LuxTrust Cloud Signature Policies

Version number: 1.0

Publication Date: 15/09/2015

Effective Date: 15/09/2015

Copyright © 2015
All rights reserved

Document Information

Document title:	LuxTrust Cloud Signature Policies
Document Code	LT-2015-09-06-01-R-E
Project Reference:	LuxTrust S.A.
Document Type	Policy
Document Distribution List	IT, Security, Application Providers, Users
Document Classification	Public
Document Owner	IT

Version History

Version	Who	Date	Reason of modification
0.1	Sealweb	08/2015	First Draft
0.2	LuxTrust	09/2015	First Review
0.25	Sealweb	09/2015	Second version (per-format appendix)
0.26	LuxTrust	09/2015	Minor changes and clarifications
0.9	Sealweb	09/2015	Pre-final version with Embedded PAdES policy
1.0	Sealweb/LuxTrust	09/2015	Proof-reading

Table of Contents

Intellectual Property Rights

Without limiting the “all rights reserved” copyright on the present document, and except as duly licensed under written form, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without prior written permission of LuxTrust S.A..

References

[1] ISO 32000-1: *Document management - Portable document format - Part 1: PDF 1.7*.

[2] ETSI TS 119 132 – *Electronic Signatures and Infrastructures (ESI); XAdES digital signatures, Parts 1-2*

[3] ISO 19005-1: *Document Management – Electronic document file format for long term preservation – Part 1: Use of PDF 1.4* (PDF/A-1)

[4] ISO 19005-2: *Document management – Electronic document file format for long-term preservation – Part 2: Use of ISO 32000-1* (PDF/A-2)

[5] ISO 19005-3:2012: *Document management -- Electronic document file format for long-term preservation -- Part 3: Use of ISO 32000-1 with support for embedded files* (PDF/A-3)

[6] ETSI EN 319 102-1 – *Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation*

[7] ETSI EN 319 142-1 – *Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 1: Building blocks and PAdES baseline signatures*.

[8] ETSI EN 319 142-2 – *Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Extended PAdES signatures*.

[9] *Regulation (EU) 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*, July, 23th, 2014.

[10] 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*

[11] ETSI TS 119 102-1 – *Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation requirements*

[12] ETSI TS 119 312 – *Electronic Signatures and Infrastructures (ESI);Cryptographic suites*

[13] CEN CWA 14170:2001, *Security Requirements for Signature Creation Applications*

[14] CEN CWA 14171:2001, *Procedures for Electronic Signature Verification*

[15] *LuxTrust Time Stamping V2 Policy*, under « LuxTrust Global Timestamping CA » (https://www.luxtrust.lu/fr/repository)

[16] Loi du 22 mars 2000 relative à la création d'un Registre national d'accréditation, d'un Conseil national d'accréditation, de certification, de normalisation et de promotion de la qualité et d'un organisme luxembourgeois de normalisation.

[17] Loi modifiée du 14 août 2000 relative au commerce électronique modifiant le code civil, le nouveau code de procédure civile, le code de commerce, le code pénal et transposant la directive 1999/93/EC relative à un cadre communautaire pour les signatures électroniques, la directive relative à certains aspects juridiques des services de la société de l'information, certaines dispositions de la directive 97/7/CEE concernant la vente à distance des biens et des services autres que les services financiers.

[18] Règlement Grand-Ducal du 28 décembre 2001 portant détermination d'un système d'accréditation des organismes de certification et d'inspection, ainsi que des laboratoires d'essais et d'étalonnage et portant création de l'Office Luxembourgeois d'Accréditation et de Surveillance, d'un Comité d'accréditation et d'un Recueil national des auditeurs qualité et techniques.

[19] Règlement Grand-Ducal du 1er juin 2001 relatif aux signatures électroniques, au paiement électronique et à la création du Comité « Commerce Electronique ».

