2] Decision 1505/2015/EU – Technical specifications and formats relating to trusted lists pursuant to Article 22(5) of Regulation (EU) No 910/2014, September 2015
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1505&from=EN

[3] Decision 1506/2015/EU – Technical specifications relating to formats of advanced electronic signatures and advanced seals to be recognised by public sector bodies pursuant to Articles 27(5) and 37(5) of Regulation (EU) No 910/2014, September 2015
https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015D1506&from=EN

[4] IETF RFC 4998 Evidence Record Syntax (ERS), August 2007
https://tools.ietf.org/html/rfc4998

[5] IETF RFC 6283 Extensible Markup Language Evidence Record Syntax (XMLERS), July 2011
https://tools.ietf.org/html/rfc6283

[6] IETF RFC 6838 Media Type Specifications and Registration Procedures, January 2013
https://tools.ietf.org/html/rfc6838

[7] IETF RFC 7230 Hypertext Transfer Protocol (HTTP/1.1) : Message Syntax and Routing, 6/2014
https://tools.ietf.org/html/rfc7230

[8] IETF RFC 7231 Hypertext Transfer Protocol (HTTP/1.1) : Semantics and Content, 6/2014
https://tools.ietf.org/html/rfc7231

[9] IETF RFC 7232 Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests, 6/2014
https://tools.ietf.org/html/rfc7232

[10] IETF RFC 7233 Hypertext Transfer Protocol (HTTP/1.1): Range Requests, 6/2014
https://tools.ietf.org/html/rfc7233

[11] IETF RFC 7234 Hypertext Transfer Protocol (HTTP/1.1): Caching, 6/2014
https://tools.ietf.org/html/rfc7234

[12] IETF RFC 7235 Hypertext Transfer Protocol (HTTP/1.1): Authentication, 6/2014
https://tools.ietf.org/html/rfc7235

[13] IETF RFC 8446 The Transport Layer Security (TLS) Protocol Version 1.3, 8/2018
https://tools.ietf.org/html/rfc8446

[14] ISO 32000-1: Document management - Portable document format - Part 1: PDF 1.7, 2008
https://www.iso.org/standard/51502.html

[15] ISO 32000-2: Document management - Portable document format - Part 2: PDF 2.0, 2017
https://www.iso.org/standard/63534.html

[16] ISO 19005-1: Document Management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1), 2005
https://www.iso.org/standard/38920.html

[17] ISO 19005-2: Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1 (PDF/A-2), 2011
https://www.iso.org/standard/50655.html

[18] W3C: Extensible Markup Language (XML) 1.0 (Fifth Edition), 11/2008
https://www.w3.org/TR/2008/REC-xml-20081126/

[19] W3C: XML Schema Definition Language (XSD) 1.1 Part 1: Structures, 4/2012
https://www.w3.org/TR/2012/REC-xmlschema11-1-20120405/

[20] W3C: XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes, 4/2012
https://www.w3.org/TR/2012/REC-xmlschema11-2-20120405/

[21] W3C XML Signature Syntax and Processing Version 1.1, Recommendation, April 2013
https://www.w3.org/TR/xmldsig-core/

[22] ETSI EN 319 102-1 – Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, May 2016
http://www.etsi.org/deliver/etsi_en/319100_319199/31910201/01.01.01_60/en_31910201v010101p.pdf

[23] ETSI EN 319 142-1 – Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures, April 2016
http://www.etsi.org/deliver/etsi_en/319100_319199/31914201/01.01.01_60/en_31914201v010101p.pdf

[24] ETSI EN 319 142-2 – Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles, April 2016
http://www.etsi.org/deliver/etsi_en/319100_319199/31914202/01.01.01_60/en_31914202v010101p.pdf

[25] ETSI EN 319 132-1 – Electronic Signatures and Infrastructures (ESI); XAdES digital signatures, Parts 1: Building blocks and XAdES baseline signatures, April 2016
http://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.01.01_60/en_31913201v010101p.pdf

[26] ETSI EN 319 132-2 – Electronic Signatures and Infrastructures (ESI); XAdES digital signatures, Parts 2: Extended XAdES signatures, April 2016
http://www.etsi.org/deliver/etsi_en/319100_319199/31913202/01.01.01_60/en_31913202v010101p.pdf

[27] ETSI TS 119 101 – Electronic Signatures and Infrastructures (ESI); Policy requirements for applications for signature creation and signature validation, March 2016
http://www.etsi.org/deliver/etsi_ts/119100_119199/119101/01.01.01_60/ts_119101v010101p.pdf

[28] ETSI TS 119 102-1 – Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation, August 2018
https://www.etsi.org/deliver/etsi_ts/119100_119199/11910201/01.02.01_60/ts_11910201v010201p.pdf

[29] ETSI TS 119 172-1 – Electronic Signatures and Infrastructures (ESI); Signature Policies; Part 1: Building blocks and table of contents for human readable signature policy documents, July 2015
http://www.etsi.org/deliver/etsi_ts/119100_119199/11917201/01.01.01_60/ts_11917201v010101p.pdf

[30] ETSI TS 119 312 – Electronic Signatures and Infrastructures (ESI); Cryptographic suites, February 2019
https://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.03.01_60/ts_119312v010301p.pdf

[31] ETSI TS 119 612– Electronic Signatures and Infrastructures (ESI);Trusted Lists, v2.1.1, July 2015
http://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.01.01_60/ts_119612v020101p.pdf

[32] OASIS Digital Signature Service Core Protocols, Elements, and Bindings, v1.0, April 2007
http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf

[33] OASIS Advanced Electronic Signature Profiles of the OASIS Digital Signature Service, v1.0, April 2007
http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-AdES-spec-v1.0-os.pdf

[34] LuxTrust BLINK Portal – Transport Layer Specifications, v1.2.4 or higher, Mars 2018 or later

[35] LuxTrust Cloud Validation Services – Generic DSS Specifications, v1.2.5 or higher, Mars 2020 or later

[36] LuxTrust Cloud Validation Services – Fully Delegated PAdES, v1.2.5 or higher, Mars 2020 or later

[37] LuxTrust Cloud Validation Services – Partially Delegated PAdES, v1.2.5 or higher, Mars 2020 or later

[38] LuxTrust Cloud Validation Services – Partially Delegated XAdES, v1.2.5 or higher, Mars 2020 or later

[39] LuxTrust Cloud Validation Services – Fully Delegated XAdES, v1.2.5 or higher, Mars 2020 or later

Table of Contents

1. Introduction

1.1. Overview

A signature validation policy specifies the rules and constraints that determine the overall behavior and results of a signature validation process concerning all stakeholders involved in a common application context and it is referenced using a globally unique object identifier

The current document presents the LuxTrust validation policies for advanced and qualified signatures and seals (cf. [1]) with the corresponding validation process being exposed as a cloud service via the LuxTrust BLINK portal. No physical person user is directly involved in BLINK workflows. BLINK workflows are completely automated, which means that the protocol for accessing a BLINK service is designed for consumption by automated applications on server machines. Nevertheless, physical person users might be involved when indirectly calling the validation service via business applications. In particular, physical persons might, besides server machines, be consumers of validation reports that are supplied by the service as the result of performed validations.

BLINK exposes its services via restful web interfaces over HTTPS (cf. [7], [8], [9], [10], [11], [12], [13] and [34]), with OASIS DSS being used as the application layer protocol (cf. [32] and [33]). A dedicated XML format (cf. [18], [19] and [20]) has been specified for representing the validation report which is supplied as the result in the service response, with details concerning the report format being contained in the technical specifications of the service (cf. [35], [36], [37], [38] and [39]). Each validation report is formatted as a machine- and human-readable XML document (cf. [18], [19] and [20]) and sealed by LuxTrust (cf. [21], [25] and [26]) with an advanced or qualified electronic seal for proving its authenticity and integrity.

LuxTrust configures its validation service in accordance with one of the validation policies specified in the present document. In addition, an application provider (APP) can define a custom validation policy that must be derived from a policy specified in the present document and agreed to with LuxTrust when concluding a service contract. In that case, the service configuration for the given APP will apply the rules of the agreed derived policy.

The LuxTrust validation service performs validation of electronic signatures and seals on signed artefacts, provided that the to be validated signatures and seals comply with [3] and conform with the supported standards for advanced electronic signatures which are defined in [23] and [24] for PDF documents (cf. [14], [15], [16] and [17]) and in [25] and [26] based on [21] for any generic content. Regardless of specific legal implications, the present document uses the unspecific term *signature* when referring to an electronic signature or to an electronic seal. More specific terms are only used in the present document when an explicit distinction between a signature and a seal is required.

The LuxTrust validation service applies the process specified in [22] with amendments made in [28], while it adheres to the security constraints specified in [27]. Based on [30], the validation process also examines whether applied cryptographic algorithms are strong enough with regard to the assumed signing time of a given signature.

The option to select a validation sub-process by omitting certain evidences as explained in [22] and [28] is not supported. The LuxTrust validation service always considers all applicable and available evidences when performing a validation.

The LuxTrust validation service always applies the **shell model** for X.509 certificate path building and validation (cf. section 5.2.6 of [28]).

The LuxTrust validation service only accepts suitable trust anchors published for the assumed signing time in the Member States trusted lists (cf. [2] and [31]), with the root of the trusted lists being exposed and signed by the European Commission according to the underlying announcement in the European Official Journal. Nevertheless, custom trust anchors can be specified and agreed to when deriving a custom policy.

The LuxTrust validation service validates all signatures of a given input document individually and supplies status indications for each such signature independently of status indications supplied for other signatures pertaining to the same input document. Determining the overall validation outcome from the status indications and structural relationships of the independently validated signatures is left up to the discretion of the calling business application. The LuxTrust validation service does not provide such an interpretation.

The caller of the LuxTrust validation service must directly or indirectly specify the media type (cf. [6]) of an input document for a request which is typically performed by the caller in selecting a dedicated validation mode as explained in the respective service interface specification (cf. [35], [36], [37], [38] and [39]). The validation mode also determines the eligible signature formats for the given request and the specifically applied default policy.

As a general principle, the LuxTrust validation service does not validate whether an input document conforms to a given document format profile. For example, the LuxTrust validation service does not validate, whether a PDF input document conforms to a given PDF archive format profile (cf. [16] and [17]). This particular aspect is completely left up to the discretion of the business application that calls the service.

The LuxTrust validation service is an automated service, which supplies diagnostics regarding the signatures pertaining to a given input. Although the diagnostics are represented in human-readable XML format, it is recommended that the relying party business application visualizes the technical details of the validation result for end-users in a way that is suitable to maximize transparency and understanding of the diagnostics.

