

Version number: 1.1.3

Publication Date: 25/11/2016

Effective Date: 25/11/2016

Copyright © 2016 All rights reserved

Document Information

Document Title	LuxTrust Cloud Signature PoliciesLuxTrust 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	Thomas Kopp	

Version History

Version	Date	Reason of Modification	
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	ntegration of amended changes concerning shared responsibilities – new definition	

Table of Contents

DOCUMENT	INFORMATION	2
VERSION HIS	STORY	2
TABLE OF CO	DNTENTS	3
INTELLECTU	AL PROPERTY RIGHTS	6
DISCLAIMER		6
REFERENCES		7
1	INTRODUCTION	8
1.1	Overview	8
1.2	Business or Application Domain	8
1.2.1	Scope and Boundaries of Signature Policy	8
1.2.2	Domain of Applications	8
1.2.3	Transactional Context	9
1.3	DOCUMENT AND POLICY NAMES, IDENTIFICATION AND CONFORMANCE RULES	9
1.3.1	Signature Policy Document and Signature Policies Names	9
1.3.2	Signature Policy Document and Signature Policies Identifiers	9
1.3.3	Conformance Rules	9
1.3.4	Distribution Points	9
1.4	SIGNATURE POLICY DOCUMENT ADMINISTRATION	9
1.4.1	Signature Policy Authority	9
1.4.2	Contact Address	9
1.4.3	Approval Procedures	10
1.5	Definitions and Acronyms	10
2	SIGNATURE APPLICATION PRACTICES STATEMENTS	10
2.1	REQUIREMENTS ON APPLICATION PROVIDER APPLICATIONS	10
2.2	REQUIREMENTS ON THE SIGNATURE CREATION/VERIFICATION APPLICATION	10
3	BUSINESS SCOPING PARAMETERS	10
3.1	BSPs Mainly Related to the Concerned Application/Business Process	10
3.1.1	BSP (a): Workflow (Sequencing and Timing) of Signatures	10
3.1.2	BSP (b): Data to be signed	11
3.1.3	BSP (c): The Relationship between Signed Data and Signature(s)	11
3.1.4	BSP (d): Targeted Community	11
3.1.5	BSP (e): Allocation of Responsibility for Signature Validation and Augmentation	11
3.2	BSPs Mainly Influenced by the Legal/Regulatory Provisions Associated to the Concerned Application/Business Process	11
3.2.1	BSP (f): Legal type of The Signatures	11
3.2.2	BSP (g): Commitment Assumed by the Signatory	12
3.2.3	BSP (h): Level of Assurance on Timing Evidences	12
3.2.4	BSP (i): Formalities of Signing	12
3.2.5	BSP (j): Longevity and Resilience to Change	12
3.2.6	BSP (k): Archival	13
3.3	BSPs Mainly Related to the Actors Involved in Creating/Augmenting/Validating Signatures	13
3.3.1	BSP (I): Identity (and Roles/Attributes) of the Signatories	13

VERSION 1.1.3

3.3.2	BSP (m): Level of Assurance Required for the Authentication of the Signatory	13
3.3.3	BSP (n): Signature Creation Devices	13
3.4	OTHER BSPs	13
3.4.1	BSP (o): Other Information to be Associated with the Signature	13
3.4.2	BSP (p): Cryptographic Suites	13
3.4.3	BSP (q): Technological Environment	13
4	REQUIREMENTS / STATEMENTS ON TECHNICAL MECHANISMS AND STANDARDS IMPLEMENTATION	14
5	OTHER BUSINESS AND LEGAL MATTERS	14
6	COMPLIANCE AUDIT AND OTHER ASSESSMENTS	14
7	ANNEX A: FULLY DELEGATED PADES SIGNATURE REQUIREMENTS	15
7.1	BSPs Mainly Related to the Concerned Application/Business Process	15
7.1.1	BSP (a): Workflow (Sequencing and Timing) of Signatures	15
7.1.2	BSP (b): Data to be signed	15
7.1.3	BSP (c): The Relationship between Signed Data and Signature(s)	15
7.1.4	BSP (d): Targeted Community	15
7.1.5	BSP (e): Allocation of Responsibility for Signature Validation and Augmentation	15
7.2	BSPs Mainly Influenced by the Legal/Regulatory Provisions Associated to the Concerned Application/Business Process	15
7.2.1	BSP (f): Legal Type of the Signatures	15
7.2.2	BSP (g): Commitment Assumed by the Signatory	15
7.2.3	BSP (h): Level of Assurance on Timing Evidences	15
7.2.4	BSP (i): Formalities of Signing	15
7.2.5	BSP (j): Longevity and Resilience to Change	15
7.2.6	BSP (k): Archival	15
7.3	BSPs Mainly Related to the Actors Involved in Creating/Augmenting/Validating Signatures	16
7.3.1	BSP (I): Identity (and Roles/Attributes) of the Signatories	16
7.3.2	BSP (m): Level of Assurance Required for the Authentication of the Signatory	16
7.3.3	BSP (n): Signature Creation Devices	16
7.4	OTHER BSPs	16
7.4.1	BSP (o): Other Information to be Associated with The Signature	16
7.4.2	BSP (p): Cryptographic Suites	16
7.4.3	BSP (q): Technological Environment	16
7.5	TECHNICAL COUNTERPARTS OF BSPS – STATEMENT SUMMARY	16
7.6	INPUT AND OUTPUT CONSTRAINTS FOR SIGNATURE CREATION, AUGMENTATION AND VALIDATION PROCEDURES	17
7.6.1	Input Constraints to be used when Generating, Augmenting and/or Validating Signatures in The Context of The Id Signature Policy	lentified 17
7.6.2	Output Constraints to be Used when Validating Signatures in The Context of The Identified Signature Policy	19
7.6.3	Output Constraints to be used for Generating/Augmenting Signatures in The Context of The Identified Signature Policy \cdot	19
8	ANNEX B: PARTIALLY DELEGATED XADES SIGNATURE REQUIREMENTS	20
8.1	BSPs Mainly Related to the Concerned Application/Business Process	20
8.1.1	BSP (a): Workflow (Sequencing and Timing) of Signatures	20
8.1.2	BSP (b): Data to be signed	20
8.1.3	BSP (c): The Relationship between Signed Data and Signature(s)	20
8.1.4	BSP (d): Targeted Community	20
8.1.5	BSP (e): Allocation of Responsibility for Signature Validation and Augmentation	20
8.2	BSPs Mainly Influenced by the Legal/Regulatory Provisions Associated to the Concerned Application/Business Process	20
8.2.1	BSP (f): Legal Type of the Signatures	20