[20] Règlement Grand-Ducal du 21 décembre 2004 portant organisation de la notification des prestataires de services délivrant des certificats qualifiés mettant en place un système d'accréditation des prestataires de service de certification, créant un comité signature électronique et déterminant la procédure d'agrément des auditeurs externes.

[21] *LuxTrust ORELY Portal – SAML Specifications*, LuxTrust, 2015, v.1.0.2 or higher version

[22] *LuxTrust ORELY Portal – DSS Specifications*, LuxTrust, 2015, v.1.0.1 or higher version

[23] *LuxTrust ORELY Portal – Fully Delegated PAdES Specifications*, LuxTrust, 2015, v.1.0.3 or higher version

[24] *LuxTrust ORELY Portal – Partially Delegated XAdES Specifications,* LuxTrust, 2015, v.1.0.0 or higher version

1 Introduction

1.1 Overview

The current document presents the signature policies for LuxTrust ORELY.

LuxTrust ORELY is a central authentication and signature service portal used by Application providers (APP) to authenticate physical person users (Signatories) and apply signatures to documents.

LuxTrust ORELY services are configured in accordance with each Application provider, which then relies on them for the creation of electronic signatures by its users. Applications providers must enter a contractual relationship and a service agreement with LuxTrust before offering the signature service to end-users.

1.2 Business or Application Domain

1.2.1 Scope and Boundaries of Signature Policy

The signature policies specified herein 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.

The Application providers are responsible for the management and implementation of the interaction with the end-user (Signatory) through a web browser or through an alternative graphical user interface, as well as for the technical integration of LuxTrust ORELY services into their technical workflow.

This signature policy contains two kinds of requirements: explicit and well-defined requirements regarding the actors (Signatory, LuxTrust, Application provider), and requirements on the Application provider's signature policy contents, as several details depend on the actual Application provider's use case.

