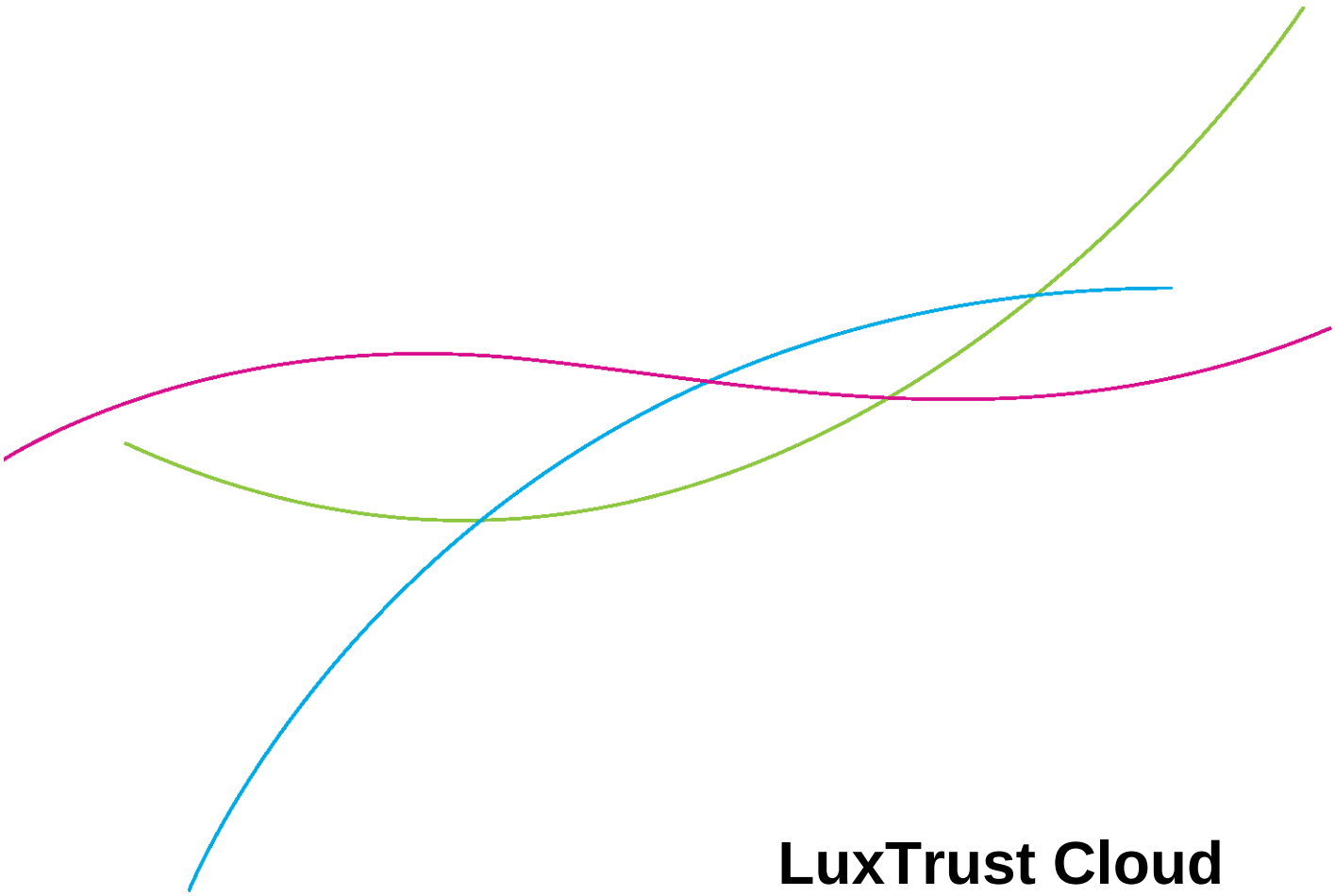

LuxTrust Cloud Signature Policies

Document reference:
LT-2015-09-06-02-R-E

Date issued:
2018-03-22

Version: 1.1.4

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
0.1	08/2015	First Draft
0.2	09/2015	First Review
0.25	09/2015	Second version (per-format appendix)
0.26	09/2015	Minor changes and clarifications
0.9	09/2015	Pre-final version with Fully Delegated PAdES policy
1.0	09/2015	Proof-reading
1.1.0	10/2015	Partially Delegated XAdES policy
1.1.1	03/2016	Partially Delegated PAdES policy
1.1.2	05/2016	Minor corrections and clarification concerning signing formalities
1.1.3	11/2016	Integration of amended changes concerning shared responsibilities – new definition
1.1.4	03/2018	Extension for seal services

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] Regulation 1502/2015/EU – Minimum technical specifications and procedures for assurance levels, September 2015
http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R1502&from=EN

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

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

[5] 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

[6] 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

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

[8] 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

[9] 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

[10] 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

[11] 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

[12] 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

[13] 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

[14] 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

[15] ETSI TS 119 312 – Electronic Signatures and Infrastructures (ESI);Cryptographic suites, May 2017
http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.02.01_60/ts_119312v010201p.pdf

[16] 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

[17] LuxTrust Time Stamping V2 Policy, v1.9, July 2017
https://www.luxtrust.lu/upload/data/repository/luxtrust_time_stamping_v2_policy_v1_9.pdf

[18] LuxTrust ORELY Portal – SAML Specifications, v1.0.5 or higher, April 2016

[19] LuxTrust ORELY Portal – Proprietary Attributes Definitions, v1.0.2 or higher, July 2016

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

[21] LuxTrust Cloud Signature Services – Generic DSS Specifications, v1.2.4 or higher, Mars 2018

[22] LuxTrust Cloud Signature Services – Fully Delegated PAdES, v1.2.4 or higher, Mars 2018

[23] LuxTrust Cloud Signature Services – Partially Delegated PAdES, v1.2.4 or higher, Mars 2018

[24] LuxTrust Cloud Signature Services – Partially Delegated XAdES, v1.2.4 or higher, Mars 2018

Table of Contents

1. Introduction

1.1. Overview

The current document presents the policies for LuxTrust advanced signature and seal services (cf. [1]) provided via the ORELY and BLINK portals.

- ORELY is a central authentication and signature service portal used by application providers (APPs) for enabling physical person users (Signatories) for interactively creating electronic signatures or seals of documents after successfully having been authenticated with a suitable level of assurance (cf. [2]), and for interactively verifying electronic signatures or seals of documents. Depending on the certificate profile employed by the signatory, a physical person user of ORELY may also act on behalf of a legal person. ORELY workflows always require the presence of a physical person user, which becomes evident by the ORELY access protocol design that uses user redirection between APP and the portal as a key paradigm (cf. Figure 1).

- BLINK is another central portal used by APPs for automatically creating electronic seals or signatures of documents after successful authentication with a suitable level of assurance (cf. [2]). The portal is also employed for automatically verifying or extending electronic seals or signatures of documents. No physical person user is directly involved in BLINK workflows. BLINK workflows are completely automated, which means that its access protocol is designed for consumption of services by unattended applications (server machines). Nevertheless, physical person users might be involved when indirectly dealing with the services via the APP applications (cf. Figure 2).

ORELY and BLINK are complementary trust portals, with the former being designated for interactive use and the latter being designated for automatic use by APPs. ORELY offers SAML over HTTPS on the transport layer, while BLINK exposes restful web services over HTTPS. By contrast, both portals use the same protocol on the application layer, i.e. DSS, in order to provide the same overall experience for service integrators (cf. [18], [19], [20], [21], [22], [23] and [24] for further technical details).