VERSION 1.1.3

8.2.2	BSP (g): Commitment Assumed by the Signatory	20
8.2.3	BSP (h): Level of Assurance on Timing Evidences	20
8.2.4	BSP (i): Formalities of Signing	20
8.2.5	BSP (j): Longevity and Resilience to Change	20
8.2.6	BSP (k): Archival	21
8.3	BSPs Mainly Related to the Actors Involved in Creating/Augmenting/Validating Signatures	21
8.3.1	BSP (I): Identity (and Roles/Attributes) of the Signatories	21
8.3.2	BSP (m): Level of Assurance Required for the Authentication of the Signatory	21
8.3.3	BSP (n): Signature Creation Devices	21
8.4	Other BSPs	21
8.4.1	BSP (o): Other Information to be Associated with The Signature	21
8.4.2	BSP (p): Cryptographic Suites	21
8.4.3	BSP (q): Technological Environment	21
8.5	TECHNICAL COUNTERPARTS OF BSPS – STATEMENT SUMMARY	21
8.6	INPUT AND OUTPUT CONSTRAINTS FOR SIGNATURE CREATION, AUGMENTATION AND VALIDATION PROCEDURES	22
8.6.1	Input Constraints to be used when Generating, Augmenting and/or Validating Signatures in The Context of The Id Signature Policy	entified 22
8.6.2	Output Constraints to be Used when Validating Signatures in The Context of The Identified Signature Policy	24
8.6.3	Output Constraints to be used for Generating/Augmenting Signatures in The Context of The Identified Signature Policy .	24
9	ANNEX C: PARTIALLY DELEGATED PADES SIGNATURE REQUIREMENTS	25
9.1	BSPs Mainly Related to the Concerned Application/Business Process	25
9.1.1	BSP (a): Workflow (Sequencing and Timing) of Signatures	25
9.1.2	BSP (b): Data to be signed	25
9.1.3	BSP (c): The Relationship between Signed Data and Signature(s)	25
9.1.4	BSP (d): Targeted Community	25
9.1.5	BSP (e): Allocation of Responsibility for Signature Validation and Augmentation	25
9.2	BSPs Mainly Influenced by the Legal/Regulatory Provisions Associated to the Concerned Application/Business Process	25
9.2.1	BSP (f): Legal Type of the Signatures	25
9.2.2	BSP (g): Commitment Assumed by the Signatory	25
9.2.3	BSP (h): Level of Assurance on Timing Evidences	25
9.2.4	BSP (i): Formalities of Signing	25
9.2.5	BSP (j): Longevity and Resilience to Change	26
9.2.6	BSP (k): Archival	26
9.3	BSPs Mainly Related to the Actors Involved in Creating/Augmenting/Validating Signatures	26
9.3.1	BSP (I): Identity (and Roles/Attributes) of the Signatories	26
9.3.2	BSP (m): Level of Assurance Required for the Authentication of the Signatory	26
9.3.3	BSP (n): Signature Creation Devices	26
9.4	Other BSPs	26
9.4.1	BSP (o): Other Information to be Associated with The Signature	26
9.4.2	BSP (p): Cryptographic Suites	26
9.4.3	BSP (q): Technological Environment	26
9.5	TECHNICAL COUNTERPARTS OF BSPS – STATEMENT SUMMARY	26
9.6	INPUT AND OUTPUT CONSTRAINTS FOR SIGNATURE CREATION, AUGMENTATION AND VALIDATION PROCEDURES	27
9.6.1	Input Constraints to be used when Generating, Augmenting and/or Validating Signatures in The Context of The Ide Signature Policy	entified 27
063	Signature Folicy	، <u>۲</u>
9.0.2	Output Constraints to be used for Concerting Augmenting Signatures in The Context of The Identified Signature Policy	29 20
9.0.3	. Output constraints to be used for Generating/Augmenting Signatures in The Context of The Identified Signature Policy	29

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.

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 http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=51502
- [4] ISO 19005-1: Document Management Electronic document file format for long term preservation Part 1: Use of PDF 1.4 (PDF/A-1), 2005
 - http://www.iso.org/iso/catalogue_detail?csnumber=38920
- [5] ISO 19005-2: Document management Electronic document file format for long-term preservation Part 2: Use of ISO 32000-1 (PDF/A-2), 2011 http://www.iso.org/iso/catalogue_detail?csnumber=50655
- [6] W3C XML Signature Syntax and Processing (Second Edition), Recommendation, June 2008 https://www.w3.org/TR/xmldsig-core/
- [7] 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
- [8] 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
- [9] 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 60/en 31914202v010101p.pdf
- [10] ETSI EN 319 132-1 Electronic Signatures and Infrastructures (ESI); XAdES digital signatures, Parts 1: Building blocks and XAdES baseline signatures, April 2016 <u>http://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.01.01_60/en_31913201v010101p.pdf</u>
- [11] ETSI EN 319 132-2 Electronic Signatures and Infrastructures (ESI); XAdES digital signatures, Parts 2: Extended XAdES signatures, April 2016 <u>http://www.etsi.org/deliver/etsi_en/319100_319199/31913202/01.01.01_60/en_31913202v010101p.pdf</u>
- [12] 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_60/ts_119101v010101p.pdf
- [13] 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_06/ts_11917201v010101p.pdf
- [14] ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI);Cryptographic suites, November 2014 http://www.etsi.org/deliver/etsi_ts/119300_119399/119312/01.01.01_60/ts_119312v010101p.pdf
- [15] 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
- [16] LuxTrust Time Stamping V2 Policy, v1.7, October 2016 https://www.luxtrust.lu/en/repository
- [17] LuxTrust ORELY Portal SAML Specifications, v1.0.5, April 2016
- [18] LuxTrust ORELY Portal DSS Specifications, v1.0.3, February 2016
- [19] LuxTrust ORELY Portal Fully Delegated PAdES Specifications, v1.0.4, February 2016
- [20] LuxTrust ORELY Portal Partially Delegated XAdES Specifications, v1.0.2, February 2016
- [21] LuxTrust ORELY Portal Partially Delegated PAdES Specifications, LuxTrust, v1.1.0, April 2016
- [22] LuxTrust ORELY Portal Proprietary Attributes Definitions, v1.0.2, July 2016

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 (APPs) to authenticate physical person users (Signatories) and apply signatures to documents, with physical persons also being capable to act on behalf of a moral person based on the employed certificate in question.

LuxTrust configures ORELY services in accordance with each APP, 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 APPs 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, APP), and requirements on APP's signature policy contents, as several details depend on the actual APP's use case.



Figure 1 – Signature workflow and signature policy's scope

APPs, in Fully Delegated mode, sticking to the present signature policy shall derive their specific rules from the present policy, as shown in Figure 1 (blue area).

In Partially Delegated mode, the signature policy's scope would the APP can take more responsibilities into account (e.g. display of DTBS) which results in a modified diagram with regard to Figure 1.

1.2.2 Domain of Applications

Not applicable (unrestricted)

LuxTrust S.A.