Due to the fact that the validation service can also not provide visualization means for the signed content, it is strongly recommended that the relying party business application offers such means in order to enable end users to ensure that the signed content is exactly the one that is expected to be signed in order to suitably honor the *What You See Is What Is Signed* (WYSIWIS), respectively the *What You See Is What Has Been Signed* (WYSIWHBS) paradigm. This aspect is crucial for the overall security model of applied electronic signatures and seals. Specifically PDF documents are known to be vulnerable regarding such attacks, with an intruder being capable for tricking signatories to sign a different version of the document than the intended one. Those attacks may consequently also be employed to deceive relying parties, which can at the same time be signatories.

For enabling business applications to better cope with such attacks, the LuxTrust validation report not only indicates signed byte ranges but all byte ranges of a validated PDF document and additionally outlines which byte ranges are signed by which signature. This information can be useful for a business application to present each version of given PDF document individually combined with diagnostics of a mapped signature if any in order to maximize transparency for end users and thus enabling them to take correct business decisions.

The structure of the present document follows the standard specified in [29].

Due to the subsequently specified rules may appear quite complex to non-technical readers/stakeholders of the present policy document, the remaining part of the present overview provides **an informal, non-normative summary of the essential policy requirements**.

- The present policy document specifies validation rules for electronic signatures and seals that must conform to the ETSI standards for Advanced Electronic Signatures, in particular to PAdES respectively XAdES (cf. [23], [24], [25] and [26]).

- Although an individual policy is defined for each supported signature format and validation mode for the purpose of appropriately addressing signature format-specific details and mode-depending responsibilities of the involved actors, namely LuxTrust and the APP that has a validation service contract with LuxTrust, the overall set of validation rules is common for all policies of the present document[1].

- In the fully delegated validation mode, the service receives entire document from the business application, in particular a PDF document in the case of a PAdES-specific policy, respectively an XML document in the case of a XAdES-specific policy and is consequently enabled to specifically validate, whether a hash calculated over signed content matches with the hash in the corresponding signed data object. The input document is instantly deleted after validation. By, contrast in the partially delegated validation mode, the service only receives a set of signed data objects in the case of a PAdES-specific policy, respectively a signed Manifest in the case of a XAdES-specific policy, which in that case obliges the business application to specifically verify, whether supplied hashes match with the actually signed content.

- In any case, the business application must enable relying party end-user to visualize signed parts/versions of a document in order to verify whether the signed content matches with the user's expectations so that the right decisions can be taken and that prevention of fraud is better addressed.

- The validation service validates all signatures and seals pertaining to the same input document and supplies resulting diagnostics in a single report. It does however not make any interpretation of supplied diagnostics or mutual relationship of those signatures and seals.

- The validation algorithm conforms to [28]. It uses the shell model for certificate validation as specified in section 5.2.6 of that standard. The algorithm only uses trust anchors that are published in the Member States Trusted Lists (cf. [2] and [31]), unless custom trust anchors are explicitly agreed between LuxTrust and the APP based on a derived policy.

- The validation algorithm only accepts trusted and qualified timestamps as proofs of existence of data that are used during validation. During this process, any expired or obsolete elements are not taken into account. In particular, expiration can also concern cryptographic algorithms when they do not conform to the requirements specified in [30] for the point of time for which they are required to be resilient. The validation algorithm always takes all eligible elements contained in a signed data object into account for performing a *Validation for Signatures providing Long Term Availability and Integrity of Validation Materia*l based on the actually

[1] The common rules are detailed in the initial chapters, while the specific rules are contained in the annexes of the present document.

existing profile of a given signature as specified in section 5.1.2 of [28], with optional sub-process selection not being supported.

- The validation algorithm verifies and determines signed attributes contained in a signed data object, in particular signature policy and commitment type indications. It does however not interpret those elements and leaves it up to the discretion of the business applications as to whether those elements are used for taking further business decisions.

1.2. Business or Application Domain

1.2.1. SCOPE AND BOUNDARIES OF VALIDATION POLICIES

The validation policies specified in the present document are suitable for a large scope of application and business domains, whenever there is a need for validating electronic signatures.

An APP is responsible for the technical integration of the LuxTrust validation service into its application workflow(s). Due to the service being exposed via the BLINK portal, end users are not directly involved in the exchanges between the application and the service portal. Consequently, no provisions are made for interfacing with physical users that may indirectly receive and consume service results via the business application calling the LuxTrust validation service.

The present policy document defines explicit requirements regarding the actors (LuxTrust and APP), and additional options, which can be exploited by an APP for defining complementary policy constraints as needed. An APP shall derive its specific rules when needed from a policy defined by the present document.

Independently of the media type of input documents, The LuxTrust validation service can generally be called by an APP in a **Partially Delegated Mode** or in a **Fully Delegated Mode**, while the former means that the APP only sends a digest value of signed data, i.e. a signed data representation (SDR) to the service, with the entire signed data (SD) being sent in the latter case. Therefore, the APP takes more responsibilities in the **Partially Delegated Mode** due to having to validate, whether a supplied digest value matches the corresponding signed data.

Due to the absence of a graphical user interface, the APP must irrespectively of the working mode

- ensure that the content of the signed data corresponds to the SD and
- enable physical person relying parties to visualize the content as needed
- make provisions regarding suitable consumption of the outcome of the validation process
    - By enabling parsing and interpretation of the validation report in a suitable automated manner and/or
    - By enabling physical person relying parties to visualize the validation report, which can be achieved via a suitable trustworthy browser.
    - By enabling physical person relying parties to suitably visualize both, signed and unsigned parts of the content, and to provide guidance and awareness regarding

possible attacks that may trick end users when omitting WYSIWHBS verification (also cf. 1.1)[2]

1.2.2. DOMAIN OF APPLICATIONS

Not applicable (unrestricted)

1.2.3. TRANSACTIONAL CONTEXT

In its own signature policy, the APP may define the final transactional context, according to its needs. For the purpose of the present policies, signature validation takes place within the context of the validation flow specified by LuxTrust, through a sequence of messages exchanged between the APP and the LuxTrust BLINK portal.

In order to do so, requests and responses are exchanged via a mutually authenticated restful HTTP-based web service (cf. [7], [8], [9], [10], [11], [12], [13] and [34]), which is exposed by the BLINK portal to the APP business application[3]. A dedicated application-layer profile based on the DSS Verify request/response is used to represent validation requests/responses (cf. [32], [33], [35], [36], [37], [38] and [39]).

1. Depending on the chosen validation mode (cf. 1.2.1), the APP sends a validation request to the LuxTrust portal that either contains the document(s) to be validated or digest values thereof together with signatures and complementary transactional parameters.

2. The LuxTrust service parses the request and

    2.1. when successful

        2.1.1. performs the validation on the input

        2.1.2. creates a validation report

        2.1.3. seals the created report and

        2.1.4. returns a response comprising the sealed report

    2.2. otherwise

        2.2.1. returns an error message

In this respect, the LuxTrust validation service operates independently of APP's context.

When using a **Partially Delegated Mode**, it is the APPs responsibility to validate that each sent digest value matches with the corresponding signed data, while such a complementary validation

[2] The LuxTrust validation service report contains appropriate information for enabling business applications to implement suitable end user support (e.g. bytes ranges that in the case of PDF documents may be used for presenting each document version individually).
[3] Note that transport layer details (cf. [34]) apply entirely to validation service, even when they had initially been specified for creation services only.

should ideally happen prior to call the LuxTrust validation service in order to avoid unnecessary service requests in the case of a mismatch.

For the purpose of matching a digest value with signed data, it is important

- To apply the digest algorithm which had been specified during signature creation,
- That the applied digest algorithm is considered secure (cf. [30]) at the time of signing and has not become weak until the time of validation or has been protected by complementary preservation means,
- That the implementation for (re-)calculating the applied digest algorithm is correct and trustworthy and
- That any explicit or implicit transformation of input bytes for calculating the corresponding digest value is correct with respect to the media type of the given input document (cf. [6]). For instance, in the case of a PDF document (cf. [14] and [15]), the byte ranges indicated in the signature dictionary directly specify the input bytes for digest calculation, while in the case of a generic document (cf. [21]) explicitly or implicitly defined content transformations might be necessary in order to obtain the input bytes for digest calculation.

1.3. Document and Policy Names, Identification and Conformance Rules

1.3.1. VALIDATION POLICY DOCUMENT AND VALIDATION POLICY NAMES

The validation policies covered by the current document are ***LuxTrust Cloud Validation Policies*** with specific annexes for supported AdES formats and individual operation modes.

1.3.2. VALIDATION POLICY DOCUMENT AND VALIDATION POLICY IDENTIFIERS

Validation policy name	Validation policy OID
LuxTrust Fully Delegated PAdES AdES Validation Policy	1.3.171.1.4.2.1.1
LuxTrust Partially Delegated XAdES AdES Validation Policy	1.3.171.1.4.2.2.1
LuxTrust Partially Delegated PAdES AdES Validation Policy	1.3.171.1.4.2.3.1
LuxTrust Fully Delegated XAdES AdES Validation Policy	1.3.171.1.4.2.4.1
LuxTrust Fully Delegated PAdES QES Validation Policy	1.3.171.1.4.4.1.1
LuxTrust Partially Delegated XAdES QES Validation Policy	1.3.171.1.4.4.2.1
LuxTrust Partially Delegated PAdES QES Validation Policy	1.3.171.1.4.4.3.1
LuxTrust Fully Delegated XAdES QES Validation Policy	1.3.171.1.4.4.4.1

1.3.3. CONFORMANCE RULES

Electronic signatures validated under the present validation policies (1.3.1) comply with the eIDAS Regulation on electronic identification and trust services for electronic transactions (cf. [1]).

The content of the present document conforms to [29].

1.3.4. DISTRIBUTION POINTS

The validation policy document is available on the LuxTrust website (cf. base URL https://www.luxtrust.lu/en/repository).

1.4. Validation Policy Document Administration

1.4.1. VALIDATION POLICY AUTHORITY

LuxTrust contact information	
Postal Address	LuxTrust S.A. IVY Building 13-15, Parc d'Activités L-8308 Capellen
E-mail address	mailto:cspboard@luxtrust.lu
Website	www.luxtrust.lu

1.4.2. CONTACT ADDRESS

For specific questions concerning the present policy document, please use the following email address or telephone number:

Email: questions@luxtrust.lu

Phone: +352 24 550 550

1.4.3. APPROVAL PROCEDURES

The Policy Approval Authority within LuxTrust S.A. is the LuxTrust CSP Board. LuxTrust announces modifications of the published validation policies prior to those policies becoming applicable.