By using those portals, all generic use cases consisting of any combination of interactive or automated advanced electronic signature or seal creation, validation and/or augmentation can be covered, if the required services have been technically made available and integrated by the APP.

LuxTrust configures ORELY and BLINK in accordance with each APP. Consequently, a specific service profile is in effect for the signatories of a given application. Nevertheless, profile settings can be overwritten by specific request parameters. APPs must establish a contractual relationship and a service agreement with LuxTrust prior to consume signature and seal services for making them available to physical and/or legal person end-users. In particular, an APP can also be the legal person user of the covenanted service.

Note that any physical or legal person signatory also requires a private key and a corresponding certificate for signing, which necessitates a suitable complementary contractual agreement between the signatory and LuxTrust.

Although electronic signatures and electronic seals differ regarding their legal effect (cf. [1]), they are largely similar with regard to the employed technical standards and the underlying cryptographic aspects. Therefore, regardless of their specific legal nature, the present document uses the unspecific term *signature service* when referring to advanced electronic signature and/or seal creation, validation and augmentation services, which are provided via nay of the LuxTrust portals. Specific terms are only applied when an explicit distinction between an electronic signature and an electronic seal becomes necessary.

Similarly, the present document uniformly employs the neutral term *portal* when referring to ORELY or BLINK, unless an explicit distinction between the two becomes necessary.

Due to the fact that signature processes widely differ from each other with regard to the signature format and the implied operation mode options (cf. 3.2.4) for arranging responsibilities between an APP and LuxTrust, the present document defines a dedicated base signature policy for each offered mode.

A signature policy specifies the rules and constraints that determine the overall process for all involved stakeholders. It is associated with a globally unique object identifier.

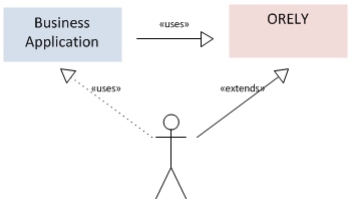

FIGURE 1: ORELY USAGE SCENARIO

FIGURE 2: BLINK USAGE SCENARIO

1.2. Business or Application Domain

1.2.1. SCOPE AND BOUNDARIES OF SIGNATURE POLICY

The signature policies specified in the present document are suitable for a large scope of application and business domains, with various levels of authentication, whenever there is a need for advanced electronic signatures or seals.

An APP is responsible for the technical integration of LuxTrust cloud signature services into its application workflow(s).

- In the case of ORELY, the APP is also responsible for management and implementation of interactions with the signatory through a web browser or through an alternative graphical user interface due to the underlying protocol design requiring user redirection between the application and service portal.

- In the case of BLINK, end users are not directly involved in the exchanges between the application and the service portal, so that the previous obligation becomes obsolete in this particular context.

The present policy document defines two kinds of requirements: explicit and well-defined requirements regarding the actors (Signatory, LuxTrust, APP), and additional requirements concerning complementary APP signature policy content for covering a specific APP use case.

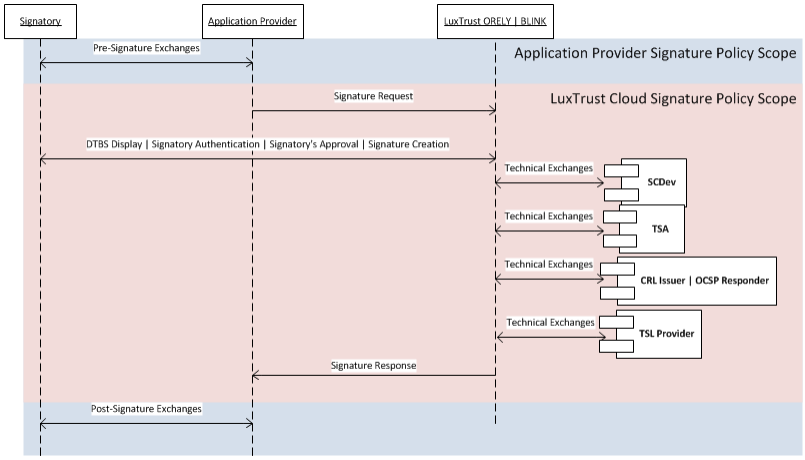

FIGURE 3: SIGNATURE POLICY SCOPE

An APP sticking to the present signature policy shall derive its specific rules from the present policy, as shown in the blue area (cf. Figure 3).

In the Partially Delegated mode, the APP can even consider more responsibilities than in the Fully Delegated mode (e.g. DTBS presentation or SDO formatting) which then results in a modified diagram regarding **Error! Reference source not found.** (cf. 1.2.3).

Due to the absence of a graphical user interface in the case of the BLINK portal, the APP must in that context make provisions for DTBS and signature attribute presentation when needed.

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 signature policies, signature generation takes place within the context of the signature flow specified by LuxTrust, through a sequence of messages exchanged between the APP, the signatory and the LuxTrust portal. The transport layer protocol is specified in [18], [19] for ORELY and in [20] for BLINK; the common application layer protocol is specified in [21] and either [22] or [23] or [24] depending on the signed object type in use:

1. The APP sends a sign request to the LuxTrust portal containing the document to be signed or one or more hashes of document[s] to be signed and complementary transactional parameters (cf. [21])

2. In the case of

   2.1. ORELY, the portal interacts with the signatory for authentication and signature creation and optional augmentation or validation

      2.1.1. Either independently of APP's interface ("fully delegated mode", cf. 3.2.4)

      2.1.2. Or through APP's interface ("partially delegated mode"),

   2.2. BLINK, the signatory is required to provide authentication credentials through APPs interface, with the latter also covering presentation of DTBS and signature attributes as needed. The portal does not directly interact with the signatory when processing a request.

   Each mode implies specific requirements.

3. LuxTrust portal sends a signature response which contains the signed document or one or more signed hashes, unless an error has occurred to the APP.

In this respect, LuxTrust signature services operate independently of APP's signature context.

1.3. Document and Policy Names, Identification and Conformance Rules

1.3.1. SIGNATURE POLICY DOCUMENT AND SIGNATURE POLICY NAMES

The signature policies covered by the current document are ***LuxTrust Cloud Signature Policies*** with specific annexes for supported AdES formats and profiles.

1.3.2. SIGNATURE POLICY DOCUMENT AND SIGNATURE POLICY IDENTIFIERS

Signature policy name	Signature policy OID
LuxTrust Fully Delegated PAdES Signature Policy	1.3.171.1.4.1.1.2
LuxTrust Partially Delegated XAdES Signature Policy	1.3.171.1.4.1.2.2
LuxTrust Partially Delegated PAdES Signature Policy	1.3.171.1.4.1.3.2

1.3.3. CONFORMANCE RULES

Electronic signatures produced under the present signature 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 is conformant with [14].