T +352 26 68 15-1 F +352 26 68 15-789 E info@luxtrust.lu

1.2.3 Transactional Context

2.

.

The APP may 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 APP, the Signatory and LuxTrust ORELY (cf. Figure 1):

- 1. The APP 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)
 - LuxTrust ORELY interacts with the Signatory for authentication and signature generation, either
 - a. Independently of APP's interface ("fully delegated mode", cf. 3.2.4); or
 - b. Through APP's interface ("partially delegated mode").
 - Each mode implies specific requirements.
- 3. LuxTrust ORELY sends a signature response to the APP (which contains the signed document or the signed hash(es), unless an error occurred)

In this respect, LuxTrust ORELY 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 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 elDAS Regulation on electronic identification and trust services for electronic transactions [1].

The contents of this document comply with [13].

1.3.4 Distribution Points

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

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: <u>cspboard@luxtrust.lu</u>		
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

VERSION 1.1.3

1.4.3 Approval Procedures

The Policy Approval Authority within LuxTrust S.A. is the LuxTrust CSP Board. LuxTrust announces modifications of the Signature Policies in the repository as available on https://www.luxtrust.lu/en/repository prior to those policies becoming applicable.

1.5 Definitions and Acronyms

APP	Application provider		
BSP	Business	scoping parameter	
DTBS	Data to-b	e-signed	
PAdES	PDF adva	nced electronic signature	
PDF	Portable of	document format	
SCA	Signature creation application (LuxTrust ORELY, in our context)		
SP	Service provider (other name for the APP)		
TSP	Trust Service Portal		
XAdES	XML advanced electronic signature		
XML	Extensible markup language		
Augment	ation	The process of incorporating certain material (e.g. time stamps, validation data and even archival-related material) into signatures in order to make them more resilient against change or for enlarging their longevity	

Validation Data Elements that prove that the signature validation has passed or failed (certificates, OCSP responses or CRLs)

2 Signature Application Practices Statements

2.1 Requirements on Application Provider Applications

According to the Signature creation model of [7], 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, APP's application must comply with technical standards [17], [18], and depending on the use case [19] and/or [20] and/or [21] and [22] 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 [12]

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 and validation, the relevant requirements from [12] 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.

Format and working mode specific BSP's, which are described in their respective annexes, complete these BSPs:

- 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 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 S.A.	T +352 26 68 15-1	IVY Building	www.luxtrust.lu	10/29
	F +352 26 68 15-789	13-15, Parc d'activités	TVA : LU 20976985	
	E info@luxtrust.lu	L-8308 Capellen, Luxembourg	R.C.S. Luxemboura : B 112233	

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

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 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 Requirements or Annex C: Partially Delegated PAdES Signature Requirements) or any generic document format (particularly 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. LuxTrust erases all copies of the received documents, if any, from its servers once sent back (signed) to the APP.

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 [7]) are:

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

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 APP's signature policy, signatures produced by LuxTrust ORELY shall be validated based on the European trusted lists [15]. LuxTrust ORELY signatures comply with the eIDAS Regulation [1].

Nevertheless, APPs may, in accordance with LuxTrust, define additional "trust anchors" in their signature policy or exclude "trust anchors" when necessary. These trust anchors can be configured in LuxTrust ORELY and be used in trust chains and certificate validation paths for the specific APP. 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 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" (cf. 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.

This also applies to "partially delegated mode" (cf. 3.2.4), however, validation performed by LuxTrust ORELY does not cover the aspect, 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 guarantee an appropriate and complete validation.

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

Alternatively, to the validation or augmentation of signatures being performed by LuxTrust ORELY, the APP may manage these operations independently (e.g. based on a local signing library). In this case, the APP becomes solely responsible for the 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 ORELY service supports all legal types of advanced electronic signature for natural persons [1]:

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

All advanced electronic signatures are¹...

- (a) Uniquely linked to the signatory;
- (b) Capable of identifying the signatory;

F

¹ As defined in [1], art. 26.

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

3.2.2 BSP (g): Commitment Assumed by the Signatory

The APP depending on its use case defines commitment type; technically, the APP may specify the commitment type associated to the signature in its signature request to LuxTrust ORELY.

If the APP 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. Timestamping is provided by the LuxTrust Global timestamping authority [16] with the production policy in force being employed for the production service. Otherwise, the B-B signature level contains a "claimed [UTC] signing time" of the signature [7].

3.2.4 BSP (i): Formalities of Signing

Presentation of the DTBS to the Signatory is mandatory. In addition, the Signatory must be able to access the signature attributes on her/his own discretion during signing. Technically, two implementations are available, which correspond to two distinct working modes:

a) Partially Delegated Mode: APP's software shall allow the Signatory to inspect the DTBS and LuxTrust ORELY shall make the attributes of the signature accessible to the Signatory before the start of the LuxTrust ORELY signature process.

Alternatively to LuxTrust ORELY making the signature attributes accessible to the Signatory, this requirement can be addressed by the APP e.g. based on a tailoring the presentation layer. In the latter case, APP is responsible for fully addressing above-cited transparency requirements concerning the presentation layer and unobstructed access to the signatures attributes. In any event, APP shall guarantee that

- i. "the presented document shall be equal in content to the data that is signed [that is, the document sent to LuxTrust ORELY for signature, or its cryptographic hash]" [7]
- ii. the user interface conforms to [7] and [12]
- b) Fully Delegated Mode: LuxTrust ORELY 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 technical integration of LuxTrust ORELY services do not tamper with LuxTrust ORELY's presentation of the DTBS and access to the signature attributes for the Signatory.

All the following signature attributes must be accessible for visualization by the Signatory during the process:

- Signing certificate
- Signature policy identifier
- Commitment type

In addition, existing signatures in the DTBS and their validation status must be accessible for visualization by the Signatory during the process, with validation performed by LuxTrust ORELY. Alternatively, to the validation being performed by LuxTrust ORELY, the APP may perform this validation independently (e.g. based on a local signing library). In this case, the APP becomes solely responsible for the validation.

LuxTrust ORELY user interface focuses on Signatory's authentication and legal requirements on expression of will by the Signatory when her/his approval is required. The fulfillment 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 timestamping authority [16] with the production policy in force being employed for the production service. Such a timestamp is valid during at most five years, and no less than 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.

Note that a B-LT signature's longevity can further 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.

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) as long as its longevity.

3.2.6 BSP (k): Archival

The present policy has no archival requirement on the generated advanced electronic signatures. LuxTrust ORELY does not keep a copy of the generated advanced electronic 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 an advanced electronic signature is to be self-contained and not requiring additional out-of-band information for proofing its evidence.

If needed, archival of the signature is on APP'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 in order to provide evidence concerning the LuxTrust Services it provided and archived for 10 (ten) years and can be used in legal procedures.