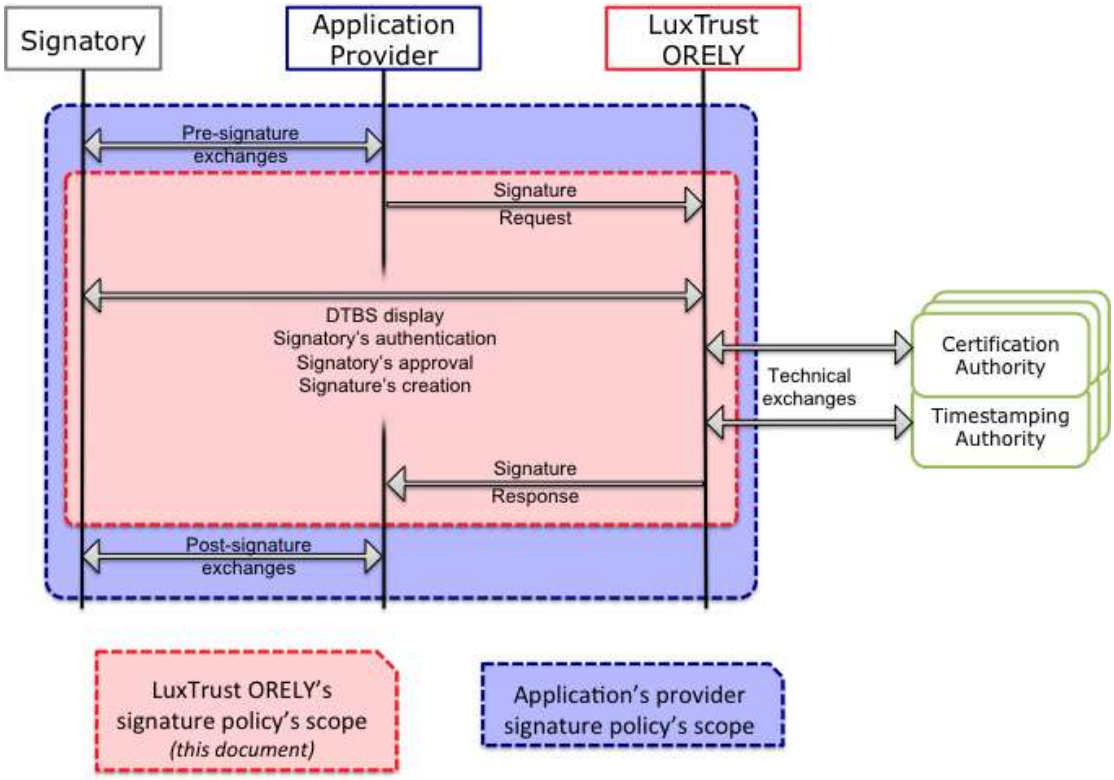

Figure 1 – Signature workflow and signature policy's scope

Application Providers sticking to the present signature policy shall derive their specific rules from the present policy, as shown in Figure 1 (blue area).

1.2.2 Domain of Applications

Not applicable (unrestricted).

1.2.3 Transactional Context

The Application provider shall define, in its own signature policy, the final transactional context, according to its needs. For the purpose of the present signature policy, the signature generation takes place within the context of the "Signature flow" specified by LuxTrust ORELY, through a sequence of messages exchanged between the Application Providers, the Signatory and LuxTrust ORELY (see Figure 1, p. 8):

1. The Application provider sends a signature request to LuxTrust ORELY (containing the document to be signed or one or more hashes of document[s] to be signed and transactional parameters)
2. LuxTrust ORELY interacts with the Signatory for authentication and signature generation, either
    a. Independently of the Application provider's interface ("fully delegated mode", see 3.2.4); or
    b. Through the Application provider's interface ("partially delegated mode").

    Each mode implies specific requirements.
3. LuxTrust ORELY sends a signature response to the Application provider (which contains the signed document or the signed hash[es], unless an error occurred)

In this respect, LuxTrust ORELY services operate independently of the Application provider's signature context.

1.3 Document and Policy Names, Identification and Conformance Rules

1.3.1 Signature Policy Document and Signature Policies 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 Policies Identifiers

Signature policy name	Signature policy OID
LuxTrust Fully Delegated PAdES Signature Policy	1.3.171.1.4.1.1.1
LuxTrust Partially Delegated XAdES Signature Policy	1.3.171.1.4.1.2.1
LuxTrust Partially Delegated PAdES Signature Policy	1.3.171.1.4.1.3.1

1.3.3 Conformance Rules

Electronic signatures produced under the above signature policies (1.3.1) comply with the eIDAS Regulation on electronic identification and trust services for electronic transactions [9].

The contents of this document comply with [10].

1.3.4 Distribution Points

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

1.4 Signature Policy Document Administration

1.4.1 Signature Policy Authority

LuxTrust contact information	
Postal Address:	LuxTrust S.A. IVY Building Parc d'Activités, 13-15 L-8308 Capellen
E-mail address:	info@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: ca@LuxTrust.lu

Phone: +352 2668 151

1.4.3 Approval Procedures

The Policy Approval Authority within LuxTrust S.A. is called the LuxTrust CSP Board. It is the high-level management body with final authority and responsibility for:

- Specifying and approving the LuxTrust infrastructure and practices.
- Approving, among others, the LuxTrust Signature Policies
- Defining the review process for practices and policies including responsibilities for maintaining the Signature Policies
- Defining the review process that ensures that the LuxTrust service properly implements the above practices.
- Publication to the Application providers, Signatories and Relying Parties of the Signature Policies and Certification Practice Statements and their revisions.

Prior to becoming applicable, modifications to the Signature Policies are announced in the repository as available on https://repository.luxtrust.lu.