1.3.4. DISTRIBUTION POINTS

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

1.4. Signature Policy Document Administration

1.4.1. SIGNATURE POLICY AUTHORITY

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

1.4.2. CONTACT ADDRESS

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

Email: cspboard@luxtrust.lu

Phone: +352 2668 151

1.4.3. APPROVAL PROCEDURES

The Policy Approval Authority within LuxTrust S.A. is the LuxTrust CSP Board. LuxTrust announces modifications of the published Signature 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 Comprises the SD and additional attributes for being signed
DTBSF	Data to Be Signed Formatted Components of the DTBS, formatted and put in the correct sequence for the chosen SDO type
DTBSR	Data to Be Signed Representation Data sent by the SCA to the SCDev for signing, usually a cryptographic hash of the DTBSF
PAdES	PDF Advanced Electronic Signature
PDF	Portable Document Format
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 Document selected for signing
SDO	Signed Data Object Result of the SCA process after integrating of the signed DTBSR regarding the respective SDO type
SDO type	Format of the SDO An interoperable advanced electronic signature standard; cf. [9], [10], [11] and [12]
Signatory	The physical or legal person which creates an advanced electronic signature
SP	Service provider Alternative name for an APP
SVA	Signature Validation Application
TSA	Time-Stamping Authority
TSL	Trust-Service Status List
TSP	Trust Service Portal
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, OCSP responses or CRLs

2. Signature Application Practices Statements

2.1. Requirements for Application Provider Applications

According to the Signature creation model of [8], APP's application is the DA, that is, an "application that uses a signature creation system to create a signature". As such, APP's application must conform to technical standards [18] and [19] or [20], [21] and, depending on the signed object type in use, [22], [23] or [24]. 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 signature service and the signatory
- it must not tamper with LuxTrust client-side software components
- it must securely maintain logs to ensure the imputability of transactions between its application, the LuxTrust signature service and the signatory

When working in “partially delegated mode” (3.2.4), the APP directly contributes to the implementation of the signature service. Its interface must additionally satisfy the requirements specified in [13].

2.2. Requirements for the Signature Creation/Verification Application

When applicable, i.e. when integrating a web interface, DA, SCA and SVA development should follow the “OWASP Best Practices”.

For signature creation and validation, the relevant requirements from [13] are applicable.

3. Business Scoping Parameters

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

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

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

Description of the *working mode* between LuxTrust and the APP is contained in "BSP (i): Formalities of Signing".

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

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

The present signature policy addresses creation of a single advanced electronic signature comprising possible timestamp and proof-data extensions regarding a single instance or multiple DTBS instances at the same time. A DTBS can consist of any binary data that may specifically represent a PDF document, any other document, or alternatively contain one or more document hashes.

LuxTrust cloud signature services can be used to implement business workflows with multiple signatures; in such a case, each single signature within the APP workflow will be produced using a dedicated signature transaction according to the present policy. The APP signature policy shall in that case describe the workflow managing the individual signature transactions.

The present signature policy also addresses verification and augmentation of multiple advanced signatures associated with a signed data object during a single transaction[1].

3.1.2. BSP (b): DATA TO BE SIGNED

The APP is responsible for the contents and the correct formatting of the DTBS with respect to applicable standards. In particular, it must ensure that the DTBS does not contain malicious code or data that could mislead the signatory, alter the DTBS visual presentation or damage LuxTrust signature services.

[1] Note that technical availability of individual signature service features depends on the actual implementation status of the LuxTrust portals (cf. [18], [19], [20], [21], [22], [23] and [24] for further technical details).

The DTBS format can be PDF (Annex A: Fully Delegated PAdES Signature Requirements or Annex C: Partially Delegated PAdES Signature Requirements) or any generic document format (particularly XML) (Annex B: Partially Delegated XAdES Signature Requirements).

LuxTrust cloud signature services guarantee the confidentiality of the DTBS according to applicable laws on privacy and Luxembourg laws regarding the financial sector. LuxTrust particularly erases all copies of received documents, if any, from its servers instantly after having performed the corresponding signature transaction.

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

The relationship between signed data and signature(s) depends on the signature's format.

The supported signature levels (from [8]) are:

1. B-B (basic signature)
2. B-T (signature with time)
3. B-LT (signature with long-term validation material)
4. Not supported via ORELY: B-LTA (Signatures providing long-term availability and integrity of validation material)

In all cases, the signature-policy-identifier and commitment-type-indication fields must be present.

3.1.4. BSP (d): TARGETED COMMUNITY

Unless otherwise specified within the APP signature policy, signatures produced by LuxTrust cloud signature services shall be validated based on the European trusted lists [16]. Signatures that are created by LuxTrust cloud signature services comply with the eIDAS Regulation [1].

In accordance with LuxTrust, APPs may define particular "trust anchors" in their signature policy or exclude individual "trust anchors" as needed in order to use a corresponding configuration during certificate path validations. In such a case, LuxTrust cannot be held responsible for acceptance or rejection of generated signatures by third parties/software that cannot support such a configuration or be aware of it.

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

LuxTrust cloud signature services timestamp signatures according to the request profile (B-T, B-LT or B-LTA when supported); section 3.2.3 provides details concerning timestamping of the signatures.

Regarding B-LT signatures, LuxTrust signature services augment the initial signature following its creation when the corresponding signature level is explicitly requested (which is the original default).

When in "fully delegated mode" (cf. 3.2.4), the LuxTrust ORELY portal automatically validates existing signatures on the DTBS. Should the DTBS contain an invalid signature, that information

is indicated to the signatory. LuxTrust ORELY will not abort the signature process due to an invalid signature being contained in the DTBS.

This also applies to "partially delegated mode" (cf. 3.2.4); however, validation performed by LuxTrust ORELY does not cover the aspect of whether a presented document is equal in content to the signed data (cf. 3.2.4 for details). This latter aspect must be guaranteed by the APP in order to ensure an appropriate and complete validation for particularly a detached DTBS.

If the APP workflow requires pre-existing signatures to be validated, the constraint has to be enforced by the APP before calling LuxTrust signature creation services.

This latter constraint particularly applies to use of the BLINK portal, which neither exposes a graphical user interface, nor directly integrates a physical person user in the signature workflow. Consequently, those responsibilities are completely delegated to the APP when consuming signature services provided via that particular portal.

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

LuxTrust cloud signature services support all legal types of advanced electronic signature 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 and seals;
2. Advanced electronic signatures and seals supported by a qualified certificate;
3. Advanced electronic signatures and seals

Advanced electronic signatures and seals are[2]

(a) Uniquely linked to the signatory;

(b) Capable of identifying the signatory;

(c) Created using electronic signature or seal 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.

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

The APP shall define the actual legal signature type in its signature policy and process. Technically, the APP shall specify the minimum or exact legal level in the sign request to LuxTrust cloud signature services (cf. the *SignatureQAA* parameter in [21]).

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

The APP, depending on its use case, defines the commitment type for signature or seal creation; technically, the APP may specify the commitment type associated to the signature in the sign request sent to LuxTrust cloud signature services.

If the APP specifies no commitment, the default value is ***proof of approval***.

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

The TSP provides a signature timestamp by default or when explicitly requested, thus augmenting the signature to at least B-T. Timestamping is provided by the LuxTrust Qualified Timestamping Authority (cf. [17]) with the production policy being in force regarding signature or seal creation in production.

Otherwise, the B-B signature level contains the claimed [UTC] signing time of the signature [8].

3.2.4. BSP (i): FORMALITIES OF SIGNING

Presentation of the DTBS to the signatory is mandatory for creating an advanced electronic signature. It is optional for creating an advanced electronic seal if the APP workflow can ensure authenticity of the DTBS by other means, in particular by employing suitable controls and security measures regarding provision of the DTBS including its content.

In addition, the signatory must be able to access the signature attributes on his/her own discretion during signing, unless attributes are determined by a predefined setting that is known to the signatory by out-of-band means.