The following evidences can be revealed from 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
- As to whether the signature request was successful

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

3.3.1 BSP (I): Identity (and Roles/Attributes) of the Signatories

The APP may provide LuxTrust ORELY with the Signatory's identity and minimum assurance level of the authentication means (cf. 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 APP's signature policy or terms of service, and implemented within APP's workflow.

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

The APP 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. However, the APP may typically employ LuxTrust ORELY 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": low, substantial and high assurance levels [2]. Additionally, LuxTrust ORELY also supports a "No/minimal" assurance level.

In any case, the APP is the sole responsible for the signature request's minimum assurance level.

As concerns the accepted "trust anchors", cf. 3.1.4.

3.3.3 BSP (n): Signature Creation Devices

LuxTrust ORELY 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 signature request.

The APP shall configure its system in accordance with LuxTrust in order 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 APP, 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.

The document [14] 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 ORELY specifications [17], [18], [19], [20], [21] and [22] specify technological constraints on the environment.

4 <u>Requirements / Statements on Technical Mechanisms and Standards</u> <u>Implementation</u>

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.

Annex A: Fully Delegated PAdES Signature Requirements 7

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

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

BSP (a): Workflow (Sequencing and Timing) of Signatures 7.1.1

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]. When the signature's level is B-B or B-T, the document should be in PDF/A-1b or PDF/A-2b format ([4] and [5]). When the signature's level is B-LT, the document should be in PDF/A-1a or PDF/A-2a format ([4] and [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 [3]. The signature format is PAdES ([8] and [9]).

BSP (d): Targeted Community 7.1.4

No further requirement from 3.1.4

Note 1: When an APP defines specific trust anchors (cf. 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 APP's signature policy. Therefore, that software may validate or reject electronic signatures that would be rejected or validated respectively by LuxTrust ORELY's or APP's signature policies.

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

No further requirement from 3.1.5; in particular, ORELY implicitly validates pre-existing signatures and shows the results to the signatory, who may voluntary abstain from signing (CANCEL), but ORELY never impedes the signing process. In this respect, repeated (serial) signatures requests (cf. [19]) are essentially technical and do not depend on the existing signatures' validity.

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

7.2.1 BSP (f): Legal Type of the Signatures

No further requirement from 3.2.1

7.2.2 BSP (g): Commitment Assumed by the Signatory

No further requirement from 3.2.2

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

No further requirement from 3.2.3

BSP (i): Formalities of Signing 7.2.4

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

7.2.5 BSP (j): Longevity and Resilience to Change

F

No further requirement from 3.2.5

7.2.6 BSP (k): Archival

No further requirement from 3.2.6

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

7.3.1 BSP (I): Identity (and Roles/Attributes) of the Signatories

No further requirement from 3.3.1

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

No further requirement from 3.3.2

7.3.3 BSP (n): Signature Creation Devices

No further requirement from 3.3.3

7.4 Other BSPs

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

No further requirement from 3.4.1

7.4.2 BSP (p): Cryptographic Suites

No further requirement from 3.4.2

7.4.3 BSP (q): Technological Environment

No further requirement from 3.4.3

Technical Counterparts of BSPs – Statement Summary 7.5

Table 7.1 : Signature Policy Statement Summary

Name and identifier of the signature policy authority: LuxTrust S.A. IVY Building 13-15, Parc d'Activités L-8308 Capellen Name and identifier of the signature policy: LuxTrust Fully Delegated PAdES Signature Policy (1.3.171.1.4.1.1.1)

BSP	BSP title	Business statement summary	Technical statement
(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	[8] and [9]
(c)	Relationship between DTBS & signature(s)	Defined by the APP among the following signature levels: 1) basic signature 2) signature with time 3) signature with long-term validation data PAdES signatures are enveloped	Signature levels from [7]
(d)	Targeted community	Any entity that shall be or that choses to be compliant with the eIDAS Regulation	Signature format
(e)	Allocation of responsibility for signature validation and augmentation	Managed by the APP, if required, otherwise managed by ORELY	LuxTrust ORELY based on provisions made by APP as indicated in 7.1.5 and 3.1.5
(f)	Legal type of signature	 (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 signature request [17] ([Signature] 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	<i>Fully Delegated Mode</i> (3.2.4) is the only supported mode.	LuxTrust ORELY servers responsibility and implementation

т

VERSION 1.1.3

BSP	BSP title	Business statement summary	Technical statement	
			counterpart	
(j)	Longevity & resilience to change	Signing's certificate or timestamp's duration, whichever is higher	Ditto	
(k)	Archival	No requirement		
(I)	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 assurance levels [2].	 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		
(p)	Cryptographic suites	State-of-art cryptographic suites	Cryptographic libraries	
(q) Technological environment		Cf. LuxTrust specifications [17], [18], [19] and [22]	LuxTrust implementation	
Signa state	ture creation/validation application practices ments	-	-	

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: LuxTrust S.A. IVY Building 13-15, Parc d'Activités L-8308 Capellen

Name and identifier of the signature policy: LuxTrust Fully Delegated PAdES Signature Policy (1.3.171.1.4.1.1.1)

		Business statement	Technical counterpart	
BSP	BSP title	summary	statement	Constraint value at signature creation (SCA or APP)
(a)	Workflow	Workflow is defined by	Multiple PAdES	APP constraints : OrderInSequence: (APP-defined)
	(sequencing &	the APP	signatures are	SCA constraints : SequencingNature: Mandated-serial
	timing)		necessarily serial	
		Defined by the APP	Signature levels from [7]	SCA constraints TimingRelevance:
		among the following		TimingRelevanceOnEvidence:
		signature levels:		1) MandatedSignedQProperties-signing-time
		1) basic signature		2) MandatedUnsignedQProperties-signature-time-stamp
		2) Signature with		3) Manualeu Onsigneu QProperties-signature-time-stamp
		5) Signature with		
		validation data		
		Validation data		APP constraints : MassSigningAcceptable : no
(b)	Data to be signed	Format: PDF	[8] and [9]	APP constraints :
(~)	Pata to be digited		[0] unu [0]	ConstraintOnDTBS : PDF
				DOTBSAsAWholeOrInParts:whole
(c)	The relationship	Defined by the APP	Signature levels from [7]	APP constraints :
	between signed	among the following		 SignatureRelativePosition:envelopped
	data and	signature levels:		1) MandatedSignatureFormat:B-B
	signature(s)	1) basic signature		MandatedSignatureFormat:B-T
		2) signature with time		MandatedSignatureFormat:B-LT
		signature with		
		long-term		
		validation data		
(d)	Targeted	Any entity that shall be	Use of PAdES format	None
	community	or that choses to be		
		compliant with the		
		eIDAS Regulation		