1.5. Definitions and Acronyms

API	Application Programming Interface
APP	Application Provider
BSP	Business Scoping Parameter
CA	Certification Authority
DA	Driving Application Application of the APP that supplies the SD
DTBS	Data to Be Signed or Data Been Signed Comprises the SD and additional attributes for being signed or being validated
DTBSF	Data to Be Signed Formatted or Data Been Signed Formatted Components of the DTBS, formatted and put in the correct sequence for the chosen SDO type
DTBSR	Data to Be Signed Representation or Data Been Signed Representation Data sent by the SCA to the SCDev for signing, usually a secure digest value of the DTBSF
PAdES	PDF Advanced Electronic Signature
PDF	Portable Document Format
POE	Proof of Existence of some data, typically provided by means of a trusted or qualified timestamp
SCA	Signature creation application
SCDev	Signature Creation Device Cryptographic device or server system for creating an electronic signature of a DTBSR
SD	Signer's Document or Signed Data Document selected for signing or Signed Document, with semantic depending on the corresponding use case (signature creation or validation)
SDO	Signed Data Object Result of the SCA process after integrating of the signed DTBSR regarding the respective SDO type
SDR	Signer’s Document Representation or Signed Data Representation Usually a secure digest value of an SD
SDO type	Format of the SDO An interoperable advanced electronic signature standard; cf. [23], [24], [25] and [26]
Signatory	The physical or legal person which creates an advanced electronic signature or seal
SP	Service provider Alternative name for an APP
SVA	Signature Validation Application
TSA	Time-Stamping Authority
TSL	Trust Service List of a Member State
XAdES	XML Advanced Electronic Signature
XML	Extensible Markup Language
Augmentation	The process of incorporating certain material like time stamps, validation data and even archival-related material into signatures in order to make them more resilient against change or for extending their longevity
Validation Data	Elements that prove that the signature validation has passed or failed like certificates of intermediate CAs, OCSP responses or CRLs

2. Validation Application Practices Statements

2.1. Requirements for Application Provider Applications

According to the signature validation model of [22] and amendments originating from [28], the APP application is the DA, which is, an *application that uses a signature validation system to validate a signature*[4]. As such, an APP application must conform to the technical specifications (cf. [34] and [35]) and to the mode-specific protocol specifications regarding the selected validation mode (cf. [36], [37], [38] and [39]). It must additionally follow LuxTrust technical and integration guidance. In particular,

- It must not send ill-formed or malicious data (messages) to the LuxTrust portal,
- It must not tamper with or examine/record data exchanged between the LuxTrust validation service and the business application,
- It must not tamper with LuxTrust client-side software components,
- It must securely maintain logs to ensure the imputability of transactions between its application and the LuxTrust validation service.

When working in **Partially Delegated Mode** (cf. 1.2.1), the APP directly contributes to the implementation of the validation service. Its application must additionally satisfy the requirements specified in [27] as far as it takes certain service responsibilities into account, such as validating whether a digest value supplied to the validation service matches with the corresponding signed data.

2.2. Requirements for the Signature Creation/Verification Application

When applicable, i.e. when integrating a web interface, DA, SCA and SVA development shall follow the Open Web Application Security Project (OWASP) best practices.

For signature creation and validation, the relevant requirements from [27] are applicable.

Additionally, the requirements and guidelines specified in section 1.2.1, specifically with regard to transparency, security and coverage of the WYSIWHBS aspect, shall be taken into account by the APP.

[4] Instead of directly integrating the LuxTrust validation service, the APP may alternatively integrate the LuxTrust COSI application that exposes a simplified restful API and rich signature workflow management capabilities for widely leveraging access to LuxTrust services. In this case, COSI becomes part of the DA.

3. Business Scoping Parameters

The description of the validation policies general business scoping parameters (BSP) is applicable to all business cases and is independent of the employed signature format.

Format and working mode specific BSPs, which are specified in the respective annexes, complete the general BSPs:

- Annex A: Fully Delegated PAdES Validation Requirements
- Annex B: Partially Delegated XAdES Validation Requirements
- Annex C: Partially Delegated PAdES Validation Requirements
- Annex D: Fully Delegated XAdES Validation Requirements

Description of the *validation mode* between LuxTrust and the APP is contained in 3.2.4.

3.1. BSPs Mainly Related to the Concerned Application/Business Process

3.1.1. BSP (a): WORKFLOW (SEQUENCING AND TIMING) OF SIGNATURES

The present validation policies address validation of the advanced electronic signatures comprising possible timestamps and proof-data extensions regarding a single instance or multiple instances of DTBS during a single transaction[5], while a single report is returned by the service after a successfully performed validation.

LuxTrust validation service can be used by an APP to implement business workflows comprising multiple transactions; in such a case, each single transaction within the APP workflow will be performed according to one of the present policies depending on the chosen validation mode. The APP validation policy shall in that case describe the workflow that manages the individual validation transactions.

3.1.2. BSP (b): DATA TO BE VALIDATED

The APP is responsible for the content and the correct formatting of the data to be validated with respect to applicable standards. In particular, it must ensure that the data to be validated does not contain malicious code or scripts that could alter the data to be validated or damage LuxTrust services (also cf. remarks regarding signed content in section 1.1).

In particular, the format of an SD can be PDF (Annex A: Fully Delegated PAdES Validation Requirements or Annex C: Partially Delegated PAdES Validation Requirements) or any generic document format (particularly XML) (Annex B: Partially Delegated XAdES Validation Requirements or Annex D: Fully Delegated XAdES Validation Requirements).

[5] Note that technical availability of individual service features depends on the actual implementation status of the LuxTrust portal (cf. [35], [36], [37], [38] and [39] for further technical details).

The LuxTrust validation service guarantees the confidentiality of an SD according to applicable laws on privacy and Luxembourg laws regarding the financial sector. LuxTrust particularly and immediately erases all copies of a received SD, if any, from its servers after having performed a requested transaction.

3.1.3. BSP (c): THE RELATIONSHIP BETWEEN SIGNED DATA AND SIGNATURE(S)

The relationship between signed data and signature(s) specifically depends on the signature profile. The supported signature profiles (from [22]) are:

1. B-B (basic signature)
2. B-T (signature with time)
3. B-LT (signature with long-term validation material)
4. B-LTA (Signatures providing long-term availability and integrity of validation material)

The present document defines two sets of validation policies that determine the overall rules applied during a given validation transaction for implementing the process specified in the applicable standards (cf. [22] and [28]), i.e.

- a set of policies for validating whether a given examined digital signature achieves an eIDAS legal type of at least an Advanced Electronic Signature (using the policy label *AdES*; cf. [1], [2] and [31]), which is the default, and
- a set of policies for validating whether a given examined digital signature achieves an eIDAS legal type of a Qualified Electronic Signature (using the policy label *QES*; cf. [1], [2] and [31])

The validation report will also indicate the corresponding legal type for examined signatures and involved timestamps in the event that they can be validated successfully.

3.1.4. BSP (d): TARGETED COMMUNITY

Unless otherwise specified within a derived APP validation policy, the LuxTrust validation service validates signatures based on the European trusted lists (cf. [2] and [31]) and complies with the eIDAS Regulation [1].

In accordance with LuxTrust, an APP may define a custom validation policy for integrating particular trust anchors and/or for excluding default trust anchors in order to use the resulting configuration to enable specific certificate path validations. In such a case, LuxTrust cannot be held responsible for acceptance or rejection of validated signatures by third party software that cannot support such a configuration or that is not aware of it.

3.1.5. BSP (e): ALLOCATION OF RESPONSIBILITY FOR SIGNATURE VALIDATION AND AUGMENTATION

In addition to the clock of the service host, which is synchronized with a trustworthy accurate time source, the LuxTrust validation service employs trusted and qualified timestamps (cf. [1]) according to the request profile (B-T, B-LT or B-LTA) as a proof of existence (POE; cf. [22] and [28]) regarding

elements of the DTBS that are cryptographically covered by the given timestamps; section 3.2.3 provides further details concerning timestamping of signatures.

When working in **Fully Delegated Mode** (cf. 1.3.2), the LuxTrust validation service validates existing signatures on the DTBS. Should the DTBS contain an invalid signature, that information is indicated in the result supplied by the service. LuxTrust will NOT abort the validation process due to an invalid signature being contained in the DTBS.

A single validation report supplied by the LuxTrust validation service may contain results regarding multiple signatures pertaining to an SD, while any interpretation of those results or an overall diagnostics of the outcome, in particular any semantic interrelationship of independently validated signatures, is completely left up to the business application. The LuxTrust validation service does not perform any semantic interpretations; it solely provides diagnostics regarding individually validated signatures in accordance with the applicable standards (cf. [22] and [28]).

This also applies when working in **Partially Delegated Mode** (cf. 1.3.2); however, validation performed by the LuxTrust service does in this particular case not cover the aspect of whether a provided SDR matches with the corresponding SD. This latter aspect must be guaranteed by the APP in order to ensure an appropriate and complete validation in its business application.

When requiring long-term validation for signatures, the APP must make provisions for suitable augmentation, while this functionality can be provided by LuxTrust as a complementary service.

Alternatively to the validation or augmentation of signatures using LuxTrust services, the APP may manage these operations independently by possibly using third party tools. In this case, the APP becomes solely responsible for correct validation and/or augmentation.

3.2. BSPs Mainly Influenced by the Legal/Regulatory Provisions Associated to the Concerned Application/Business Process

3.2.1. BSP (f): LEGAL TYPE OF THE SIGNATURES

The LuxTrust validation service supports validation for all legal types of advanced electronic signatures for legal persons or for physical persons that act on their own behalf or on behalf of a legal person (cf. [1]):

1. Qualified electronic signatures supported by an X.509 v3 qualified certificate;
2. Advanced electronic signatures supported by an X.509 v3 qualified certificate;
3. Advanced electronic signatures supported by an X.509 v3 certificate

By achieving one of the above-cited legal types after successful validation and by using trust anchors published in the Member States trusted lists (cf. [2] and [31]), the corresponding advanced electronic signature indicates by virtue of the underlying supervision process that it is[6]

[6] As defined in [1], art. 26 and art. 36 respectively

(a) Uniquely linked to the signatory;

(b) Capable of identifying the signatory;

(c) Created using electronic signature creation data that the signatory can, with a high level of confidence, use under his or her sole control; and

(d) Linked to the data signed therewith in such a way that any subsequent change in the data is detectable.

The APP shall define the actual requested minimum legal type for signatures in its policy and process. Optionally, the APP can enforce a qualified legal type for all signatures to be validated during a single service transaction by specifying the corresponding policy in the request (cf. 1.3.2 and [35]).

Optionally, the APP may with LuxTrust consent derive a custom policy for particularly implementing trust anchors that are not published in the Member States trusted lists.

As mentioned in section 3.1.3, the legal type of a signature is indicated in the validation report when it can be validate successfully.