The following rules apply regarding the underlying operation mode (cf. 1.2.3) and to the respective portal in use:

1. When using the BLINK portal, the APP software shall enable the signatory to inspect the DTBS or, in the case seal creation, guarantee its authenticity by other means. The APP software shall enable the signatory to access the signature attributes before the start of the signature creation process, unless attributes are known due to using a predefined setting.

2. When using the ORELY portal,

    2.1. In ***Partially Delegated Mode***, the APP software shall enable the signatory to inspect the DTBS, and the LuxTrust portal shall make the attributes of the signature accessible to the signatory before the start of the signature creation process.

    Alternatively, this latter requirement may be addressed by the APP by using a tailored presentation layer. In this case, the APP is responsible for fully addressing above-cited transparency requirements concerning the presentation layer and unobstructed access to the signature attributes. In any event, APP shall guarantee that

    - The presented document shall be equal in content to the data that is signed [8],

- The user interface conforms to [8] and [13].

2.2. In ***Fully Delegated Mode***, the LuxTrust portal shall allow the signatory to inspect the DTBS and make signature attributes accessible to the signatory before the start of the LuxTrust ORELY signature process. The APP shall guarantee that its implementation and its technical integration of the LuxTrust services do not tamper with the LuxTrust DTBS presentation and with the access of the signatory to the signature attributes.

All the following signature attributes must be accessible for inspection by the signatory during the process, or known by out-of-band means:

- Signing certificate
- Signature policy identifier
- Commitment type

Additionally when using the ORELY portal, existing signatures on the DTBS and their validation status must be accessible for inspection by the signatory during the process, with validation performed by the LuxTrust implementation. As an alternative to the validation performed by LuxTrust ORELY, the APP may perform this validation independently. In this case, the APP becomes solely responsible for validation.

The user interface focuses on the signatory's authentication and legal requirements for expression of will by the signatory when his/her approval is required. The fulfilment of any business-specific requirements originating from the APP workflow remains under APP's responsibility.

In all cases, the APP shall give the signatory access to the signed document.

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

The expected longevity of the electronic signature depends on its level.

- B-B signature: the signature’s longevity is that of the signing certificate at the time of the signature.
- B-T signature: the signature’s longevity is that of the timestamp, delivered by LuxTrust Qualified Timestamping Authority (cf. [17]) with the production policy being in force regarding signature or seal creation in production. Such a timestamp is valid for a period of at most 5 (five) years, and no less than 4 (four) years.
- B-LT signature: the signature’s longevity is that of the above-cited B-T signature. It is augmented by proof elements added for the contained signatures.
- B-LTA signature: the signature’s longevity is that of the above-cited B-LT signature. It is (possibly repeatedly) augmented with an additional document/archive timestamp and corresponding proof elements. Alternatively, a centralized electronic signature preservation service may be employed to ensure an equivalent period of longevity.

In any case, the cryptographic algorithms and parameters are chosen in order to ensure that the electronic signature’s resilience can be maintained (at least) for the duration of its longevity.

3.2.6. BSP (k): ARCHIVING

The present policy has no archiving requirement regarding the generated advanced electronic signatures. LuxTrust does not keep a copy of either the signed documents or the generated advanced electronic 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. The goal of an advanced electronic signature is to be self-contained and 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.

Nevertheless, LuxTrust cloud signature services transaction logs are backed up in order to provide evidence concerning the supplied service, archived for 10 (ten) years and accessible for use during legal proceedings.

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

- The message digest of the formatted data to be signed, including all signed properties
- The digital signature of this message digest
- The NTP-synchronized creation time of the log record in question
- The identifier of the requesting APP
- The unique subject serial number of the employed signatory certificate enabling identification thereof
- Status of the signatory certificate at signing time
- 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 may provide LuxTrust signature services with the signatory's identity and minimum assurance level corresponding to the authentication means (cf. 3.3.2) regarding a sign request (cf. [21]).

The present signature policy contains no requirement concerning the signatory's role. When specific constraints are required by the business use case (signature delegation, access rights, 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.

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

The APP may provide LuxTrust signature services with the minimum assurance level regarding the means the signatory may use to authenticate himself/herself (cf. the *MinQAA* parameter in

[19]). This enables LuxTrust signature services to support different authentication methods from different vendors while maintaining a consistent level of assurance and security. However, the APP may typically employ LuxTrust authentication services for guaranteeing the minimum required assurance level.

Supported means are classified in conformity with the eIDAS levels of assurance for "electronic identification means", i.e. low, substantial, and high (cf. [2]).

In any case, the APP is solely responsible for specifying the minimum assurance level of a sign request, while this optional feature is supported for the ORELY portal only. In any event, the LuxTrust cloud signature services provided via ORELY or BLINK guarantee that employed authentication means always satisfy the required assurance level regarding the legal signature type specified in a sign request (cf. 3.2.1).

As concerns the accepted “trust anchors”, cf. 3.1.4.

3.3.3. BSP (n): SIGNATURE CREATION DEVICES

LuxTrust ensures that the signatory can only sign using a device and certificate that conforms to the requirements set by the APP, as specified in its sign request (cf. [21]).

The APP shall configure its system in accordance with LuxTrust in order to use an applicable and correct set of parameters in its requests.

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 default cryptographic suite for signature generation will be RSA SHA-256.

LuxTrust signature services may implement other algorithms for signature creation, namely the Elliptic Curve DSA algorithm with appropriate and state-of-the-art key sizes, as well as other hashing functions with appropriate and state-of-the-art hash lengths.

The document [15] can be consulted as a reference for state-of-art parameters and cryptographic suites.

Note: SHA-1 is still supported, exclusively for verification to provide compatibility with legacy systems.

3.4.3. BSP (q): TECHNOLOGICAL ENVIRONMENT

The LuxTrust specifications [18] , [19], [20], [21], [22], [23] and [24] specify technological constraints on the environment.

4. Requirements for Statements on Technical Mechanisms and Standards Implementation

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

This section contains the requirements that are specific to fully delegated PAdES signatures.

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 SIGNED

In the context of PAdES, the DTBS must be a PDF document, as defined in [3] and [4].

When the signature's level is B-B or B-T, the document should be in PDF/A-1b or PDF/A-2b format (cf. [5] and [6]).

When the signature's level is B-LT or B-LTA, the document should be in PDF/A-1a or PDF/A-2a format (cf. [5] and [6]).

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 [3] and [4].

The signature format is PAdES (cf. [9] and [10]).

7.1.4. BSP (d): TARGETED COMMUNITY

No further requirement beyond 3.1.4

Note 1: When an APP defines specific trust anchors (cf. 3.1.4), it should be noted that generated signatures might not be correctly be validated by third party tools (such as Adobe's *Acrobat Reader)* without adequate configuration.

Note 2: Conversely, third party tools may have their own pre-configured list of trust anchors that may differ from that of the LuxTrust or APP signature policy. Therefore, such software may validate or reject electronic signatures that the LuxTrust or the APP signature policy would reject or validate, respectively.

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

No further requirement beyond 3.1.5; in particular, ORELY, in contrast to BLINK, implicitly validates pre-existing signatures and shows the results to the signatory, who may voluntarily abstain from signing and voluntarily abort the process, but ORELY never impedes the signing

process. In this respect, repeated signature requests do not depend on the validity of existing signatures.