17/29

VERSION 1.1.3

		Business statement	Technical counterpart	
BSP	BSP title	summary	statement	Constraint value at signature creation (SCA or APP)
(e)	Allocation of responsibility for signature validation and augmentation	Managed by the APP, if required, otherwise managed by ORELY	LuxTrust ORELY based on provisions made by APP as indicated in 7.1.5 and 3.1.5	SCA: ValidationRequiredBeforeAugmenting:yes
(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 signature request [17] ([Signature] QAA level, TSP-Type and TSP-ID)	 APP constraints: ConstraintsOnCertificateMetadata: LegalPersonSignerRequired: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 signature request	 APP constraint: CommitmentTypesRequired: MandatedSignedQProperties-commitment-type- indication:no SCA constraint: CommitmentTypesRequired: MandatedSignedQProperties-commitment-type- indication:yes
(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	Fully delegated mode	LuxTrust ORELY servers responsibility and implementation	SCA & APP constraints: • WYSIWYSRequired:yes • WYSIWHBSRequired:yes • ProperAdviceAndInformationRequired:yes • UserInterfaceDesignConstraints:yes • CorrectValidationAndArchivalProcedures:no
(j)	Longevity and resilience to change	Signing's certificate or timestamp's duration, whichever is higher	Ditto	(none)
(k)	Archival	No requirement		(none)
(I)	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 assurance levels [2].	 Corresponding signature request's parameter Specific trust anchors configuration 	 SCA constraints: X509CertificateValidationConstraints:SetOfTrustAnchor s:(APP-defined² or EU Trusted List)
(n)	Signature creation devices	(Optionally defined by the APP among the LuxTrust supported devices)	Signature request's parameters	
(0)	Other information to be associated with the signature	No requirement		

 $^2\,\mathrm{APP}\text{-}\mathrm{defined}$ requires a specific signature policy

18/29

VERSION 1.1.3

BSP	BSP title	Business statement summary	Technical counterpart statement	Constraint value at signature creation (SCA or APP)
(p)	Cryptographic	State-of-art	Cryptographic libraries	Cf. [14] for cryptographic constraints reference
-	Suites	cryptogruphic suites		
(q)	Technological	LuxTrust specifications	LuxTrust implementation	(none)
	environment	[17], [18], [19] and [22]		

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. [20] for implementation details)

Other variants are not supported.

8.1.2 BSP (b): Data to be signed

The data to be signed is either [20]:

- Any MIME-type/format and number of documents, technically represented as an XML <dsig:Manifest> element ([6]), 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 ([10] and [11]). 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 from 3.1.4

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

No further requirement from 3.1.5; in particular, ORELY or the APP implicitly validates pre-existing signatures and shows the results to the signatory, who may voluntary abstain from signing (CANCEL), but ORELY never impedes the signing process. In this respect, XML countersignatures requests ([20]) are essentially technical and do not depend on the countersigned signatures' validity.

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 from 3.2.1

8.2.2 BSP (g): Commitment Assumed by the Signatory

No further requirement from 3.2.2

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

No further requirement from 3.2.3

8.2.4 BSP (i): Formalities of Signing

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

The APP is responsible for the presentation, in a readable format, of the signed data. 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 takes the option to present the signature attributes, the APP takes full responsibility for this particular aspect and the requirement to satisfy all needs indicated in 3.2.4.

8.2.5 BSP (j): Longevity and Resilience to Change

No further requirement from 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.

Lux]	Frust	SA
		0.0.0

8.2.6 BSP (k): Archival

No further requirement from 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 (I): Identity (and Roles/Attributes) of the Signatories

No further requirement from 3.3.1

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

No further requirement from 3.3.2

8.3.3 BSP (n): Signature Creation Devices

No further requirement from 3.3.3

8.4 Other BSPs

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

No further requirement from 3.4.1

8.4.2 BSP (p): Cryptographic Suites

No further requirement from 3.4.2

8.4.3 BSP (q): Technological Environment

No further requirement from 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: LuxTrust S.A. IVY Building 13-15, Parc d'Activités L-8308 Capellen Name and identifier of the signature policy: LuxTrust Partially Delegated XAdES Signature Policy (1.3.171.1.4.1.2.1)

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
(b)	Data to be signed (DTBS)	 Any MIME-type/format and number of document hashes, technically represented as an XML <dsig:manifest> element OR</dsig:manifest> A single XML detached XAdES signature (countersigning) 	[6], [10] and [11]
(c)	Relationship between DTBS & signature(s)	Defined by the APP among the following signature levels: 1) basic signature 2) signature with time 3) signature with long-term validation data The signature is an XML detached signature, and the signature format is XAdES ([10] and [11]).	Signature levels from [7]
(d)	Targeted community	Any entity that shall be or that choses to be compliant with the eIDAS Regulation	Signature format

VERSION 1.1.3

BSP	BSP title	Business statement summary	Technical statement
(e)	Allocation of responsibility for signature validation and augmentation	Managed by the APP, if required, otherwise managed by ORELY	LuxTrust ORELY based on provisions made by APP as indicated in 8.1.5 and 3.1.5
(f)	Legal type of signature	 (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 signature request [17] ([Signature] 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 Delegated Mode (3.2.4) is the only supported mode.	APP's responsibility and implementation for DTBS; LuxTrust ORELY or alternatively APP enables signature attributes visualization, with the enabling party becoming solely responsible for providing correct and full transparency
(j)	Longevity & resilience to change	Signing's certificate or timestamp's duration, whichever is higher	Ditto
(k)	Archival	No requirement	
(I)	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 assurance levels [2].	 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	
(n)	Cryptographic suites	State-of-art cryptographic suites	Cryptographic libraries
(q)	Technological environment	Cf. LuxTrust specifications [17], [18], [20] and [22]	LuxTrust implementation
Signatur practice	e creation/validation application s 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:	
LuxTrust S.A.	
IVY Building	
13-15, Parc d'Activités	
L-8308 Capellen	
Name and identifier of the signature policy: LuxTrust Partially Delegated XAdES Signature Policy (1.3.171.1.4.1.2.1)	