1.5 Definitions and Acronyms

APP	Application provider
BSP	Business scoping parameter
DTBS	Data to be signed
PAdES	PDF advanced signature
PDF	Portable document format [1]
SCA	Signature creation application (LuxTrust ORELY, in our context)
SP	Service provider (other name for the APP)

TSP	Trust Service Portal
XAdES	XML advanced signature
XML	Extensible markup language

2 Signature Application Practices Statements

2.1 Requirements on Application Provider Applications

According to the Signature creation model of [6], the APP's application is the "Driving application", that is, an "application that uses a signature creation system [LuxTrust ORELY] to create a signature". As such, the APP's application must comply with technical standards and follow LuxTrust ORELY technical and integration guidance. In particular,

- it must not send ill-formed or malicious data (messages) to LuxTrust ORELY service
- it must not tamper with or examine/record data exchanged between LuxTrust ORELY service and the Signatory
- it must not tamper with LuxTrust ORELY client-side software components
- it must securely maintain logs so as to ensure the imputability of transactions between its application, LuxTrust ORELY 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 comply with requirements from [13] and [14]

2.2 Requirements on the Signature Creation/Verification Application

When applicable (signature through a web interface), the signature creation application development should follow the “OWASP Best Practices”.

For signature creation, requirements from [13] are applicable.

For signature validation, requirements from [14] are applicable.

3 Business Scoping Parameters

The description of the signature policy's business scoping parameters (BSP) is manifold: first, the global BSP's are described below and are applicable to all business cases. In particular, they do not depend on the signature's format.

Second, these BSP's are completed by format-specific BSP's, which are described in their respective annexes:

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

Third, some business scoping parameters depend on the *working mode* between LuxTrust and the Application provider (see “BSP (i): Formalities of Signing”, p. 15).

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 a single advanced electronic signature, with possible timestamp and proof-data extensions, which signs a single or multiple DTBS at the same time (typically, but not limited to document hashes).

LuxTrust ORELY can however be used to implement business workflows with multiple signatures; in such case, each single signature within the Application provider’s workflow will be produced by a separate, distinguished signature transaction according to the present signature policy. Workflow and signatures’ management shall then be described in the Application provider’s signature policy.

3.1.2 BSP (b): Data to be signed

The Application provider is responsible for the contents and the correct formatting of the DTBS (with respect to the applicable standard). 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 ORELY.

The DTBS’s format can be PDF (Annex A: Fully Delegated PAdES Signature) or XML (Annex B: Partially Delegated XAdES Signature Requirements).

LuxTrust ORELY services guarantee the confidentiality of the DTBS, according to the applicable laws on privacy, as well as according to the Luxembourg laws on the financial sector. All copies of the received documents, if any, are erased from LuxTrust servers once sent back (signed) to the Application provider.

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 [6]) are:

1. B-B (basic signature)
2. B-T (signature with time)
3. (optionally) B-LT (signature with long-term validation data)

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 Application provider’s signature policy, signatures produced by LuxTrust ORELY shall be validated using the European trust list. LuxTrust ORELY signatures comply with the eIDAS Regulation [9] and should be accepted in any EU member state.

Nevertheless, Application providers may, in accordance with LuxTrust, define additional "trust anchors" in their signature policy. These trust anchors can be configured in LuxTrust ORELY and be used in trust chains and

certificate validation paths for the specific Application provider. In such case, LuxTrust ORELY cannot be held responsible for the acceptance or rejection of the generated signatures by third parties/software.

3.1.5 BSP (e): Allocation of Responsibility for Signature Validation and Augmentation

LuxTrust ORELY timestamps the signatures according to the signature request's profile (B-T or B-LT); section 3.2.3 provides details on the timestamping of the signatures.

Regarding B-LT signatures, LuxTrust ORELY augments the initial signature following its creation.

When in "fully delegated mode" (see 3.2.4), LuxTrust ORELY automatically validates existing signatures in the DTBS. Should the DTBS contain an invalid signature, that information is returned to the Signatory. LuxTrust ORELY *will not* cancel or interrupt the signature process because of an invalid signature contained in the DTBS.