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 SIGNING

In the context of this policy, ***Fully Delegated Mode*** (cf. 3.2.4) is the only mode available.

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: SIGNATURE POLICY STATEMENT SUMMARY

Name and identifier of the signature policy authority: -**Error! Reference source not found.**
Name and identifier of the signature policy: LuxTrust Fully Delegated PAdES Signature Policy (1.3.171.1.4.1.1.2)

BSP	BSP title	Business statement summary	Technical statement counterpart
(a)	**Workflow (sequencing & timing) of signatures**	*Workflow is defined by the APP*	*Multiple PAdES signatures are necessarily serial*
(b)	**Data to be signed (DTBS)**	*Format: PDF*	*[9] and [10]*
(c)	**Relationship between DTBS & signature(s)**	*Defined by the APP from among the following signature levels:* *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 (not supported via ORELY) *PAdES signatures are enveloped*	*Signature levels from [8]*
(d)	**Targeted community**	*Any entity that must be or that chooses to be compliant with the eIDAS Regulation*	*Signature format*
(e)	**Allocation of responsibility for signature validation and augmentation**	*Managed by APP, if required, otherwise (but only in case of ORELY) managed by LuxTrust signature service*	*Provisions made by APP when needed as indicated in 7.1.5 and 3.1.5*
(f)	**Legal type of signature**	*Defined by the APP to be one of these legal types:* *1. Qualified electronic signatures;* *2. Advanced electronic signatures supported by a qualified certificate;* 3. *Advanced electronic signatures*	*Parameters in the sign request (cf. [21], specifically Signature QAA)*

BSP	BSP title	Business statement summary	Technical statement counterpart
(g)	**Commitment assumed by the signatory**	*"Proof of approval" unless defined by the APP*	*Commitment-type attribute is mandatory in the generated signatures. It is an optional parameter of the sign request*
(h)	**Level of assurance on timing evidence**	*Claimed by signatory for the basic level, timestamp for higher levels*	*LuxTrust Qualified Timestamping Authority, when applicable*
(i)	**Formalities of signing**	***Fully Delegated Mode** (cf. 3.2.4) is the only supported mode.*	*LuxTrust signature services responsibility and implementation in the case of ORELY; delegated to the APPs responsibility in the case of BLINK*
(j)	**Longevity & resilience to change**	*Signing certificate or timestamp validity, whichever is higher*	*Ditto*
(k)	**Archival**	*No requirement*	
(l)	**Identity of signatories**	*No requirement*	
(m)	**Level of assurance required for the authentication of the signatory.**	*Optionally defined by the APP; Supported means are classified according to the eIDAS levels for "electronic identification means": low, substantial, and high (cf. [2])*	• *Corresponding sign request parameter* • *Specific trust anchors configuration*
(n)	**Signature creation devices**	*Optionally defined by the APP from among the LuxTrust supported devices*	*Sign request parameters*
(o)	**Other information to be associated with the signature**	*No requirement*	
(p)	**Cryptographic suites**	*State-of-art cryptographic suites*	*Cryptographic libraries*
(q)	**Technological environment**	*Cf. LuxTrust specifications [18] , [19],[21] and [22]*	*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 SIGNATURE POLICY

TABLE 7.2

Name and identifier of the signature policy authority: -**Error! Reference source not found.**
Name and identifier of the signature policy: LuxTrust Fully Delegated PAdES Signature Policy (1.3.171.1.4.1.1.2)

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint value at signature creation (SCA or APP)
(a)	Workflow (sequencing & timing)	*Workflow is defined by the APP*	*Multiple PAdES signatures are necessarily serial*	APP constraints: OrderInSequence: *APP-defined* SCA constraints: SequencingNature: Mandated-serial
		Defined by the APP from among the following signature levels: *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 (not supported via ORELY)	*Signature levels from [8]*	SCA constraints TimingRelevance: TimingRelevanceOnEvidence: 1) MandatedSignedQProperties-signing-time 2) MandatedUnsignedQProperties-signature-time-stamp 3) MandatedUnsignedQProperties-signature-time-stamp 4) MandatedUnsignedQProperties-signature-time-stamp
				APP constraints: MassSigningAcceptable: • No regarding sign requests sent to ORELY • Yes otherwise
(b)	Data to be signed	*Format: PDF*	*[9] and [10]*	APP constraints: • ConstraintOnDTBS: PDF • DOTBSAsAWholeOrInParts: whole
(c)	The relationship between signed data and signature(s)	*Defined by the APP from among the following signature levels:* *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 (not supported via ORELY)	*Signature levels from [8]*	APP constraints: SignatureRelativePosition: enveloped 1) MandatedSignatureFormat: B-B 2) MandatedSignatureFormat: B-T 3) MandatedSignatureFormat: B-LT 4) MandatedSignatureFormat: B-LTA
(d)	Targeted community	*Any entity that must be or that chooses to be compliant with the eIDAS Regulation*	Use of PAdES format	None
(e)	Allocation of responsibility for signature validation and augmentation	*Managed by APP, if required, otherwise (but only in case of ORELY) managed by LuxTrust signature service*	*LuxTrust ORELY based on provisions made by APP when needed as indicated in 7.1.5 and 3.1.5*	SCA: ValidationRequiredBeforeAugmenting: yes

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint value at signature creation (SCA or APP)
(f)	Legal type of the signatures	*Defined by the APP to be one of the legal types:* *1. Qualified electronic signatures;* *2. Advanced electronic signatures supported by a qualified certificate;* *3. Advanced electronic signatures*	*Parameters in the sign request (cf. [21], specifically Signature QAA)*	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	*"Proof of approval" unless defined by the APP*	*Commitment-type attribute is mandatory in the generated signatures.* *It is an optional parameter of the sign request*	APP constraint: • CommitmentTypesRequired: MandatedSignedQProperties-commitment-type-indication: no SCA constraint: • CommitmentTypesRequired: MandatedSignedQProperties-commitment-type-indication: yes
(h)	Level of assurance on timing evidence	*Claimed by signatory for the basic level, timestamp for higher levels*	LuxTrust Qualified Timestamping Authority, when applicable	None
(i)	Formalities of signing	*Fully delegated mode*	*LuxTrust ORELY servers responsibility and implementation*	SCA & APP constraints: • WYSIWYSRequired: yes, unless in case of seal creation when authenticity guaranteed by APP by other means • WYSIWHBSRequired: yes • ProperAdviceAndInformationRequired: yes • UserInterfaceDesignConstraints: yes • CorrectValidationAndArchivalProcedures: no
(j)	Longevity and resilience to change	*Signing certificate or timestamp validity, whichever is higher*	*Ditto*	None
(k)	Archival	*No requirement*		None
(l)	Identity (and roles/attributes) of the signatories	*No requirement*		None
(m)	Level of assurance required for the authentication of the signatory	*Optionally defined by the APP* *Supported means are classified according to the eIDAS levels for "electronic identification means": low, substantial, and high (cf. [2])*	• *Corresponding sign request parameter* • *Specific trust anchors configuration*	SCA constraints: • X509CertificateValidationConstraints:SetOfTrustAnchors: APP-defined[3] or EU Trusted List • RevocationConstraints:RevocationCheckingConstraints: eitherCheck: yes

[3] APP-defined requires a specific signature policy

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint value at signature creation (SCA or APP)
(n)	Signature creation devices	*Optionally defined by the APP from among the LuxTrust supported devices*	*Sign request parameters*	None
(o)	Other information to be associated with the signature	*No requirement*		None
(p)	Cryptographic suites	*State-of-art cryptographic suites*	*Cryptographic libraries*	Cf. [15] for cryptographic constraints reference
(q)	Technological environment	*LuxTrust specifications [18], [19], [21] and [22]*	*LuxTrust implementation*	None

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 SIGNATURE POLICY

No constraint

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

No constraint

8. Annex B: Partially Delegated XAdES Signature Requirements

This section contains the requirements that are specific to Partially Delegated XAdES signatures.