3.2.2. BSP (g): COMMITMENT ASSUMED BY THE SIGNATORY

The APP, depending on its use case, may define an expected commitment type for a signature. The LuxTrust validation service can reveal the commitment type when associated with a given signature for being taken into account by the business application.

The validation service does not interpret a commitment type that is associated with a signature.

3.2.3. BSP (h): LEVEL OF ASSURANCE ON TIMING EVIDENCES

The APP, depending on its use case, MAY define expected timing evidences for a signature. The LuxTrust validation service can, in addition to the validation point in time, also reveal

- A claimed signing time and
- Trusted or qualified time stamps based on trust anchors that are verifiable according to the Member States trusted list (cf. [2] and [31]).

Any such indication, except for a claimed signing time, may not only serve as a proof of existence (POE; cf. [22] and [28]) used by the service to perform validation of signatures beyond the validity period of involved certificates, but it can also represent a trustworthy time indicator for the business application in order to make workflow decisions on its own discretion.

The LuxTrust validation service does not interpret timing evidences beyond the fact of using them for performing signature validation as detailed in [22] and [28].

3.2.4. BSP (i): FORMALITIES OF VALIDATION

The APP, depending on its use case, may require certain formalities of validation. The LuxTrust validation service can reveal signature policy identifiers associated with a given signature for being taken into account by the business application.

The LuxTrust validation service does not interpret rules specified by signature policies that are associated with a signature. It only validates the integrity of the signature policy document when it is referenced via a URI and combined with a policy hash as part of the signature policy indication (cf. [22] and [28]).

The business application can use the content of such a referenced policy document upon successful validation in order to make workflow decisions on its own discretion. This latter option also applies to other signed attributes that are detected by the validation service.

Independently of any specific formalities of validation, the APP business application must in **Partially Delegated Mode** make additional provisions as it is described in 3.1.5 and 1.2.3 for complementing the validations performed by the LuxTrust validation service.

3.2.5. BSP (j): LONGEVITY AND RESILIENCE TO CHANGE

The expected longevity of an electronic signature depends on its profile.

- B-B signature: the signature's longevity is that of the signing certificate at the time of signing, unless the signer certificate or any ancestor certificate in the issuer chain up to the trust anchor has been revoked after signing, which in that case would instantly render the signature unverifiable.

- B-T signature: the signature's longevity is that of the signing certificate at the time of signing and is possibly extended beyond its lifetime when suitable online certificate status proofs are available. The time of signing is in this case confirmed by means of a signature timestamp, with the signature timestamp being a pre-requisite for such an extended longevity beyond the lifetime of the signing certificate. Extended longevity can be supported in this case up to the longevity of the timestamping certificate at the time of signature timestamp creation. Contrarily to a B-B signature, revocation of the signing certificate or revocation of any ancestor thereof after creation of the signature timestamp has no impact on the longevity of a B-T signature. By contrast, extended longevity of a B-T signature can be impacted when a cryptographic algorithm, which was involved in the creation of the signature timestamp, has becomes weak over time (cf. 3.4.2 regarding use and resilience of cryptographic algorithms).

- B-LT signature: the signature's longevity is that of the above-cited B-T signature. It is augmented by proof elements added to the signed data object for partly enabling offline validation of the signature depending on the longevity and eligibility of added proof data. It is important to note that longevity of a signature is not extended beyond that of aforementioned B-T augmentation, solely due to the use of additional offline status proofs. However, B-LT augmentation can facilitate the overall validation process and serve as preparatory step for B-LTA augmentation.

- B-LTA signature: the signature's longevity is that of the above-cited B-T or B-LT signature. It is augmented with complete proof elements regarding pre-existing elements of the signed data object that are needed for validation of the signer's signature, with the entire structure being covered by a document/archive timestamp. This enables extension of signature longevity up to the longevity of the timestamping certificate of that covering document/archive timestamp at the time of its creation. This maximum signature longevity extension also requires that all proofs added for the sake of augmentation are eligible and remain during the desired period assessable as valid at the time of document/archive

timestamp creation, while such an assessment also relies on availability of suitable online status proofs. An extended longevity of a B-LTA signature can be impacted when a cryptographic algorithm, which was involved in the creation of the document/archive timestamp, has become weak over time (cf. 3.4.2 regarding use and resilience of cryptographic algorithms).

- A B-LTA signature can repeatedly be augmented by adding an enveloping B-LTA structure, whenever timely necessary due to the risk of expiration of any involved proof element or exceptionally, due to premature weakness of a cryptographic algorithm employed by any of the involved proof elements that have been added since the preceding B-LTA augmentation. It has to be kept in mind that creation of a new document/archive timestamp protects cryptographic algorithms of all covered structures from becoming weak provided that the algorithms used for creating that new timestamp remain resilient or are otherwise covered by another resilient timestamp prior to becoming weak.

- A B-LTA signature can repeatedly be augmented as often as necessary for spanning the entire required period of longevity of the initial signer's signature. As an alternative to repeated B-LTA augmentation, a centralized electronic signature preservation service (cf. [4] and [5]) may be employed to ensure an equivalent period of longevity.

In any case, the cryptographic algorithms and parameters are verified with regard to applicable cryptographic standards (cf. [30]) in order to ensure that the electronic signature's resilience can be confirmed for a given signed artefact with respect to the closest proof of existence (POE; cf. [22] and [28]) that can be detected by the validation process.

Even when the LuxTrust validation service does not support optional sub-process selection for deliberately limiting evidences to a given signature profile (also cf. section 1.1) and instead takes all available evidences into account, which are contained in a given signed data object and which make up the signature's actually existing profile, for performing *Validation for Signatures providing Long Term Availability and Integrity of Validation Materia*l, the LuxTrust validation service supports all above-cited profiles as it requested for this purpose in section 5.1.2 of [28].

In this process, obsolete elements or elements that are expired at validation time are not considered as eligible proof data for determining signature validity.

In order to prevent elements from expiring prior to reaching the end of the needed validity period as defined by the business application, it is strongly recommended that APPs make provisions for timely augmentation of signatures and seals as it is described in section 3.1.5.

Independently of the aforementioned provisions, the LuxTrust validation service tries to obtain proof data online as needed, in particular when stored elements are missing or expired in the signed data object at validation time, for the purpose of determining the signature's overall diagnostics.

It has however to be kept in mind that online proof data may not be suitable to cope with situations that cryptographic algorithms on crucial elements of a signed data object are no longer eligible according to the rules specified in section 3.4.2. In those particular cases, timely augmentation as indicated in section 3.1.5 becomes inevitable for ensuring sufficient resilience with regard to the required long-term validity of signatures and seals.

3.2.6. BSP (k): ARCHIVING

The present policy imposes no specific archiving requirements for signatures. The longevity of the latter (cf. 3.2.5) must be tailored by the APP so that it is sufficient for the considered use case. An advanced electronic signature is generally self-contained and does consequently besides certificate status services and reliable provision of trust anchors not require additional out-of-band information for proofing its evidence.

If needed, archiving of the signature has to be taken into account by the APP, which may delegate it to the signatory with respect to its own signature policy or terms of use. The LuxTrust validation service can only consider evidences that are provided in a validation request. Consequently, the APP must make provisions for suitable longevity of to be validated signatures (cf. 3.2.5) in a timely manner in order to ensure its resilience and availability at the time of validation.

Nevertheless, the LuxTrust validation service transaction logs are backed up in order to provide complementary evidence concerning the supplied service, archived for 10 (ten) years and accessible for use during legal proceedings[7].

The following types of evidence can be revealed by the LuxTrust transaction log:

- The record creation time which is synchronized with a trustworthy accurate time source
- The unique identifier of the requesting APP
- The entire validation report comprising the relevant transactional information
- Whether the request was successful

3.3. BSPs Mainly Related to the Actors Involved in Creating/Augmenting/Validating Signatures

3.3.1. BSP (l): IDENTITY (AND ROLES/ATTRIBUTES) OF THE SIGNATORIES

The APP, depending on its use case, may define certain restrictions regarding the identity of the signatory of a given signature; technically, the validation service reveals the signatory identity, which can be taken into account by the business application for making workflow decisions at its own discretion.

The present validation policy contains no requirement concerning the signatory's role. When specific constraints are required by the business use case (signature delegation, power of attorney like authority to act on the behalf on some organization, etc.) they shall be described in the APP signature policy or terms of use and implemented by the APP workflow.

[7] Note that the indicated retention period can be adapted based on an APP-specific policy if a specific contract has been established with LuxTrust beforehand.

3.3.2. BSP (m): LEVEL OF ASSURANCE REQUIRED FOR THE AUTHENTICATION OF THE SIGNATORY

The signatory level of assurance is implied by performing validation based on the trust anchors published in the Member States trusted lists (cf. (cf. [2] and [31]), unless this requirement is changed in the context of a derived custom validation policy.

The APP, depending on its use case, may define restrictions regarding the minimum assurance level required for identifying or authenticating the signatory of a given signature. The LuxTrust validation service reveals the legal type of a signature (cf. 3.1.3 and 3.2.1), which ensures the corresponding minimum assurance level (cf. [1]). The business application can consider this information for making workflow decisions at its own discretion (cf. 3.1.4 for accepted trust anchors).

3.3.3. BSP (n): SIGNATURE CREATION DEVICES

Upon successful validation of a signature, the LuxTrust validation service implicitly reveals by detection of the legal type of a signature (cf. 3.1.3 and 3.2.1), whether a **Qualified Signature Creation Device** (QSCD) according to [1] has been used by the signatory. The business application can use this information in order to make workflow decisions on its own discretion.

3.4. Other BSPs

3.4.1. BSP (o): OTHER INFORMATION TO BE ASSOCIATED WITH THE SIGNATURE

No specific requirement

3.4.2. BSP (p): CRYPTOGRAPHIC SUITES

Unless otherwise specified in the configuration of the service for the APP, the eligible cryptographic suites for signature validation are taken from [30] while support of algorithms being restricted to the technical capabilities of the service (cf. 3.4.3)

3.4.3. BSP (q): TECHNOLOGICAL ENVIRONMENT

The LuxTrust specifications (cf. [34], [35], [36], [37], [38] and [39]) specify technological constraints on the environment.

4. Requirements for Statements on Technical Mechanisms and Standards Implementation

Validation policy statement summaries are format- and working-mode-specific (cf. Annex A: Fully Delegated PAdES Validation Requirements or Annex B: Partially Delegated XAdES Validation Requirements or Annex C: Partially Delegated PAdES Validation Requirements or Annex D: Fully Delegated XAdES Validation Requirements).

5. Other Business and Legal Matters

The present section is addressed in the contract between LuxTrust and the APP.

6. Compliance Audit and Other Assessments

The present section is addressed in the contract between LuxTrust and the APP.