VERSION 1.1.3

DCD.		Business statement	Technical counterpart	
BSP (2)	BSP title	summary Workflow is defined by	statement	Constraint value at signature creation (SCA or APP)
(d)		the APP_XAdES_detached		Mandated Unsigned OProperties-counter-signature
	timing)	signatures under the	Signatures	(countersignature)
		present profile may		
		cover multiple		
		countersignatures		
		depending on APP's		
		workflow.		
		Defined by the APP	Signature levels from [7]	SCA constraints TimingRelevance:
		among the following		TimingRelevanceOnEvidence:
		signature ieveis:		1) MandatedSignedQProperties-signing-time
		 Dusic signature signature with time 		2) Manualed Onsigned QProperties-signature-time-stamp 3) Mandated Insigned OProperties-signature-time-stamp
		3) signature with		sy manuacedons.Brieder roperties signature time stamp
		long-term		
		validation data		
				APP constraints : MassSigningAcceptable : no
(b)	Data to be signed	Any MIME-	[6], [10] and [11]	APP constraints :
		type/format		DOTBSAsAWholeOrInParts:whole
		of		SCA constraints:
		documents.		ContentRelatedConstraintsAsPartOfSignatureElements:
		technically		MandatedSignedQProperties-DataObjetFormat
		represented		([20], 5.3.3.15)
		as an XML		
		<dsig:manifes< td=""><td></td><td></td></dsig:manifes<>		
		t> element		
		UR A single XMI		
		- A Siliyie XiviL detached		
		XAdES		
		signature		
		(countersigni		
		ng)		
(c)	The relationship	Defined by the APP	Signature levels from [7]	APP constraints :
	data and	signature levels:		SignatureRelativePosition:envelopped MandatodSignatureFormat: P. P.
	signature(s)	1) basic signature		2) MandatedSignatureFormat:B-T
	8	2) signature with time		3) MandatedSignatureFormat:B-LT
		3) signature with		
		long-term		SCA Constraints:
		validation data		SignatureRelativePosition:detached
(d)	Targeted	Any entity that shall be	Use of XAdES format	None
	community	or that choses to be		
		eIDAS Regulation		
(e)	Allocation of	Managed by the APP, if	LuxTrust ORELY based on	SCA: ValidationRequiredBeforeAugmenting:yes
	responsibility for	required, otherwise	provisions made by APP	
	signature	managed by ORELY	as indicated in 8.1.5 and	
	validation and		3.1.5	
10	augmentation			
(†)	Legal type of the	(defined by the APP to	Parameters in the	APP constraints:
	Signatures		([Sianature] OAA level	ConstraintsOnceruncateivietadata: LegalPersonSignerRequired:no
		1. Qualified	TSP-Type and TSP-ID)	LegalPersonSignerAllowed:ves
		sianatures	,, ,	EUQualifiedCertificateRequired: (APP-defined:
) Advanced		yes/no)
		2. Advancea		EUSSCDRequired: (APP-defined: yes/no)
		sianatures		EUAdESigRequired:yes
		supported by		
		a qualified		
		certificate;		
		3. Advanced		
		electronic		
		signatures)		

VERSION 1.1.3

		Business statement	Technical counterpart	
BSP	BSP title	summary	statement	Constraint value at signature creation (SCA or APP)
(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
(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 delegated mode	APP's responsibility and implementation for DTBS; LuxTrust ORELY or alternatively APP enables signature attributes visualization, with the enabling party becoming solely responsible for providing correct and full transparency	 SCA & APP constraints: WYSIWYSRequired:yes WYSIWHBSRequired:yes ProperAdviceAndInformationRequired:yes UserInterfaceDesignConstraints:yes CorrectValidationAndArchivalProcedures:no
(j)	Longevity and resilience to change	Signing's certificate or timestamp's duration, whichever is higher	Ditto	(none)
(k)	Archival	No requirement		(none)
(I)	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 assurance levels [2].	 Corresponding signature request's parameter Specific trust anchors configuration 	 SCA constraints: X509CertificateValidationConstraints:SetOfTrustAnchors :(APP-defined³ or EU Trusted List)
(n)	Signature creation devices	(Optionally defined by the APP among the LuxTrust supported devices)	Signature request's parameters	
(0)	Other information to be associated with the signature	No requirement		
(p)	Cryptographic suites	State-of-art cryptographic suites	Cryptographic libraries	Cf. [14] for cryptographic constraints reference
(q)	Technological environment	LuxTrust specifications [17], [18], [20] and [22]	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

 $^{^{3}\,\}mathrm{APP}\text{-defined}$ 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].

When the signature's level is B-B or B-T, the document should be in PDF/A-1b or PDF/A-2b format or any format that ensures the "long-term preservation" of the "visual appearance" of the document ([4] or [5]).

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].

The signature format is PAdES ([8] and [9]).

9.1.4 BSP (d): Targeted Community

No further requirement from 3.1.4

Note 1: When an APP defines specific trust anchors (cf. 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 APP's signature policy. Therefore, that software may validate or reject electronic signatures that would be rejected or validated respectively by LuxTrust ORELY's or APP's signature policies.

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

No further requirement from 3.1.5; in particular, ORELY or the APP shall validate pre-existing signatures and shall show the results to the signatory, who may voluntary abstain from signing (CANCEL), but ORELY never impedes the signing process. 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 document⁴.

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 from 3.2.1

9.2.2 BSP (g): Commitment Assumed by the Signatory

No further requirement from 3.2.2

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

No further requirement from 3.2.3

9.2.4 BSP (i): Formalities of Signing

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

The APP is responsible for the faithful presentation of the PDF to be-signed to the signatory.

If the APP takes the option to present the signature attributes, the APP takes full responsibility for this particular aspect and the requirement to satisfy all needs indicated in 3.2.4.

⁴ The process can be supported by software that may be optionally provided for the APP environment. However, such a support when applicable does NOT free the APP from the obligation to handle preparation and request of signature augmentation.

9.2.5 BSP (j): Longevity and Resilience to Change

No further requirement from 3.2.5

9.2.6 BSP (k): Archival

No further requirement from 3.2.6

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

9.3.1 BSP (I): Identity (and Roles/Attributes) of the Signatories

No further requirement from 3.3.1

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

No further requirement from 3.3.2

9.3.3 BSP (n): Signature Creation Devices

No further requirement from 3.3.3

9.4 Other BSPs

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

No further requirement from 3.4.1

9.4.2 BSP (p): Cryptographic Suites

No further requirement from 3.4.2

9.4.3 BSP (q): Technological Environment

No further requirement from 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: LuxTrust S.A. IVY Building 13-15, Parc d'Activités L-8308 Capellen Name and identifier of the signature policy: LuxTrust Partially Delegated PAdES Signature Policy (1.3.171.1.4.1.3.1)

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	[8] and [9]
(c)	Relationship between DTBS & signature(s)	 Defined by the APP among the following signature levels: 1) basic signature 2) signature with time 3) signature with long-term validation data PDF signatures are enveloped. 	Signature levels from [7]
(d)	Targeted community	Any entity that shall be or that choses to be compliant with the eIDAS Regulation	Signature format
(e)	Allocation of responsibility for signature validation and augmentation	Managed by the APP, if required, otherwise managed by ORELY	LuxTrust ORELY based on provisions made by APP as indicated in 9.1.5 and 3.1.5