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

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

XAdES detached signatures cover serial signature use cases, depending on APP's workflow:

- Initial signatures applied to a Manifest or
- Countersignatures (cf. [24] for implementation details)

Other variants are not supported.

8.1.2. BSP (b): DATA TO BE SIGNED

The data to be signed is either (cf. [24]):

- Any MIME-type/format and number of documents, technically represented as an XML <dsig:Manifest> element (cf. [7]), which contains the set of hashes of documents to be signed
- A single XML detached XAdES signature (countersigning)

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

In all cases, the signature is an XML detached signature, and the signature format is XAdES (cf. [11] and [12]).

Except for countersigning, the APP is responsible for the correct application of normalization and canonicalization algorithms to documents prior to hash calculations.

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; in particular, ORELY, in contrast to BLINK, or the APP, implicitly validates pre-existing signatures and shows the results to the signatory, who may voluntarily abstain from signing and voluntarily abort the process, but ORELY never impedes the signing process. In this respect, XML countersignatures requests (cf. [24]) are essentially technical and do not depend on the countersigned signatures' validity.

Note that the APP is responsible for calculating hashes of signatures and for verifying that they match with the corresponding parts of the DTBS 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 SIGNING

In the context of this policy, ***Partially Delegated Mode*** (cf. 3.2.4) is the only mode available.

Unless the APP can guarantee DTBS authenticity by other means in the case of seal creation, the APP is responsible for the presentation of the signed data in a readable format. This policy recommends using XSLT, XPath or XQuery to design and implement the display of the signed data to the signatory, as their semantics are standardized and acknowledged.

If the APP chooses the option of presenting the signature attributes, the APP takes full responsibility for this particular aspect and the requirement to satisfy all needs indicated in 3.2.4. In any event, the signature attributes must be accessible for or known to the signatory during signing.

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

No further requirement beyond 3.2.5

Note: XML data should be canonicalized before being hashed and signed in order to make signed data resilient to a limited set of XML transformations that can be induced by XML parsers and similar XML-specific software, but workflows and applications should not rely on such mechanisms.

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: SIGNATURE POLICY STATEMENT SUMMARY

Name and identifier of the signature policy authority: -**Error! Reference source not found.**
Name and identifier of the signature policy: LuxTrust Partially Delegated XAdES Signature Policy (1.3.171.1.4.1.2.2)

BSP	BSP title	Business statement summary	Technical statement counterpart
(a)	**Workflow (sequencing & timing) of signatures**	*Workflow is defined by the APP* *XAdES detached signatures under the present profile may cover multiple countersignatures depending on APP's workflow.*	*XML Manifest detached signatures*

BSP	BSP title	Business statement summary	Technical statement counterpart
(b)	**Data to be signed (DTBS)**	• *Any MIME-type/format and number of document hashes, technically represented as an XML <dsig:Manifest> element OR* • *A single XML detached XAdES signature (countersigning)*	[7], [11] and [12]
(c)	**Relationship between DTBS & signature(s)**	*Defined by the APP from among the following signature levels:* *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 (not supported via ORELY) The signature is an XML detached signature, and the signature format is XAdES (cf. [11] and [12]).	*Signature levels from [8]*
(d)	**Targeted community**	Any entity that must be or that chooses to be compliant with the eIDAS Regulation	*Signature format*
(e)	**Allocation of responsibility for signature validation and augmentation**	*Managed by APP, if required, otherwise (but only in case of ORELY) managed by LuxTrust signature service*	*LuxTrust ORELY based on provisions made by APP when needed as indicated in 8.1.5 and 3.1.5*
(f)	**Legal type of signature**	*Defined by the APP to be one of these legal types:* *1. Qualified electronic signatures;* *2. Advanced electronic signatures supported by a qualified certificate;* 3. *Advanced electronic signatures*	*Parameters in the sign request (cf. [21], specifically Signature QAA)*
(g)	**Commitment assumed by the signatory**	*"Proof of approval" unless defined by the APP*	*Commitment-type attribute is mandatory in the generated signatures. It is an optional parameter of the sign request*
(h)	**Level of assurance on timing evidence**	*Claimed by signatory for the basic level, timestamp for higher levels*	LuxTrust Qualified Timestamping Authority, when applicable

BSP	BSP title	Business statement summary	Technical statement counterpart
(i)	**Formalities of signing**	***Partially Delegated Mode*** *(cf. 3.2.4) is the only supported mode.*	• *In the case of ORELY portal: APP's responsibility and implementation for DTBS suitable management; LuxTrust or alternatively APP enables signature attributes inspection, with the enabling party becoming solely responsible for providing correct and full transparency* • *In the case of the BLINK portal: Entirely delegated to the APPs responsibility*
(j)	**Longevity & resilience to change**	*Signing certificate or timestamp validity, whichever is higher*	*Ditto*
(k)	**Archival**	*No requirement*	
(l)	**Identity of signatories**	*No requirement*	
(m)	**Level of assurance required for the authentication of the signatory.**	*Optionally defined by the APP* *Supported means are classified according to the eIDAS levels for "electronic identification means": low, substantial, and high (cf. [2])*	• *Corresponding sign request parameter* • *Specific trust anchors configuration*
(n)	**Signature creation devices**	*Optionally defined by the APP from among the LuxTrust supported devices*	*Sign request parameters*
(o)	**Other information to be associated with the signature**	*No requirement*	
(p)	**Cryptographic suites**	*State-of-art cryptographic suites*	*Cryptographic libraries*
(q)	**Technological environment**	*Cf. LuxTrust specifications [18] , [19], [21] and [24]*	*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 SIGNATURE POLICY

TABLE 8.2

Name and identifier of the signature policy authority: -**Error! Reference source not found.**
Name and identifier of the signature policy: LuxTrust Partially Delegated XAdES Signature Policy (1.3.171.1.4.1.2.2)

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint value at signature creation (SCA or APP)
(a)	Workflow (sequencing & timing)	*Workflow is defined by the APP. XAdES detached signatures under the present profile may cover multiple countersignatures depending on APP's* workflow.	XML Manifest detached signatures	SCA constraints: SequencingNature: *APP-defined, as below* • MandatedUnsignedQProperties-counter-signature (countersignature)
		Defined by the APP from among the following signature levels: *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 (not supported via ORELY)	*Signature levels from [8]*	SCA constraints TimingRelevance: TimingRelevanceOnEvidence: 1) MandatedSignedQProperties-signing-time 2) MandatedUnsignedQProperties-signature-time-stamp 3) MandatedUnsignedQProperties-signature-time-stamp 4) MandatedUnsignedQProperties-signature-time-stamp
				APP constraints: MassSigningAcceptable: • No regarding sign requests sent to ORELY • Yes otherwise