7. Annex A: Fully Delegated PAdES Validation Requirements

This section contains the specific requirements for **Fully Delegated PAdES** validation mode.

7.1. BSPs Mainly Related to the Concerned Application/Business Process

7.1.1. BSP (a): WORKFLOW (SEQUENCING AND TIMING) OF SIGNATURES

PAdES signatures are serial.

7.1.2. BSP (b): DATA TO BE VALIDATED

In the context of PAdES, the SD must be a PDF document, as defined in [14] and [15].

When the signature's level is B-B or B-T, the SD should be in PDF/A-1b or PDF/A-2b format (cf. [16] and [17]).

When the signature's level is B-LT or B-LTA, the SD should be in PDF/A-1a or PDF/A-2a format (cf. [16] and [17]).

7.1.3. BSP (c): THE RELATIONSHIP BETWEEN SIGNED DATA AND SIGNATURE(S)

In the context of the present policy, the signature is embedded within the signed PDF document, as defined in [23] and [24].

7.1.4. BSP (d): TARGETED COMMUNITY

No further requirement beyond 3.1.4

7.1.5. BSP (e): ALLOCATION OF RESPONSIBILITY FOR SIGNATURE VALIDATION AND AUGMENTATION

No further requirement beyond 3.1.5

7.2. BSPs Mainly Influenced by the Legal/Regulatory Provisions Associated to the Concerned Application/Business Process

7.2.1. BSP (f): LEGAL TYPE OF THE SIGNATURES

No further requirement beyond 3.2.1

7.2.2. BSP (g): COMMITMENT ASSUMED BY THE SIGNATORY

No further requirement beyond 3.2.2

7.2.3. BSP (h): LEVEL OF ASSURANCE ON TIMING EVIDENCE

No further requirement beyond 3.2.3

7.2.4. BSP (i): FORMALITIES OF VALIDATION

No further requirement beyond 3.2.4

7.2.5. BSP (j): LONGEVITY AND RESILIENCE TO CHANGE

No further requirement beyond 3.2.5

7.2.6. BSP (k): ARCHIVAL

No further requirement beyond 3.2.6

7.3. BSPs Mainly Related to the Actors Involved in Creating/Augmenting/Validating Signatures

7.3.1. BSP (l): IDENTITY (AND ROLES/ATTRIBUTES) OF THE SIGNATORIES

No further requirement beyond 3.3.1

7.3.2. BSP (m): LEVEL OF ASSURANCE REQUIRED FOR THE AUTHENTICATION OF THE SIGNATORY

No further requirement beyond 3.3.2

7.3.3. BSP (n): SIGNATURE CREATION DEVICES

No further requirement beyond 3.3.3

7.4. Other BSPs

7.4.1. BSP (o): OTHER INFORMATION TO BE ASSOCIATED WITH THE SIGNATURE

No further requirement beyond 3.4.1

7.4.2. BSP (p): CRYPTOGRAPHIC SUITES

No further requirement beyond 3.4.2

7.4.3. BSP (q): TECHNOLOGICAL ENVIRONMENT

No further requirement beyond 3.4.3

7.5. Technical Counterparts of BSPs – Statement Summary

TABLE 7.1: VALIDATION POLICY STATEMENT SUMMARY

Name and identifier of the signature policy authority: LUXTRUST PKI (1.3.171.1)
Name and identifier of the signature policy: • AdES Minimum Legal Level ➔LuxTrust Fully Delegated PAdES AdES Validation Policy (1.3.171.1.4.2.1.1) • QES Minimum Legal Level ➔ LuxTrust Fully Delegated PAdES QES Validation Policy (1.3.171.1.4.4.1.1)

BSP	BSP title	Business statement summary	Technical statement counterpart
(a)	**Workflow (sequencing & timing) of signatures**	Workflow is defined by the APP from among the following signature profiles: 1) basic signature 2) signature with time 3) signature with long-term validation material 4) signatures providing long-term availability and integrity of validation material	PAdES signatures are serial Signature profiles specified in [22] and [28]
(b)	**Data to be validated (DTBS)**	Format: PDF	Media types specified in [14], [15], [16] and [17]
(c)	**Relationship between DTBS & signature(s)**	PAdES signature format required Defined by the APP from among the following signature profiles: 1) basic signature 2) signature with time 3) signature with long-term validation material 4) signatures providing long-term availability and integrity of validation material	PAdES signatures are enveloped Signature format specified in [23] and [24] Signature profiles specified in [22] and [28]
(d)	**Targeted community**	Any entity that must be or that chooses to be compliant with the eIDAS Regulation	AdES Signature format and Member States trusted lists (cf. [2] and [31]), unless overridden by a custom policy
(e)	**Allocation of responsibility for signature validation and augmentation**	DTBS validated by LuxTrust Augmentation to be performed by APP if required	Provisions made by APP when needed as indicated in 7.1.5 and 3.1.5
(f)	**Legal type of signature**	Upon successful validation, one of the following types: 1. Qualified electronic signatures; 2. Advanced electronic signatures supported by a qualified certificate; 3. Advanced electronic signatures	Parameters in the verify request (cf. [35], specifically validation policy OID)
(g)	**Commitment assumed by the signatory**	Attribute is detected when available	No interpretation performed by validation service
(h)	**Level of assurance on timing evidence**	Trusted and Qualified timestamps, validation time supplied by SVA, claimed signing time detected	Detected and verifiable elements; except for claimed signing time, used as POE; no further interpretation performed by validation service
(i)	**Formalities of validation**	No requirement beyond the general ones of 3.2.4; Signature policy identified detected when available and signature policy hash validated when applicable according available signature content	No signature policy interpretation performed by validation service
(j)	**Longevity & resilience to change**	Detection of maximum resilience according AdES profile of signature	Signature profiles specified in [22] and [28]
(k)	**Archival**	No requirement	
(l)	**Identity of signatories**	No requirement	
(m)	**Level of assurance required for the authentication of the signatory**	No requirement besides eIDAS regarding applied policy; validation based on Member States trusted lists (cf. [2] and [31]), unless overridden by a custom policy	No interpretation performed by validation service besides detection of the underlying legal signature type
(n)	**Signature creation devices**	Implicit detection of QSCD in case of QES	No interpretation performed by validation service
(o)	**Other information to be associated with the signature**	No requirement	

(p)	**Cryptographic suites**	Cryptographic suites satisfying [30]	LuxTrust cryptographic libraries
(q)	**Technological environment**	LuxTrust s specifications (cf. [34], [35], [36], [37], [38] and [39])	LuxTrust implementation
Signature creation/validation application practices statements		-	-

The APP defines other parameters like specific (signed and unsigned) attributes and placement of a visible signature etc.

7.6. Input and Output Constraints for Signature Creation, Augmentation and Validation Procedures

7.6.1. INPUT CONSTRAINTS TO BE USED WHEN GENERATING, AUGMENTING AND/OR VALIDATING SIGNATURES IN THE CONTEXT OF THE IDENTIFIED VALIDATION POLICY

TABLE 7.2: ADDITIONAL VALIDATION POLICY CONSTRAINTS

Name and identifier of the signature policy authority: LUXTRUST PKI (1.3.171.1)
Name and identifier of the signature policy: • AdES Minimum Legal Level ➔LuxTrust Fully Delegated PAdES AdES Validation Policy (1.3.171.1.4.2.1.1) • QES Minimum Legal Level ➔ LuxTrust Fully Delegated PAdES QES Validation Policy (1.3.171.1.4.4.1.1)

BSP	BSP title	Constraint value for signature validation (SVA or APP)
(a)	**Workflow (sequencing & timing) of signatures**	SVA constraints: • SequencingNature: Mandated-serial • TimingRelevance: TimingRelevanceOnEvidence: 1) MandatedSignedQProperties-signing-time 2) MandatedUnsignedQProperties-signature-time-stamp 3) MandatedUnsignedQProperties-signature-time-stamp 4) MandatedUnsignedQProperties-signature-time-stamp and MandatedUnsignedQProperties-archival-form
(b)	**Data to be validated (DTBS)**	APP constraints: • ConstraintOnDTBS: PDF • DOTBSAsAWholeOrInParts: whole
(c)	**Relationship between DTBS & signature(s)**	APP constraints: • ConstraintsOnTheNumberOfDOTBS=1 • SignatureRelativePosition: enveloped 1) MandatedSignatureFormat: PAdES B-B 2) MandatedSignatureFormat: PAdES B-T 3) MandatedSignatureFormat: PAdES B-LT 4) MandatedSignatureFormat: PAdES B-LTA
(d)	**Targeted community**	None
(e)	**Allocation of responsibility for signature validation and augmentation**	None
(f)	**Legal type of signature**	APP constraints: • ConstraintsOnCertificateMetadata: LegalPersonSignerRequired: APP-defined: yes/no LegalPersonSignerAllowed: yes EUQualifiedCertificateRequired: APP-defined: yes/no EUSSCDRequired: APP-defined: yes/no EUAdESigRequired: yes
(g)	**Commitment assumed by the signatory**	APP constraints: • CommitmentTypesRequired: MandatedSignedQProperties-commitment-type-indication: APP-defined: yes/no
(h)	**Level of assurance on timing evidence**	None
(i)	**Formalities of validation**	APP constraints: • WYSIWHBSRequired: APP-defined: yes/no
(j)	**Longevity & resilience to change**	None
(k)	**Archival**	None
(l)	**Identity of signatories**	None
(m)	**Level of assurance required for the authentication of the signatory**	SVA constraints: • X509CertificateValidationConstraints:SetOfTrustAnchors: APP-defined[8] or EU Trusted List • RevocationConstraints:RevocationCheckingConstraints: eitherCheck: yes
(n)	**Signature creation devices**	None
(o)	**Other information to be associated with the signature**	None
(p)	**Cryptographic suites**	SVA constraints: • CryptographicSuitesConstraints: [30]
(q)	**Technological environment**	SVA constraints: • TechnologicalEnvironmentConstraints: [35] and [36]

[8] APP-defined requires a specific derived validation policy

The APP defines other parameters like specific (signed and unsigned) attributes and placement of a visible signature etc.

7.6.2. OUTPUT CONSTRAINTS TO BE USED WHEN VALIDATING SIGNATURES IN THE CONTEXT OF THE IDENTIFIED VALIDATION POLICY

No constraint

7.6.3. OUTPUT CONSTRAINTS TO BE USED FOR GENERATING/AUGMENTING SIGNATURES IN THE CONTEXT OF THE IDENTIFIED VALIDATION POLICY

No constraint

8. Annex B: Partially Delegated XAdES Validation Requirements

This section contains the specific requirements for **Partially Delegated XAdES** validation mode.