VERSION 1.1.3

BSP	BSP title	Business statement summary	Technical statement
(6)	Legel turne of signature	(defined by the ADD to be one of the level	counterpart
(1)	Legal type of signature	(defined by the APP to be one of the legal types:	request [17] ([Signature]
		types.	OAA level, TSP-Type and TSP-
		1. Qualifiea electronic signatures;	ID)
		2. Advanced electronic signatures	
		supportea by a qualified	
		2 Advanced electronic signatures)	
		3. Advanced electronic signatures)	
(g)	Commitment assumed by the	"proof of approval" unless defined by the	Commitment-type attribute
	Signatory	AFF	apperated signatures
			It is an ontional parameter
			of the signature request
(h)	Level of assurance on timing	Claimed by signatory for the basic level,	LuxTrust Global
	evidences	timestamp for higher levels	timestamping authority,
			when applicable
(i)	Formalities of signing	Partially Delegated Mode (3.2.4) is the only	APP's responsibility and
		supported mode.	implementation for DTBS;
			LuxTrust ORELY or
			diternatively APP enables
			signature attributes
			enablina party becomina
			solely responsible for
			providing correct and full
			transparency
(j)	Longevity & resilience to change	Signing's certificate or timestamp's duration,	Ditto
		whichever is higher	
(k)	Archival	No requirement	
(1)	Identity of Signatories	No requirement	
(m)	Level of assurance required for the	(Uptionally defined by the APP)	Corresponding
	authentication of the Signatory.	the eIDAS levels for "electronic identification	signature request s
		means": low substantial and high assurance	 Specific trust anchors
		levels [2].	configuration
(n)	Signature creation devices	(Optionally defined by the APP among the	Signature request's
	0	LuxTrust supported devices)	parameters
(o)	Other information to be associated	No requirement	
	with the signature		
(p)	Cryptographic suites	State-of-art cryptographic suites	Cryptographic libraries
(q)	Technological environment	Cf. LuxTrust specifications [17], [18], [21] and	LuxTrust implementation
		[22]	
Signatu	re creation/validation application	-	-
practice	es 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:			
LuxTrust S.A.			
IVY Building			
.3-15, Parc d'Activités			
L-8308 Capellen			
Name and identifier of the signature policy: LuxTrust Partially Delegated PAdES Signature Policy (1.3.171.1.4.1.3.1)			
Identifier of the concerned signature(s) in the concerned signature workflow: (only applicable for the APP)			