When in "partially delegated mode" (see 3.2.4), there is no validation of third-party signatures.

If the Application provider's workflow requires previous signatures to be validated, such constraint has to be enforced within its workflow, before calling LuxTrust ORELY signature creation service.

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 ORELY service supports all legal types of advanced electronic signature for natural persons [9]:

1. Qualified electronic signatures;
2. Advanced electronic signatures supported by a qualified certificate;
3. Advanced electronic signatures.

All advanced electronic signatures are[1]…

(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 sole control; and

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

The Application provider shall define the actual legal type of signature in its signature policy and process. Technically, the Application provider shall specify the minimum or exact legal level of the signature in its signature request to LuxTrust ORELY.

Note: qualified electronic signatures require at least a B-T signature level (see 3.1.3).

3.2.2 BSP (g): Commitment Assumed by the Signatory

Commitment type is defined by the Application provider depending on its use case; technically, the Application provider may specify the commitment type associated to the signature in its signature request to LuxTrust ORELY.

If the Application provider specifies no commitment, the default commitment value is "*proof of approval*".

3.2.3 BSP (h): Level of Assurance on Timing Evidences

The TSP provides a timestamp by default or when explicitly requested, thus augmenting the signature to B-T. The timestamp is provided by the LuxTrust Global timestamping authority [15] with the production policy in force being employed for the production service[2].

Otherwise, the B-B signature level contains a "claimed [UTC] signing time" of the signature [6].

[1] As defined in [9], art. 26.

[2] Note that an document/archive timestamp in order to augment the signature to B-LTA is not supported (cf. 3.2.5)

3.2.4 BSP (i): Formalities of Signing

Presentation of the DTBS and signature attributes to the Signatory is mandatory. Technically, two implementations are available, which correspond to two distinct working modes:

a) *Partially Delegated Mode:* The Application provider's software shall present the DTBS and signature attributes to the Signatory before the start of the LuxTrust ORELY signature process. In that case, the Application provider shall guarantee that

   i. "the presented document shall be equal in content to the document that is signed [that is, the document sent to LuxTrust ORELY for signature, or its cryptographic hash]" [6]

   ii. the user interface conforms to [6], [13] and [14]

b) *Fully Delegated Mode:* LuxTrust ORELY shall present the DTBS and signature attributes to the Signatory before signature creation. The Application provider shall guarantee that its implementation and technical integration of LuxTrust ORELY services do not tamper with LuxTrust ORELY's presentation of the DTBS and other signature attributes to the Signatory.

All the following signature attributes shall be presented to the Signatory:

- Signing certificate
- Signature policy identifier
- Commitment type
- Existing signatures in the DTBS and their validation status

LuxTrust ORELY user interface focuses on Signatory's authentication and legal requirements on expression of will by the Signatory when his/her approval is needed. The fulfillment of any business-specific requirements originating from the Application provider workflow remains under the Application provider's responsibility.

In all cases, the Application provider 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 timestamping authority [15] with the production policy in force being employed for the production service. Such timestamp is valid during at most 5 (five) years, and no less than 4 (four).
- B-LT signature: the signature's longevity is that of the above-cited B-T signature. It is augmented by proof elements being added for the contained signatures,

  A B-LT signature's longevity can be augmented with a renewed, additional document/archive timestamp (and its optionally proof elements) resulting in a B-LTA signature. Alternatively, a centralized electronic archiving service could be employed to ensure longevity. Note however, that B-LTA signatures are NOT supported under the present policy in conformance with the respective eIDAS implementing acts.

In any case, the cryptographic algorithms and parameters are chosen so as to ensure that the electronic signature's resilience can be maintained (at least) as long as its longevity.

3.2.6 BSP (k): Archival

The present policy has no archival requirement on the generated signatures. LuxTrust ORELY does not keep a copy of the generated signatures nor the signed documents, whose duration (cf. 3.2.5) must be tailored so that it is sufficient for the considered use case. The goal of the electronic signature is to be self-contained and not require additional out-of-band information for proofing its evidence.