8.1. BSPs Mainly Related to the Concerned Application/Business Process

8.1.1. BSP (a): WORKFLOW (SEQUENCING AND TIMING) OF SIGNATURES

XAdES Manifest signatures cover serial signature use cases

8.1.2. BSP (b): DATA TO BE VALIDATED

The SD is a single XAdES Manifest signature with possible countersignatures. Other variants are not supported (cf. [18], [19], [20] and [21]).

8.1.3. BSP (c): THE RELATIONSHIP BETWEEN SIGNED DATA AND SIGNATURE(S)

In the context of the present policy, the signature is a XAdES Manifest signature as defined in [25] and [26].

8.1.4. BSP (d): TARGETED COMMUNITY

No further requirement beyond 3.1.4

8.1.5. BSP (e): ALLOCATION OF RESPONSIBILITY FOR SIGNATURE VALIDATION AND AUGMENTATION

No further requirement beyond 3.1.5

Note that the APP is responsible for validating that digest value contained in Manifest references match with the referenced documents as indicated in 3.1.5.

8.2. BSPs Mainly Influenced by the Legal/Regulatory Provisions Associated to the Concerned Application/Business Process

8.2.1. BSP (f): LEGAL TYPE OF THE SIGNATURES

No further requirement beyond 3.2.1

8.2.2. BSP (g): COMMITMENT ASSUMED BY THE SIGNATORY

No further requirement beyond 3.2.2

8.2.3. BSP (h): LEVEL OF ASSURANCE ON TIMING EVIDENCE

No further requirement beyond 3.2.3

8.2.4. BSP (i): FORMALITIES OF VALIDATION

The requirements of 3.2.4 apply.

When validating digest values in a Manifest, the APP needs to also respect possible constraints for input bytes transformations as indicated in 1.2.3, while this may imply for the current policy using XSLT, XPath or XQuery and other technologies that the business application would have to support for this purpose.

8.2.5. BSP (j): LONGEVITY AND RESILIENCE TO CHANGE

No further requirement beyond 3.2.5

Note that also access to SD is required for possible digest renewal during signature augmentation.

8.2.6. BSP (k): ARCHIVAL

No further requirement beyond 3.2.6

Note: APPs should ensure that detached signatures are archived together with the signed data.

8.3. BSPs Mainly Related to the Actors Involved in Creating/Augmenting/Validating Signatures

8.3.1. BSP (l): IDENTITY (AND ROLES/ATTRIBUTES) OF THE SIGNATORIES

No further requirement beyond 3.3.1

8.3.2. BSP (m): LEVEL OF ASSURANCE REQUIRED FOR THE AUTHENTICATION OF THE SIGNATORY

No further requirement beyond 3.3.2

8.3.3. BSP (n): SIGNATURE CREATION DEVICES

No further requirement beyond 3.3.3

8.4. Other BSPs

8.4.1. BSP (o): OTHER INFORMATION TO BE ASSOCIATED WITH THE SIGNATURE

No further requirement beyond 3.4.1

8.4.2. BSP (p): CRYPTOGRAPHIC SUITES

No further requirement beyond 3.4.2

8.4.3. BSP (q): TECHNOLOGICAL ENVIRONMENT

No further requirement beyond 3.4.3

8.5. Technical Counterparts of BSPs – Statement Summary

TABLE 8.1: VALIDATION POLICY STATEMENT SUMMARY

Name and identifier of the signature policy authority: LUXTRUST PKI (1.3.171.1)
Name and identifier of the signature policy: • AdES Minimum Legal Level ➔ LuxTrust Partially Delegated XAdES AdES Validation Policy (1.3.171.1.4.2.2.1) • QES Minimum Legal Level ➔ LuxTrust Partially Delegated XAdES QES Validation Policy (1.3.171.1.4.4.2.1)

BSP	BSP title	Business statement summary	Technical statement counterpart
(a)	**Workflow (sequencing & timing) of signatures**	Workflow is defined by the APP from among the following signature profiles: 1) basic signature 2) signature with time 3) signature with long-term validation material 4) signatures providing long-term availability and integrity of validation material	XML Manifest detached signatures Signature profiles specified in [22] and [28]
(b)	**Data to be validated (DTBS)**	Format: A single XAdES Manifest signature with possible countersignatures	Media types specified in [18], [19], [20] and [21]
(c)	**Relationship between DTBS & signature(s)**	XAdES Manifest signature format required Defined by the APP from among the following signature profiles: 1) basic signature 2) signature with time 3) signature with long-term validation material 4) signatures providing long-term availability and integrity of validation material	Signature format specified in [25] and [26] Signature profiles specified in [22] and [28]
(d)	**Targeted community**	Any entity that must be or that chooses to be compliant with the eIDAS Regulation	AdES Signature format and Member States trusted lists (cf. [2] and [31]), unless overridden by a custom policy
(e)	**Allocation of responsibility for signature validation and augmentation**	DTBS validated by LuxTrust and with responsibilities partly delegated to APP Augmentation to be performed by APP if required	Provisions made by APP when needed as indicated in 8.1.5 and 3.1.5
(f)	**Legal type of signature**	Upon successful validation, one of the following types: 4. Qualified electronic signatures; 5. Advanced electronic signatures supported by a qualified certificate; 6. Advanced electronic signatures	Parameters in the verify request (cf. [35], specifically validation policy OID)
(g)	**Commitment assumed by the signatory**	Attribute is detected when available	No interpretation performed by validation service
(h)	**Level of assurance on timing evidence**	Trusted and Qualified timestamps, validation time supplied by SVA, claimed signing time detected	Detected and verifiable elements; except for claimed signing time, used as POE; no further interpretation performed by validation service
(i)	**Formalities of validation**	No requirement beyond the general ones of 3.2.4, but APP is responsible for certain aspects as specified in 8.2.4; Signature policy identified detected when available and signature policy hash validated when applicable according available signature content	No signature policy interpretation performed by validation service

(j)	**Longevity & resilience to change**	Detection of maximum resilience according AdES profile of signature	Signature profiles specified in [22] and [28]
(k)	**Archival**	No requirement, however APP should keep SD together with archived signature	
(l)	**Identity of signatories**	No requirement	
(m)	**Level of assurance required for the authentication of the signatory**	No requirement besides eIDAS regarding applied policy; validation based on Member States trusted lists (cf. [2] and [31]), unless overridden by a custom policy	No interpretation performed by validation service besides detection of the underlying legal signature type
(n)	**Signature creation devices**	Implicit detection of QSCD in case of QES	No interpretation performed by validation service
(o)	**Other information to be associated with the signature**	No requirement	
(p)	**Cryptographic suites**	Cryptographic suites satisfying [30]	LuxTrust cryptographic libraries
(q)	**Technological environment**	LuxTrust s specifications (cf. [34], [35], [36], [37], [38] and [39])	LuxTrust implementation
Signature creation/validation application practices statements		-	-

The APP defines other parameters like the relevance of use of a container to package the signature together with signed data, the specific attributes (signed or unsigned) of the signature, etc.

8.6. Input and Output Constraints for Signature Creation, Augmentation and Validation Procedures

8.6.1. INPUT CONSTRAINTS TO BE USED WHEN GENERATING, AUGMENTING AND/OR VALIDATING SIGNATURES IN THE CONTEXT OF THE IDENTIFIED VALIDATION POLICY

TABLE 8.2: ADDITIONAL VALIDATION POLICY CONSTRAINTS

Name and identifier of the signature policy authority: LUXTRUST PKI (1.3.171.1)
Name and identifier of the signature policy: • AdES Minimum Legal Level ➔ LuxTrust Partially Delegated XAdES AdES Validation Policy (1.3.171.1.4.2.2.1) • QES Minimum Legal Level ➔ LuxTrust Partially Delegated XAdES QES Validation Policy (1.3.171.1.4.4.2.1)

BSP	BSP title	Constraint value at signature creation (SVA or APP)
(a)	**Workflow (sequencing & timing) of signatures**	SVA constraints: SequencingNature: • MandatedUnsignedQProperties-counter-signature • TimingRelevance: TimingRelevanceOnEvidence: 1) MandatedSignedQProperties-signing-time 2) MandatedUnsignedQProperties-signature-time-stamp 3) MandatedUnsignedQProperties-signature-time-stamp 4) MandatedUnsignedQProperties-signature-time-stamp and MandatedUnsignedQProperties-archival-form
(b)	**Data to be validated (DTBS)**	APP constraints: • DOTBSAsAWholeOrInParts: whole
(c)	**Relationship between DTBS & signature(s)**	APP constraints: • SignatureRelativePosition: detached 1) MandatedSignatureFormat: XAdES B-B 2) MandatedSignatureFormat: XAdES B-T 3) MandatedSignatureFormat: XAdES B-LT 4) MandatedSignatureFormat: XAdES B-LTA SVA Constraints: • SignatureRelativePosition: enveloping
(d)	**Targeted community**	None
(e)	**Allocation of responsibility for signature validation and augmentation**	None
(f)	**Legal type of signature**	APP constraints: • ConstraintsOnCertificateMetadata: LegalPersonSignerRequired: APP-defined: yes/no LegalPersonSignerAllowed: yes EUQualifiedCertificateRequired: APP-defined: yes/no EUSSCDRequired: APP-defined: yes/no EUAdESigRequired: yes
(g)	**Commitment assumed by the signatory**	APP constraints: • CommitmentTypesRequired: MandatedSignedQProperties-commitment-type-indication: APP-defined: yes/no
(h)	**Level of assurance on timing evidence**	None
(i)	**Formalities of validation**	APP constraints: • WYSIWHBSRequired: APP-defined: yes/no
(j)	**Longevity & resilience to change**	None
(k)	**Archival**	None
(l)	**Identity of signatories**	None
(m)	**Level of assurance required for the authentication of the signatory**	SVA constraints: • X509CertificateValidationConstraints:SetOfTrustAnchors: APP-defined[9] or EU Trusted List • RevocationConstraints:RevocationCheckingConstraints: eitherCheck: yes
(n)	**Signature creation devices**	None
(o)	**Other information to be associated with the signature**	None

[9] APP-defined requires a specific derived validation policy

BSP	BSP title	Constraint value at signature creation (SVA or APP)
(p)	**Cryptographic suites**	SVA constraints: • CryptographicSuitesConstraints: [30]
(q)	**Technological environment**	SVA constraints: • TechnologicalEnvironmentConstraints: [35] and [38]

The APP defines other parameters, like the relevance of use of a container to package the signature together with signed data, the specific attributes (signed or unsigned) of the signature, etc.