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint value at signature creation (SCA or APP)
(b)	Data to be signed	• Any MIME-type/format and number of documents, technically represented as an XML <dsig:Manifest> element OR • A single XML detached XAdES signature (countersigning)	[7], [11] and [12]	APP constraints: • DOTBSAsAWholeOrInParts:whole SCA constraints: • ContentRelatedConstraintsAsPartOfSignatureElements: MandatedSignedQProperties-DataObjetFormat (cf. [24])
(c)	The relationship between signed data and signature(s)	*Defined by the APP from among the following signature levels:* *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 (not supported via ORELY)	*Signature levels from [8]*	APP constraints: • SignatureRelativePosition: detached 1) MandatedSignatureFormat: B-B 2) MandatedSignatureFormat: B-T 3) MandatedSignatureFormat: B-LT 4) MandatedSignatureFormat: B-LTA SCA Constraints: • SignatureRelativePosition: enveloping
(d)	Targeted community	*Any entity that must be or that chooses to be compliant with the eIDAS Regulation*	*Use of XAdES format*	None
(e)	Allocation of responsibility for signature validation and augmentation	*Managed by APP, if required, otherwise (but only in case of ORELY) managed by LuxTrust signature service*	*LuxTrust ORELY based on provisions made by APP when needed as indicated in 8.1.5 and 3.1.5*	SCA: ValidationRequiredBeforeAugmenting: yes

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint value at signature creation (SCA or APP)
(f)	Legal type of the signatures	*Defined by the APP to be one of these legal types:* 1. *Qualified electronic signatures;* 2. *Advanced electronic signatures supported by a qualified certificate;* 3. *Advanced electronic signatures*	*Parameters in the sign request (cf. [21], specifically Signature QAA)*	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	*"Proof of approval" unless defined by the APP*	*Commitment-type attribute is mandatory in the generated signatures.* *It is an optional parameter of the sign request*	APP constraint: • CommitmentTypesRequired: MandatedSignedQProperties-commitment-type-indication: no SCA constraint: • CommitmentTypesRequired: MandatedSignedQProperties-commitment-type-indication: yes
(h)	Level of assurance on timing evidence	*Claimed by signatory for the basic level, timestamp for higher levels*	LuxTrust Qualified Timestamping Authority, when applicable	None
(i)	Formalities of signing	*Partially delegated mode*	*APP's responsibility and implementation for DTBS;* *LuxTrust ORELY or alternatively APP enables signature attributes inspection, with the enabling party becoming solely responsible for providing correct and full transparency*	SCA & APP constraints: • WYSIWYSRequired: yes, unless in case of seal creation when authenticity guaranteed by APP by other means • WYSIWHBSRequired: yes • ProperAdviceAndInformationRequired: yes • UserInterfaceDesignConstraints: yes CorrectValidationAndArchivalProcedures: no
(j)	Longevity and resilience to change	*Signing certificate or timestamp validity, whichever is higher*	*Ditto*	None
(k)	Archival	*No requirement*		None
(l)	Identity (and roles/attributes) of the signatories	*No requirement*		None

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint value at signature creation (SCA or APP)
(m)	Level of assurance required for the authentication of the signatory	*Optionally defined by the APP* *Supported means are classified according to the eIDAS levels for "electronic identification means": low, substantial, and high (cf. [2])*	• *Corresponding sign request parameter* • *Specific trust anchors configuration*	SCA constraints: • X509CertificateValidationConstraints:SetOfTrustAnchors: APP-defined[4] or EU Trusted List • RevocationConstraints:RevocationCheckingConstraints: eitherCheck: yes
(n)	Signature creation devices	*Optionally defined by the APP from among the LuxTrust supported devices*	*Sign request parameters*	None
(o)	Other information to be associated with the signature	*No requirement*		None
(p)	Cryptographic suites	*State-of-art cryptographic suites*	*Cryptographic libraries*	Cf. [15] for cryptographic constraints reference
(q)	Technological environment	*LuxTrust specifications [18], [19], [21] and [24]*	*LuxTrust implementation*	None

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 SIGNATURE POLICY

No constraint

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

No constraint

[4] APP-defined requires a specific signature policy

9. Annex C: Partially Delegated PAdES Signature Requirements

This section contains the requirements that are specific to partially delegated PAdES signatures.

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 SIGNED

In the context of PAdES, the DTBS must be a PDF document, as defined in [3] and [4].

When the signature's level is B-B or B-T, the document should be in PDF/A-1b or PDF/A-2b format (cf. [5] and [6]).

When the signature's level is B-LT or B-LTA, the document should be in PDF/A-1a or PDF/A-2a format (cf. [5] and [6]).

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 [3] and [4].

The signature format is PAdES (cf. [9] and [10]).

9.1.4. BSP (d): TARGETED COMMUNITY

No further requirement beyond 3.1.4

Note 1: When an APP defines specific trust anchors (cf. 3.1.4), it should be noted that generated signatures might not be correctly validated by third party tools (such as Adobe's *Acrobat Reader)* without adequate configuration.

Note 2: Conversely, third party tools may have their own pre-configured list of trust anchors, which may differ from that of the LuxTrust or APP signature policy. Therefore, such software may validate or reject electronic signatures that would be rejected or validated, respectively, by the LuxTrust or the APP signature policy.

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

No further requirement beyond 3.1.5; in particular, ORELY, in contrast to BLINK, implicitly validates pre-existing signatures and shows the results to the signatory, who may voluntarily abstain from signing and voluntarily abort the process, but ORELY never impedes the signing

process. In this respect, repeated (serial) signatures requests are essentially technical and do not depend on the existing signatures' validity.

Note that in addition to calculating hashes of signatures and timestamps and for verifying that they match with the corresponding parts of the DTBS as indicated in 3.1.5, the APP is also responsible for extracting pre-existing signatures from the DTBS and the embedding of generated signatures and other values generated by ORELY into the PDF document[5].

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 SIGNING

In the context of this policy, ***Partially Delegated Mode*** (cf. 3.2.4) is the only mode available.

Unless the APP can guarantee DTBS authenticity by other means in the case of seal creation, the APP is responsible for the presentation of the signed data in a readable format.

If the APP chooses the option of presenting the signature attributes, the APP takes full responsibility for this particular aspect and the requirement to satisfy all needs indicated in 3.2.4. In any event, the signature attributes must be accessible for or known to the signatory during signing.

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

[5] The process can be supported by software that may be optionally provided for the APP environment. However, any such support does NOT free the APP from the obligation to handle preparation and request of signature augmentation.