If needed, archival of the signature is on the Application provider's behalf, which may delegate it to the Signatory in its own signature policy or terms of use.

Nevertheless, LuxTrust ORELY transaction logs are backed up and archived for 10 (ten) years and can be used in legal procedures.

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 Application provider may provide LuxTrust ORELY with the Signatory's identity and minimum assurance level of the authentication means (see 3.3.2) in the signature request.

The present signature policy has no requirement on 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 Application provider's signature policy or terms of service, and implemented within the Application provider's workflow.

3.3.2 BSP (m): Level of Assurance Required for the Authentication of the Signatory

The Application provider may provide, through the signature request, LuxTrust ORELY with the minimum assurance level of the means the Signatory may use to authenticate himself (herself). This allows LuxTrust ORELY to support different authentication methods from different vendors while maintaining a consistent level of assurance and security; supported means are classified along the eIDAS levels for "electronic identification means": low, substantial and high assurance levels [9]. Additionally, LuxTrust ORELY also supports a "No/minimal" assurance level.

In any case, the Application provider is the sole responsible for the signature request's minimum assurance level. For what concerns the accepted “trust anchors”, see 3.1.4.

3.3.3 BSP (n): Signature Creation Devices

LuxTrust ORELY ensures that the Signatory may only sign using a device and certificate that conforms to the requirements set by the Application provider, as specified in its signature request. For instance, by asking for the Signatory's certificate to be issued by a qualified CA, the Application provider may ensure that the Signatory will use a SSCD when signing.

The Application provider shall configure its system in accordance with LuxTrust so as to use an applicable and correct set of parameters in its signature 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 with the Application provider, the default cryptographic suite for signature generation will be RSA SHA-256.

LuxTrust ORELY may implement other algorithms for signature generation, namely the DSA algorithm and, optionally, 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.

ETSI TS [12] can be used 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

Technological constraints on the environment can be found in LuxTrust ORELY specifications [21][22][23][24].

4 Requirements / Statements on Technical Mechanisms and Standards Implementation

Signature policy statement summary are format-specific (see Annex A: Fully Delegated PAdES Signature or Annex B: Partially Delegated XAdES Signature Requirements).

5 Other Business and Legal Matters

That part is addressed in the contract between LuxTrust and the Application provider.

6 Compliance Audit and Other Assessments

The Application provider, supporting LuxTrust ORELY service under the present signature policy, shall accept and provide all required assistance and work to successfully comply and pass audit or controls related to its obligations, as expressed in 2.1, when required by LuxTrust S.A.

7 Annex A: Fully Delegated PAdES Signature Requirements

This section contains the requirements that are specific to 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 sequential.

7.1.2 BSP (b): Data to be signed

In the context of the PAdES policy, the DTBS must be a PDF document, as defined in [1].

When the signature's level is B-B or B-T, the document should be in PDF/A-1b format ([4] or [5]).

When the signature's level is B-LT, the document should be in PDF/A-1a format ([4] or [5]).

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 [1].

The signature format is PAdES [7].

7.1.4 BSP (d): Targeted Community

No further requirement.

Note 1: when Application provider's specific trust anchors are defined (see 3.1.4), it is recalled that the generated signatures may not be correctly validated by usual PDF software (such as Adobe's *Acrobat Reader)* without adequate configuration (that is, manual client-side configuration of the client software's trust anchors).

Note 2: conversely, PDF software usually has its own pre-configured list of trust anchors, which may differ from that of LuxTrust ORELY or the Application provider's signature policy. Therefore, that software may validate electronic signatures that would be rejected by LuxTrust ORELY's or the Application provider's signature policies.

7.1.5 BSP (e): Allocation of Responsibility for Signature Validation and Augmentation

No further requirement.

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.