8.6.2. OUTPUT CONSTRAINTS TO BE USED WHEN VALIDATING SIGNATURES IN THE CONTEXT OF THE IDENTIFIED VALIDATION POLICY

No constraint

8.6.3. OUTPUT CONSTRAINTS TO BE USED FOR GENERATING/AUGMENTING SIGNATURES IN THE CONTEXT OF THE IDENTIFIED VALIDATION POLICY

No constraint

9. Annex C: Partially Delegated PAdES Validation Requirements

This section contains the specific requirements for **Partially Delegated PAdES** validation mode.

9.1. BSPs Mainly Related to the Concerned Application/Business Process

9.1.1. BSP (a): WORKFLOW (SEQUENCING AND TIMING) OF SIGNATURES

PAdES signatures are serial.

9.1.2. BSP (b): DATA TO BE VALIDATED

In the context of PAdES, the SD must be a PDF document, as defined in [14] and [15].

When the signature's level is B-B or B-T, the SD should be in PDF/A-1b or PDF/A-2b format (cf. [16] and [17]).

When the signature's level is B-LT or B-LTA, the SD should be in PDF/A-1a or PDF/A-2a format (cf. [16] and [17]).

9.1.3. BSP (c): THE RELATIONSHIP BETWEEN SIGNED DATA AND SIGNATURE(S)

In the context of the present policy, the signature is embedded within the signed PDF document, as defined in [23] and [24].

9.1.4. BSP (d): TARGETED COMMUNITY

No further requirement beyond 3.1.4

9.1.5. BSP (e): ALLOCATION OF RESPONSIBILITY FOR SIGNATURE VALIDATION AND AUGMENTATION

No further requirement beyond 3.1.5

Note that the APP is responsible for validating, whether the validated hashes of the SD signatures match with the re-calculated hashes of the corresponding SD byte ranges.

9.2. BSPs Mainly Influenced by the Legal/Regulatory Provisions Associated to the Concerned Application/Business Process

9.2.1. BSP (f): LEGAL TYPE OF THE SIGNATURES

No further requirement beyond 3.2.1

9.2.2. BSP (g): COMMITMENT ASSUMED BY THE SIGNATORY

No further requirement beyond 3.2.2

9.2.3. BSP (h): LEVEL OF ASSURANCE ON TIMING EVIDENCE

No further requirement beyond 3.2.3

9.2.4. BSP (i): FORMALITIES OF VALIDATION

The requirements of 3.2.4 apply.

The APP is also responsible for revealing additional signed metadata when contained in the SD and needed, as this cannot be detected by the validation service in the present validation mode.

9.2.5. BSP (j): LONGEVITY AND RESILIENCE TO CHANGE

No further requirement beyond 3.2.5

9.2.6. BSP (k): ARCHIVAL

No further requirement beyond 3.2.6

9.3. BSPs Mainly Related to the Actors Involved in Creating/Augmenting/Validating Signatures

9.3.1. BSP (l): IDENTITY (AND ROLES/ATTRIBUTES) OF THE SIGNATORIES

No further requirement beyond 3.3.1

9.3.2. BSP (m): LEVEL OF ASSURANCE REQUIRED FOR THE AUTHENTICATION OF THE SIGNATORY

No further requirement beyond 3.3.2

9.3.3. BSP (n): SIGNATURE CREATION DEVICES

No further requirement beyond 3.3.3

9.4. Other BSPs

9.4.1. BSP (o): OTHER INFORMATION TO BE ASSOCIATED WITH THE SIGNATURE

No further requirement beyond 3.4.1

9.4.2. BSP (p): CRYPTOGRAPHIC SUITES

No further requirement beyond 3.4.2

9.4.3. BSP (q): TECHNOLOGICAL ENVIRONMENT

No further requirement beyond 3.4.3

9.5. Technical Counterparts of BSPs – Statement Summary

TABLE 9.1: VALIDATION POLICY STATEMENT SUMMARY

Name and identifier of the signature policy authority: LUXTRUST PKI (1.3.171.1)
Name and identifier of the signature policy: • AdES Minimum Legal Level ➔ LuxTrust Partially Delegated PAdES AdES Validation Policy (1.3.171.1.4.2.3.1) • QES Minimum Legal Level ➔ LuxTrust Partially Delegated PAdES QES Validation Policy (1.3.171.1.4.4.3.1)

BSP	BSP title	Business statement summary	Technical statement counterpart
(a)	**Workflow (sequencing & timing) of signatures**	Workflow is defined by the APP from among the following signature profiles: 1) basic signature 2) signature with time 3) signature with long-term validation material 4) signatures providing long-term availability and integrity of validation material	PAdES signatures are serial Signature profiles specified in [22] and [28]
(b)	**Data to be validated (DTBS)**	Format: PDF	Media types specified in [14], [15], [16] and [17]
(c)	**Relationship between DTBS & signature(s)**	PAdES signature format required Defined by the APP from among the following signature profiles: 1) basic signature 2) signature with time 3) signature with long-term validation material 4) signatures providing long-term availability and integrity of validation material	PAdES signatures are enveloped Signature format specified in [23] and [24] Signature profiles specified in [22] and [28]
(d)	**Targeted community**	Any entity that must be or that chooses to be compliant with the eIDAS Regulation	AdES Signature format and Member States trusted lists (cf. [2] and [31]), unless overridden by a custom policy
(e)	**Allocation of responsibility for signature validation and augmentation**	DTBS validated by LuxTrust and with responsibilities partly delegated to APP Augmentation to be performed by APP, if required	Provisions made by APP when needed as indicated in 9.1.5 and 3.1.5
(f)	**Legal type of signature**	Upon successful validation, one of the following types: 1. Qualified electronic signatures; 2. Advanced electronic signatures supported by a qualified certificate; 3. Advanced electronic signatures	Parameters in the verify request (cf. [35], specifically validation policy OID)

BSP	BSP title	Business statement summary	Technical statement counterpart
(g)	**Commitment assumed by the Signatory**	Attribute is detected when available	No interpretation performed by validation service
(h)	**Level of assurance on timing evidence**	Trusted and Qualified timestamps, validation time supplied by SVA, claimed signing time detected	Detected and verifiable elements; except for claimed signing time, used as POE; no further interpretation performed by validation service
(i)	**Formalities of validation**	No requirement beyond the general ones of 3.2.4, but APP is responsible for certain aspects as specified in 9.2.4; Signature policy identified detected when available and signature policy hash validated when applicable according available signature content	No signature policy interpretation performed by validation service
(j)	**Longevity & resilience to change**	Detection of maximum resilience according AdES profile of signature	Signature profiles specified in [22] and [28]
(k)	**Archival**	No requirement	
(l)	**Identity of signatories**	No requirement	
(m)	**Level of assurance required for the authentication of the signatory**	No requirement besides eIDAS regarding applied policy; validation based on Member States trusted lists (cf. [2] and [31]), unless overridden by a custom policy	No interpretation performed by validation service besides detection of the underlying legal signature type
(n)	**Signature creation devices**	Implicit detection of QSCD in case of QES	No interpretation performed by validation service
(o)	**Other information to be associated with the signature**	No requirement	
(p)	**Cryptographic suites**	Cryptographic suites satisfying [30]	LuxTrust cryptographic libraries
(q)	**Technological environment**	LuxTrust s specifications (cf. [34], [35], [36], [37], [38] and [39])	LuxTrust implementation
Signature creation/validation application practices statements		-	-

The APP defines other parameters like specific (signed and unsigned) attributes and placement of a visible signature etc.

9.6. Input and Output Constraints for Signature Creation, Augmentation and Validation Procedures

9.6.1. INPUT CONSTRAINTS TO BE USED WHEN GENERATING, AUGMENTING AND/OR VALIDATING SIGNATURES IN THE CONTEXT OF THE IDENTIFIED

VALIDATION POLICY

TABLE 9.2: ADDITIONAL VALIDATION POLICY CONSTRAINTS

Name and identifier of the signature policy authority: LUXTRUST PKI (1.3.171.1)
Name and identifier of the signature policy: • AdES Minimum Legal Level ➔ LuxTrust Partially Delegated PAdES AdES Validation Policy (1.3.171.1.4.2.3.1) • QES Minimum Legal Level ➔ LuxTrust Partially Delegated PAdES QES Validation Policy (1.3.171.1.4.4.3.1)

BSP	BSP title	Constraint value at signature creation (SVA or APP)
(a)	Workflow (sequencing & timing)	SVA constraints: • SequencingNature: Mandated-serial • TimingRelevance: TimingRelevanceOnEvidence: 1) MandatedSignedQProperties-signing-time 2) MandatedUnsignedQProperties-signature-time-stamp 3) MandatedUnsignedQProperties-signature-time-stamp 4) MandatedUnsignedQProperties-signature-time-stamp and MandatedUnsignedQProperties-archival-form
(b)	Data to be validated	APP constraints: • ConstraintOnDTBS: PDF • DOTBSAsAWholeOrInParts: whole
(c)	The relationship between signed data and signature(s)	APP constraints: • ConstraintsOnTheNumberOfDOTBS=1 • SignatureRelativePosition: enveloped 1) MandatedSignatureFormat: PAdES B-B 2) MandatedSignatureFormat: PAdES B-T 3) MandatedSignatureFormat: PAdES B-LT 4) MandatedSignatureFormat: PAdES B-LTA
(d)	Targeted community	None
(e)	Allocation of responsibility for signature validation and augmentation	None
(f)	Legal type of the signatures	APP constraints: • ConstraintsOnCertificateMetadata: LegalPersonSignerRequired: APP-defined: yes/no LegalPersonSignerAllowed: yes EUQualifiedCertificateRequired: APP-defined: yes/no EUSSCDRequired: APP-defined: yes/no EUAdESigRequired: yes
(g)	Commitment assumed by the signatory	APP constraints: • CommitmentTypesRequired: MandatedSignedQProperties-commitment-type-indication: APP-defined: yes/no
(h)	Level of assurance on timing evidence	None
(i)	Formalities of validation	APP constraints: • WYSIWHBSRequired: APP-defined: yes/no
(j)	Longevity and resilience to change	None
(k)	Archival	None
(l)	Identity (and roles/attributes) of the signatories	None
(m)	Level of assurance required for the authentication of the signatory	SVA constraints: • X509CertificateValidationConstraints:SetOfTrustAnchors: APP-defined[10] or EU Trusted List • RevocationConstraints:RevocationCheckingConstraints: eitherCheck: yes

[10] APP-defined requires a specific derived validation policy

BSP	BSP title	Constraint value at signature creation (SVA or APP)
(n)	Signature creation devices	None
(o)	Other information to be associated with the signature	None
(p)	Cryptographic suites	SVA constraints: • CryptographicSuitesConstraints: [30]
(q)	Technological environment	SVA constraints: • TechnologicalEnvironmentConstraints: [35] and [37]

The APP defines other parameters like specific (signed and unsigned) attributes and placement of a visible signature etc.