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: SIGNATURE POLICY STATEMENT SUMMARY

Name and identifier of the signature policy authority: -**Error! Reference source not found.**
Name and identifier of the signature policy: LuxTrust Partially Delegated PAdES Signature Policy (1.3.171.1.4.1.3.2)

BSP	BSP title	Business statement summary	Technical statement counterpart
(a)	**Workflow (sequencing & timing) of signatures**	*Workflow is defined by the APP*	*Multiple PAdES signatures are necessarily serial*
(b)	**Data to be signed (DTBS)**	*Format: PDF*	*[9] and [10]*

BSP	BSP title	Business statement summary	Technical statement counterpart
(c)	**Relationship between DTBS & signature(s)**	*Defined by the APP from among the following signature levels:* *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 (not supported via ORELY) *PDF signatures are enveloped.*	*Signature levels from [8]*
(d)	**Targeted community**	*Any entity that must be or that chooses to be compliant with the eIDAS Regulation*	*Signature format*
(e)	**Allocation of responsibility for signature validation and augmentation**	*Managed by APP, if required, otherwise (but only in case of ORELY) managed by LuxTrust signature service*	*provisions made by APP when needed as indicated in 0 and 3.1.5*
(f)	**Legal type of signature**	*Defined by the APP to be one of these legal types:* *1. Qualified electronic signatures;* *2. Advanced electronic signatures supported by a qualified certificate;* *3. Advanced electronic signatures*	*Parameters in the sign request (cf. [21], specifically Signature QAA)*
(g)	**Commitment assumed by the Signatory**	*"Proof of approval" unless defined by the APP*	*Commitment-type attribute is mandatory in the generated signatures. It is an optional parameter of the sign request*
(h)	**Level of assurance on timing evidence**	*Claimed by signatory for the basic level, timestamp for higher levels*	LuxTrust Qualified Timestamping Authority, when applicable
(i)	**Formalities of signing**	***Partially Delegated Mode*** *(cf. 3.2.4) is the only supported mode.*	• *In the case of ORELY portal: APP's responsibility and implementation for DTBS suitable management; LuxTrust or alternatively APP enables signature attributes inspection, with the enabling party becoming solely responsible for providing correct and full transparency* • *In the case of the BLINK portal: Entirely delegated to the APPs responsibility*
(j)	**Longevity & resilience to change**	*Signing certificate or timestamp validity, whichever is higher*	*Ditto*
(k)	**Archival**	*No requirement*	
(l)	**Identity of signatories**	*No requirement*	

BSP	BSP title	Business statement summary	Technical statement counterpart
(m)	**Level of assurance required for the authentication of the signatory.**	*Optionally defined by the APP* *Supported means are classified according to the eIDAS levels for "electronic identification means": low, substantial, and high (cf. [2])*	• *Corresponding sign request parameter* • *Specific trust anchors configuration*
(n)	**Signature creation devices**	*Optionally defined by the APP from among the LuxTrust supported devices*	*Sign request parameters*
(o)	**Other information to be associated with the signature**	*No requirement*	
(p)	**Cryptographic suites**	*State-of-art cryptographic suites*	*Cryptographic libraries*
(q)	**Technological environment**	*Cf. LuxTrust specifications [18] , [19], [21] and [23]*	*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 SIGNATURE POLICY

TABLE 9.2

Name and identifier of the signature policy authority: -**Error! Reference source not found.**
Name and identifier of the signature policy: LuxTrust Partially Delegated PAdES Signature Policy (1.3.171.1.4.1.3.2)

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint value at signature creation (SCA or APP)
(a)	Workflow (sequencing & timing)	*Workflow is defined by the APP*	*Multiple PAdES signatures are necessarily serial*	APP constraints: OrderInSequence: *APP-defined* SCA constraints: SequencingNature: Mandated-serial
		Defined by the APP from among the following signature levels: *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 (not supported via ORELY)	*Signature levels from [8]*	SCA constraints TimingRelevance: TimingRelevanceOnEvidence: 1) MandatedSignedQProperties-signing-time 2) MandatedUnsignedQProperties-signature-time-stamp 3) MandatedUnsignedQProperties-signature-time-stamp 4) MandatedUnsignedQProperties-signature-time-stamp
				APP constraints: MassSigningAcceptable: • No regarding sign requests sent to ORELY • Yes otherwise
(b)	Data to be signed	*Format: PDF*	*[9] and [10]*	APP constraints: • ConstraintOnDTBS: PDF • DOTBSAsAWholeOrInParts:whole
(c)	The relationship between signed data and signature(s)	*Defined by the APP from among the following signature levels:* *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 (not supported via ORELY)	*Signature levels from [8]*	APP constraints: • ConstraintsOnTheNumberOfDOTBS=1 • SignatureRelativePosition: enveloped 1) MandatedSignatureFormat: B-B 2) MandatedSignatureFormat: B-T 3) MandatedSignatureFormat: B-LT 4) MandatedSignatureFormat: B-LTA

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint value at signature creation (SCA or APP)
(d)	Targeted community	*Any entity that must be or that chooses to be compliant with the eIDAS Regulation*	Use of PAdES format	None
(e)	Allocation of responsibility for signature validation and augmentation	*Managed by APP, if required, otherwise (but only in case of ORELY) managed by LuxTrust signature service*	*LuxTrust ORELY based on provisions made by APP when needed as indicated in 9.1.5 and 3.1.5*	SCA: ValidationRequiredBeforeAugmenting: yes
(f)	Legal type of the signatures	*Defined by the APP to be one of these legal types:* *1. Qualified electronic signatures ;* *2. Advanced electronic signatures supported by a qualified certificate;* 3. *Advanced electronic signatures*	*Parameters in the sign request (cf. [21], specifically Signature QAA)*	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	*"Proof of approval" unless defined by the APP*	*Commitment-type attribute is mandatory in the generated signatures.* *It is an optional parameter of the sign request*	APP constraint: • CommitmentTypesRequired: MandatedSignedQProperties-commitment-type-indication: no SCA constraint: • CommitmentTypesRequired: MandatedSignedQProperties-commitment-type-indication: yes
(h)	Level of assurance on timing evidence	*Claimed by signatory for the basic level, timestamp for higher levels*	LuxTrust Qualified Timestamping Authority, when applicable	None
(i)	Formalities of signing	*Partially delegated mode*	*APP's responsibility and implementation for DTBS;* *LuxTrust ORELY or alternatively APP enables signature attributes inspection, with the enabling party becoming solely responsible for providing correct and full transparency*	SCA & APP constraints: • WYSIWYSRequired: yes, unless in case of seal creation when authenticity guaranteed by APP by other means • WYSIWHBSRequired: yes • ProperAdviceAndInformationRequired: yes • UserInterfaceDesignConstraints: yes CorrectValidationAndArchivalProcedures: no

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint value at signature creation (SCA or APP)
(j)	Longevity and resilience to change	*Signing certificate or timestamp validity, whichever is higher*	*Ditto*	None
(k)	Archival	*No requirement*		None
(l)	Identity (and roles/attributes) of the signatories	*No requirement*		None
(m)	Level of assurance required for the authentication of the signatory	*Optionally defined by the APP Supported means are classified according to the eIDAS levels for "electronic identification means": low, substantial, and high (cf. [2])*	• *Corresponding sign request parameter* • *Specific trust anchors configuration*	SCA constraints: • X509CertificateValidationConstraints:SetOfTrustAnchors: APP-defined[6] or EU Trusted List • RevocationConstraints:RevocationCheckingConstraints: eitherCheck: yes
(n)	Signature creation devices	*Optionally defined by the APP from among the LuxTrust supported devices*	*Sign request parameters*	None
(o)	Other information to be associated with the signature	*No requirement*		None
(p)	Cryptographic suites	*State-of-art cryptographic suites*	*Cryptographic libraries*	Cf. [15] for cryptographic constraints reference
(q)	Technological environment	*LuxTrust specifications [18], [19],[21] and [23]*	*LuxTrust implementation*	None

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 SIGNATURE POLICY

No constraint

[6] APP-defined requires a specific signature policy

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

No constraint

Thomas KOPP

Digitally signed by Thomas KOPP
DN: c=FR, l=LU, o=LuxTrust S.A., ou=B112233, cn=Thomas KOPP, sn=KOPP, givenName=Thomas, serialNumber=10102351840020952923, email=thomas.kopp@luxtrust.lu, title=Professional Person
Date: 2018.03.22 13:33:03 +01'00'