7.2.2 BSP (g): Commitment Assumed by the Signatory

No further requirement.

7.2.3 BSP (h): Level of Assurance on Timing Evidences

No further requirement.

7.2.4 BSP (i): Formalities of Signing

No further requirement.

7.2.5 BSP (j): Longevity and Resilience to Change

No further requirement.

7.2.6 BSP (k): Archival

No further requirement.

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.

7.3.2 BSP (m): Level of Assurance Required for the Authentication of the Signatory

No further requirement.

7.3.3 BSP (n): Signature Creation Devices

No further requirement.

7.4 Other BSPs

7.4.1 BSP (o): Other Information to be Associated with The Signature

No specific requirement.

7.4.2 BSP (p): Cryptographic Suites

No further requirement.

7.4.3 BSP (q): Technological Environment

No further requirement.

7.5 Technical Counterparts of BSPs – Statement Summary

Table 7.1 : Signature Policy Statement Summary

Name and identifier of the signature policy authority: LuxTrust S.A. IVY Building Parc d'Activités, 13-15 L-8308 Capellen
Name and identifier of the signature policy: LuxTrust Fully Delegated PAdES Signature Policy (1.3.171.1.2.1.1.1)
Identifier of the concerned signature(s) in the concerned signature workflow: *(only applicable for the Application provider)*

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*	*[7] or [2]*

BSP	BSP title	Business statement summary	Technical statement counterpart
(c)	**Relationship between DTBS & signature(s)**	*Defined by the APP among the following four signature levels:* *1) basic signature* *2) signature with time* *3) signature with long-term validation data* *PAdES signatures are enveloped*	*Signature levels from* [6]
(d)	**Targeted community**	*Any entity in EU member states*	*Signature format*
(e)	**Allocation of responsibility for signature validation and augmentation**	*LuxTrust ORELY*	LuxTrust ORELY servers
(f)	**Legal type of signature**	*(defined by the APP among:* *1. Qualified electronic signatures;* *2. Advanced electronic signatures supported by a qualified certificate;* 3. *Advanced electronic signatures.)*	*Parameters in the signature request (QAA level, TSP-Type and TSP-ID)*
(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 signature request*
(h)	**Level of assurance on timing evidences**	*Claimed by signatory for the basic level, timestamp for higher levels*	LuxTrust Global timestamping authority, when applicable
(i)	**Formalities of signing**	*Partially or fully delegated mode*	• *Partially delegated mode: APP's responsibility and implementation* • *Fully delegated mode: LuxTrust ORELY servers*
(j)	**Longevity & resilience to change**	*Signing's certificate or timestamp's duration, whichever is higher*	*Idem.*
(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 along the eIDAS levels for "electronic identification means": low, substantial and high assurance levels [9].	• *Corresponding signature request's parameter* • *Specific trust anchors configuration*
(n)	**Signature creation devices**	*(Optionally defined by the APP among the LuxTrust supported devices)*	*Signature request's parameters*
(o)	**Other information to be associated with the signature**	*No requirement*	

BSP	BSP title	Business statement summary	Technical statement counterpart
(p)	Cryptographic suites	*State-of-art cryptographic suites*	*Cryptographic libraries*
(q)	Technological environment	*See LuxTrust specifications [21][22][23][24]*	*LuxTrust implementation*
Signature creation/validation application practices statements		-	-

Other parameters (the relevance of use of a container to package the signature(s) together with signed data, the specific attributes (signed or unsigned) of the signature, etc.) are defined by the Application provider.