9.6.2. OUTPUT CONSTRAINTS TO BE USED WHEN VALIDATING SIGNATURES IN THE CONTEXT OF THE IDENTIFIED VALIDATION POLICY

No constraint

9.6.3. OUTPUT CONSTRAINTS TO BE USED FOR GENERATING/AUGMENTING SIGNATURES IN THE CONTEXT OF THE IDENTIFIED VALIDATION POLICY

No constraint

10. Annex D: Fully Delegated XAdES Validation Requirements

This section contains the specific requirements for **Fully Delegated XAdES** validation mode.

10.1. BSPs Mainly Related to the Concerned Application/Business Process

10.1.1. BSP (a): WORKFLOW (SEQUENCING AND TIMING) OF SIGNATURES

XAdES enveloped signatures cover serial signature use cases.

10.1.2. BSP (b): DATA TO BE VALIDATED

The SD is a single XAdES enveloped signature with possible countersignatures. Other variants are not supported (cf. [18], [19], [20] and [21]).

10.1.3. BSP (c): THE RELATIONSHIP BETWEEN SIGNED DATA AND SIGNATURE(S)

In the context of the present policy, the signature is a XAdES enveloped signature as defined in [25] and [26].

10.1.4. BSP (d): TARGETED COMMUNITY

No further requirement beyond 3.1.4

10.1.5. BSP (e): ALLOCATION OF RESPONSIBILITY FOR SIGNATURE VALIDATION AND AUGMENTATION

No further requirement beyond 3.1.5

10.2. BSPs Mainly Influenced by the Legal/Regulatory Provisions Associated to the Concerned Application/Business Process

10.2.1. BSP (f): LEGAL TYPE OF THE SIGNATURES

No further requirement beyond 3.2.1

10.2.2. BSP (g): COMMITMENT ASSUMED BY THE SIGNATORY

No further requirement beyond 3.2.2

10.2.3. BSP (h): LEVEL OF ASSURANCE ON TIMING EVIDENCE

No further requirement beyond 3.2.3

10.2.4. BSP (i): FORMALITIES OF VALIDATION

No further requirement beyond 3.2.4

10.2.5. BSP (j): LONGEVITY AND RESILIENCE TO CHANGE

No further requirement beyond 3.2.5

10.2.6. BSP (k): ARCHIVAL

No further requirement beyond 3.2.6

10.3. BSPs Mainly Related to the Actors Involved in Creating/Augmenting/Validating Signatures

10.3.1. BSP (l): IDENTITY (AND ROLES/ATTRIBUTES) OF THE SIGNATORIES

No further requirement beyond 3.3.1

10.3.2. BSP (m): LEVEL OF ASSURANCE REQUIRED FOR THE AUTHENTICATION OF THE SIGNATORY

No further requirement beyond 3.3.2

10.3.3. BSP (n): SIGNATURE CREATION DEVICES

No further requirement beyond 3.3.3

10.4. Other BSPs

10.4.1. BSP (o): OTHER INFORMATION TO BE ASSOCIATED WITH THE SIGNATURE

No further requirement beyond 3.4.1

10.4.2. BSP (p): CRYPTOGRAPHIC SUITES

No further requirement beyond 3.4.2

10.4.3. BSP (q): TECHNOLOGICAL ENVIRONMENT

No further requirement beyond 3.4.3

10.5. Technical Counterparts of BSPs – Statement Summary

TABLE 10.1: VALIDATION POLICY STATEMENT SUMMARY

Name and identifier of the signature policy authority: LUXTRUST PKI (1.3.171.1)
Name and identifier of the signature policy: • AdES Minimum Legal Level ➔ LuxTrust Fully Delegated XAdES AdES Validation Policy (1.3.171.1.4.2.4.1) • QES Minimum Legal Level ➔ LuxTrust Fully Delegated XAdES QES Validation Policy (1.3.171.1.4.4.4.1)

BSP	BSP title	Business statement summary	Technical statement counterpart
(a)	**Workflow (sequencing & timing) of signatures**	Workflow is defined by the APP from among the following signature profiles: 1) basic signature 2) signature with time 3) signature with long-term validation material 4) signatures providing long-term availability and integrity of validation material	XML enveloped signatures Signature profiles specified in [22] and [28]
(b)	**Data to be validated (DTBS)**	Format: A single XML document containing a possibly countersigned enveloped XAdES signatures	Media types specified in [18], [19], [20] and [21]
(c)	**Relationship between DTBS & signature(s)**	XAdES enveloped signature format required Defined by the APP from among the following signature profiles: 1) basic signature 2) signature with time 3) signature with long-term validation material 4) signatures providing long-term availability and integrity of validation material	Signature format specified in [25] and [26] Signature profiles specified in [22] and [28]
(d)	**Targeted community**	Any entity that must be or that chooses to be compliant with the eIDAS Regulation	AdES Signature format and Member States trusted lists (cf. [2] and [31]), unless overridden by a custom policy
(e)	**Allocation of responsibility for signature validation and augmentation**	DTBS validated by LuxTrust Augmentation to be performed by APP if required	Provisions made by APP when needed as indicated in 10.1.5 and 3.1.5
(f)	**Legal type of signature**	Upon successful validation, one of the following types: 4. Qualified electronic signatures; 5. Advanced electronic signatures supported by a qualified certificate; 6. Advanced electronic signatures	Parameters in the verify request (cf. [35], specifically validation policy OID)
(g)	**Commitment assumed by the signatory**	Attribute is detected when available	No interpretation performed by validation service
(h)	**Level of assurance on timing evidence**	Trusted and Qualified timestamps, validation time supplied by SVA, claimed signing time detected	Detected and verifiable elements; except for claimed signing time, used as POE; no further interpretation performed by validation service
(i)	**Formalities of validation**	No requirement beyond the general ones of 3.2.4; Signature policy identified detected when available and signature policy hash validated when applicable according available signature content	No signature policy interpretation performed by validation service
(j)	**Longevity & resilience to change**	Detection of maximum resilience according AdES profile of signature	Signature profiles specified in [22] and [28]
(k)	**Archival**	No requirement	
(l)	**Identity of signatories**	No requirement	

(m)	**Level of assurance required for the authentication of the signatory**	No requirement besides eIDAS regarding applied policy; validation based on Member States trusted lists (cf. [2] and [31]), unless overridden by a custom policy	No interpretation performed by validation service besides detection of the underlying legal signature type
(n)	**Signature creation devices**	Implicit detection of QSCD in case of QES	No interpretation performed by validation service
(o)	**Other information to be associated with the signature**	No requirement	
(p)	**Cryptographic suites**	Cryptographic suites satisfying [30]	LuxTrust cryptographic libraries
(q)	**Technological environment**	LuxTrust s specifications (cf. [34], [35], [36], [37], [38] and [39])	LuxTrust implementation
Signature creation/validation application practices statements		-	-

The APP defines other parameters like specific (signed and unsigned) attributes etc.

10.6. Input and Output Constraints for Signature Creation, Augmentation and Validation Procedures

10.6.1. INPUT CONSTRAINTS TO BE USED WHEN GENERATING, AUGMENTING AND/OR VALIDATING SIGNATURES IN THE CONTEXT OF THE IDENTIFIED VALIDATION POLICY

TABLE 10.2: ADDITIONAL VALIDATION POLICY CONSTRAINTS

Name and identifier of the signature policy authority: LUXTRUST PKI (1.3.171.1)
Name and identifier of the signature policy: • AdES Minimum Legal Level ➔ LuxTrust Fully Delegated XAdES AdES Validation Policy (1.3.171.1.4.2.4.1) • QES Minimum Legal Level ➔ LuxTrust Fully Delegated XAdES QES Validation Policy (1.3.171.1.4.4.4.1)

BSP	BSP title	Constraint value at signature creation (SVA or APP)
(a)	Workflow (sequencing & timing)	SVA constraints: SequencingNature: • MandatedUnsignedQProperties-counter-signature • TimingRelevance: TimingRelevanceOnEvidence: 1) MandatedSignedQProperties-signing-time 2) MandatedUnsignedQProperties-signature-time-stamp 3) MandatedUnsignedQProperties-signature-time-stamp 4) MandatedUnsignedQProperties-signature-time-stamp and MandatedUnsignedQProperties-archival-form
(b)	Data to be validated	APP constraints: • ConstraintOnDTBS: XML • DOTBSAsAWholeOrInParts: whole
(c)	The relationship between signed data and signature(s)	APP constraints: • SignatureRelativePosition: enveloped 1) MandatedSignatureFormat: XAdES B-B 2) MandatedSignatureFormat: XAdES B-T 3) MandatedSignatureFormat: XAdES B-LT 4) MandatedSignatureFormat: XAdES B-LTA
(d)	Targeted community	None

BSP	BSP title	Constraint value at signature creation (SVA or APP)
(e)	Allocation of responsibility for signature validation and augmentation	None
(f)	Legal type of the signatures	APP constraints: • ConstraintsOnCertificateMetadata: LegalPersonSignerRequired: APP-defined: yes/no LegalPersonSignerAllowed: yes EUQualifiedCertificateRequired: APP-defined: yes/no EUSSCDRequired: APP-defined: yes/no EUAdESigRequired: yes
(g)	Commitment assumed by the signatory	APP constraints: • CommitmentTypesRequired: MandatedSignedQProperties-commitment-type-indication: APP-defined: yes/no
(h)	Level of assurance on timing evidence	None
(i)	Formalities of validation	APP constraints: • WYSIWHBSRequired: APP-defined: yes/no
(j)	Longevity and resilience to change	None
(k)	Archival	None
(l)	Identity (and roles/attributes) of the signatories	None
(m)	Level of assurance required for the authentication of the signatory	SVA constraints: • X509CertificateValidationConstraints:SetOfTrustAnchors: APP-defined[11] or EU Trusted List • RevocationConstraints:RevocationCheckingConstraints: eitherCheck: yes
(n)	Signature creation devices	None
(o)	Other information to be associated with the signature	None
(p)	Cryptographic suites	SVA constraints: • CryptographicSuitesConstraints: [30]
(q)	Technological environment	SVA constraints: • TechnologicalEnvironmentConstraints: [35] and [39]

The APP defines other parameters, like the relevance of use of a container to package the signature together with signed data, the specific attributes (signed or unsigned) of the signature, etc.

10.6.2. OUTPUT CONSTRAINTS TO BE USED WHEN VALIDATING SIGNATURES IN THE CONTEXT OF THE IDENTIFIED VALIDATION POLICY

No constraint

10.6.3. OUTPUT CONSTRAINTS TO BE USED FOR GENERATING/AUGMENTING SIGNATURES IN THE CONTEXT OF THE IDENTIFIED VALIDATION POLICY

No constraint

[11] APP-defined requires a specific derived validation policy