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: LuxTrust S.A. IVY Building Parc d'Activités, 13-15 L-8308 Capellen
Name and identifier of the signature policy: LuxTrust Fully Delegated PAdES Signature Policy (1.3.171.1.2.1.1.1)
Identifier of the concerned signature(s) in the concerned signature workflow: *(only applicable for the Application provider)*

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 among the following four signature levels: *1) basic signature* *2) signature with time* *3) signature with long-term validation data*	*Signature levels from* [6]	• SCA constraints TimingRelevance: TimingRelevanceOnEvidence: 1) MandatedSignedQProperties-signing-time 2) MandatedUnsignedQProperties-signature-time-stamp 3) MandatedUnsignedQProperties-signature-time-stamp

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint value at signature creation (SCA or APP)
				APP constraints : MassSigningAcceptable : no
(b)	Data to be signed	*Format: PDF*	*[7]*	APP constraints : • ConstraintOnDTBS : PDF • DOTBSAsAWholeOrInParts:whole
(c)	The relationship between signed data and signature(s)	*Defined by the APP among the following four signature levels:* *1) basic signature* *2) signature with time* 3) *signature with long-term validation data*	*Signature levels from* [6]	APP constraints : • SignatureRelativePosition:envelopped 1) MandatedSignatureFormat:B-B 2) MandatedSignatureFormat:B-T 3) MandatedSignatureFormat:B-LT
(d)	Targeted community	*Any entity in EU member states*	Use of PAdES format	None
(e)	Allocation of responsibility for signature validation and augmentation	*LuxTrust Cloud Services*	*LuxTrust ORELY*	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 among:* 1. *Qualified electronic signatures;* 2. *Advanced electronic signatures supported by a qualified certificate;* 3. *Advanced electronic signatures.)*	*Parameters in the signature request (QAA level, TSP-Type and TSP-ID)*	APP constraints: ConstraintsOnCertificateMetadata: LegalPersonSignerRequired:no LegalPersonSignerAllowed:no 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 signature request*	APP constraint: CommitmentTypesRequired: MandatedSignedQProperties-commitment-type-indication:no SCA constraint: CommitmentTypesRequired: MandatedSignedQProperties-commitment-type-indication:yes

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint value at signature creation (SCA or APP)
(h)	Level of assurance on timing evidences	*Claimed by signatory for the basic level, timestamp for higher levels*	LuxTrust Global timestamping authority, when applicable	(none)
(i)	Formalities of signing	*Partially or fully delegated mode*	• *Partially delegated mode: APP's responsibility and implementation*	SCA & APP constraints: WYSIWYSRequired:yes WYSIWHBSRequired:yes ProperAdviceAndInformationRequired:yes UserInterfaceDesignConstraints:yes CorrectValidationAndArchivalProcedures:no
			• *Fully delegated mode: LuxTrust ORELY servers*	SCA constraints: WYSIWYSRequired:yes 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's certificate or timestamp's duration, whichever is higher*	*Idem.*	(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 along the eIDAS levels for "electronic identification means": low, substantial and high assurance levels [9].	• *Corresponding signature request's parameter* • *Specific trust anchors configuration*	SCA constraints: X509CertificateValidationConstraints:SetOfTrustAnchors:(APP-defined[3] or EU Trusted List)

[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 among the LuxTrust supported devices)*	*Signature request's parameters*	
(o)	Other information to be associated with the signature	*No requirement*		
(p)	Cryptographic suites	*State-of-art cryptographic suites*	*Cryptographic libraries*	See [12] for cryptographic constraints reference.
(q)	Technological environment	*LuxTrust specifications [21][22][23][24]*	*LuxTrust implementation*	(none)

Summary of the selected signature format(s) including details on the format of the signed data, the relative placement of the signature and the signed data (e.g. enveloped, enveloping, detached), the relevance of use of a container to package the signature(s) together with signed data, the specific attributes (signed or unsigned) of the signature, and the expected level of selected signature format.

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 policy is not yet defined in the current version of the document.

9 Annex C: Partially Delegated PAdES Signature Requirements

This policy is not yet defined in the current version of the document.

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=1010235184002095 2923, email=thomas.kopp@luxtrust.lu, title=Professional Person
Reason: I am approving this document
Location: LUXEMBOURG
Date: 2015.10.01 09:14:29 +02'00'