VERSION 1.1.3

Ess Description Statement Outstant value at 2016 Outstant value at 2016 <th>DCD</th> <th></th> <th>Business statement</th> <th>Technical counterpart</th> <th></th>	DCD		Business statement	Technical counterpart	
(c) The APP Signatures are necessarily serial SCA Constraints : Sequencing Nature: Mandated-serial (c) Defined by the APP Signature levels from [7] SCA constraints : Sequencing Nature: Mandated-serial (c) Signature levels 1) basics signature SCA constraints : Sequencing Nature: Mandated-serial (c) Signature levels 1) basics signature SCA constraints : Mandated/SignedQProperties signature-time-stamp (b) Data to be signed Format: PDF [8] and [9] APP constraints : (c) The relationship Defined by the APP Signature levels from [7] APP constraints : (c) The relationship Defined by the APP Signature levels from [7] APP constraints : (d) Targeted community Signature with time Signature levels from [7] APP constraints : (d) Targeted community Any entity that shall be or that chaes to be complaint with the elDAS sequenties Signature with ime Signature setting sequenties (f) Legal type of the signature signatures sisphorted by a q adplified certificated fined:<	(a)	Workflow	Summary Workflow is defined by	Statement Multiple PAdFS	APP constraints : OrderInSequence: (APP-defined)
timing) iserad serad iming) iserad serad iming) iserador signature iming belowand signature levels: iming belowand iming belowand signature with ime iming belowand iming belowand format: PDF [8] and [9] APP constraints: (c) The relationship Defined by the APP signature levels from [7] APP constraints: (c) The relationship Defined by the APP signature levels from [7] APP constraints: (d) Targeted Any entity that shall be image by APA signature levels format (d) Targeted Any entity that shall be image by APA signature request [17] (f) Legal type of the (defined by the APP, if required, otherwise signature request [17] (f) Legal type of the (defined by the APP, if required, otherwise Parameters in the ignature signature signature signature signature (f) Legal type of the (defined by the AP	(u)	(sequencing &	the APP	signatures are necessarily	SCA constraints : SequencingNature: Mandated-serial
Image: Second Status Signature levels: Signature levels: Signature levels: 1 basis signature levels: Nandated/unsignedQProperties-signing-time 2) signature with time Nandated/UnsignedQProperties-signing-time 3) signature with time Nandated/UnsignedQProperties-signature-time-stamp (b) Data to be signed Format: PDF [8] and [9] APP constraints : MassSigningAcceptable : no (c) The relationship Defined by the APP [8] and [9] APP constraints : (c) The relationship Defined by the APP Signature levels from [7] APP constraints : (c) The relationship Defined by the APP Signature levels from [7] APP constraints : (c) Targeted Any entity that shall be Signature levels from [7] NandatedSignatureFormat:B-T 3) signature with hoggeterm validation data Use of PAdES format None (c) Targeted Any entity that shall be Use of PAdES format None (f) Legal type of the signatures Indicated in 9.1.5 and 3.1.5 ConstraintSOnCertificateMetadata:		timing)	Define the the ADD	serial	
(d) Targeted community 2 signature levels: 1) MandatedSignedQProperties-signing-time (d) Targeted community Format: PDF [8] and [9] APP constraints : AssSignatureFormat: PDF (d) Targeted community Defined by the APP signature elvels from [7] APP constraints : APP constraints : (d) Targeted community Defined by the APP, if signature elvels from [7] APA constraints : APP constraints : (f) Lageted community NandatedSignatureFormat: B-1 3) MandatedSignatureFormat: B-1 (d) Targeted community None Version and by APP ar indication and augmentation LuxTrust ORELY based on provisions made by APP ar indicated in 9.1.5 and 3.1.5 None (f) Legal type of the signatures (defined by the APP to signatures; LuxTrust ORELY based on provisions made by APP ar indicated in 9.1.5 and 3.1.5 None (f) Legal type of the signatures; AAPP constraints: APP constraints: (f) Legal type of the signatures; Advanced electronic signatures; Parameters in the signatures; AAPP constraints: (f) Legal type of the signatures; Advanced electronic signatures; Parameters in the signatures; ConstraintSonCert			Defined by the APP amona the followina	Signature levels from [7]	TimingRelevanceOnEvidence:
(b) Data to be signed Format: PDF [B] and [9] APP constraints : MassSigningAcceptable : no (b) Data to be signed Format: PDF [B] and [9] APP constraints : MassSigningAcceptable : no (c) The relationship between signed Defined by the APP (Signature evels) from [7] APP constraints : ConstraintONTBS : PDF (c) The relationship between signed Defined by the APP (Signature evels) from [7] APP constraints : ConstraintSonTheNumberOfDOTBS-1 (c) The relationship between signature (Signature evels) from [7] Signature levels from [7] APP constraints : (d) Targeted community 2 isgnature with time 3 isgnature evels from [7] MandatedSignatureFormat-B-8 2) (e) Allocation of required, otherwise managed by the APP (SignatureFormat-B-1 3) MandatedSignatureFormat-B-1 3) (f) Legal type of the signature Any entity that shall be compliant with the electronic signature; LuxTrust ORELY based on augmentation None (f) Legal type of the signatures; I. Advanced electronic signature; Andered by the APP to signature; ConstraintSOCertificateMetadata: LegalPersonSigneRequived.no (f) Legal type of the signatures; I. Advanced Parometers in t			signature levels:		1) MandatedSignedQProperties-signing-time
(b) Data to be signed Format: PDF [8] and [9] APP constraints : MassSigningAcceptable : no (b) Data to be signed Format: PDF [8] and [9] APP constraints : (c) between signed data and signature[s] Defined by the APP among the following signature levels: Signature levels from [7] APP constraints : (c) between signed data and Defined by the APP among the following signature levels: Signature levels from [7] APP constraints : (c) The relationship data and Defined by the APP among the following signature levels: Signature levels from [7] APP constraints : (d) Targeted community Any entity that shall be or that choses to be compliant with the eIOAS Regulation Use of PAdES format noged by ORELY None (f) Legal type of the signatures (defined by the APP to responsibility for signatures LuxTrust ORELY based on required, otherwise managed by ORELY None (f) Legal type of the signatures (defined by the APP to responsibility for signatures LuxTrust ORELY based on required, otherwise managed by ORELY None (f) Legal type of the signatures (defined by the APP to responsibility for signatures Signature request [12] (Signatures APP constraints: (f) Legali			1) basic signature		2) MandatedUnsignedQProperties-signature-time-stamp
(b) 5) 5) 5) 5) 100, Eterm validation data (b) Data to be signed Format: PDF [B] and [9] APP constraints : MassSigningAcceptable : no (b) Data to be signed Format: PDF [B] and [9] APP constraints : (c) The relationship between signed data and signature(s) Defined by the APP signature with long-term validation data Signature levels from [7] APP constraints : (d) Targeted community community signature validation and augmentation Any entity that shall be compliant with the elDAS Regulation Use of PAdES format provisions made by APP provisions made by APP provisions made by APP provisions made by APP provisions made by APP signatures None (f) Legal type of the signatures (defined by the APP to be on of the legal types; 2. LuxTrust ORELY based on provisions made by APP provisions made by A			 2) signature with time 3) signature with 		3) MandatedUnsignedQProperties-signature-time-stamp
validation data APP constraints : MassSigningAcceptable : no (b) Data to be signed Format: PDF [8] and [9] APP constraints : COnstraints : (c) The relationship between signed data and signature(s) Defined by the APP among the following signature levels: Signature levels from [7] among the following signature levels: APP constraints : CONStraintsOnTheNumberOfDOTBS=1 (d) Targeted community 1) basic signature 2) Signature with time signature with time dord the community Use of PAdES format None (e) Allocation of responsibility for signatures Any entity that shall be compliant with the elDAS Regulation augmentation Use of PAdES format signature equest [17] None (f) Legal type of the signatures (defined by the APP to be one of the legal types: signatures; Parameters in the signature equest [17] APP constraints: CONStraintsOnCertificateMetadata: (ESOTONE Allocation of responsibility for signatures; APP constraintsOnCertificateMetadata: (ESOTONE Allocation and augmentation APP constraints: Commitment "provide allocated in 9.1.5 and 3.1.5 (f) Legal type of the signatures (defined by the APP to be one of the legal types: signatures; Parameters in the signature equest [17] APP constraints: Signatures ConstraintsOnCertif			long-term		
(b) Data to be signed Format: PDF [B] and [9] APP constraints: MassigningAcceptable: no (b) Data to be signed Format: PDF [B] and [9] APP constraints: i ConstraintOnDTBS: PDF (c) The relationship between signed data and signature(s) Defined by the APP among the following signature levels: Signature levels from [7] APP constraints: i ConstraintS: OnTheNumberOfDOTBS=1 (d) Targeted community An y entity that shall be or that choeses to be compliant with the eIDAS Regulation Use of PAdES format None (e) Allocation of responsibility for signatures Mandaged by the APP to be one of the legal type: signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signatures; signature			validation data		
(i) Data to be signed Formula FD Formula FD Formula FD (i) The relationship Defined by the APP among the following Signature levels from [7] APP constraints0nTheNumberOfDOTBS=1 (ii) between signed ata and signature levels: I) bis: signature with time Signature levels from [7] APP constraints0nTheNumberOfDOTBS=1 (iii) J) bis: signature Signature with time Signature levels from [7] MandatedSignatureFormat:B-B MandatedSignatureFormat:B-T (iii) Targeted Any entity thot shall be Use of PAdES format None (e) Allocation of responsibility for signature or that choses to be compliant with the eluDAS Regulation LuxTrust ORELY based on provisions made by APP as indicated in 9.1.5 and 3.1.5 None (f) Legal type of the signatures (defined by the APP to be one of the legal types: Parometers in the signature signature signature signature signatures; Avanced electronic signatures; EUAS Regulified certificate; EUAS Regulified certificate; EUAS Regulified certificate; E	(b)	Data to be signed	Format: PDF	[8] and [0]	APP constraints : MassSigningAcceptable : no
(c) The relationship between signed data and signature(s) Defined by the APP among the following signature levels: 1) Signature levels from [7] bosic signature APP constraints: Constraints: 1) APP constraints: Constraints: 1) Constraints: 2) Signature with line all data data disignature format: 1) Signature with line all data data disignature format: 1) Signature with line all data data disignature format: 1) NandatedSignature format: 1) NandatedSignature format: 2) None (d) Targeted community Any entity that shall be or that choses to be compliant with the eIDAS Regulation Use of PAdES format None (e) Allocation of responsibility for signature validation and augmentation IuxTrust ORELY based on provisions made by APP as indicated in 9.1.5 and 3.1.5 None (f) Legal type of the signatures; (defined by the APP, if to bon of the legal types; Parameters in the signature signature; Parameters in the signature request [17] ((Signature] QAA level, TSP-Type and TSP-ID) • Constraints: • Constraints: (f) Legal type of the signatures; 1. Qualified electronic signatures; Parameters in the	(6)	Data to be signed	ronnat. r Di	[0] unu [0]	ConstraintOnDTBS : PDF
(c) The relationship between signed data and signature (s) Defined by the APP among the following signature levels: Signature levels from [7] APP constraints : • ConstraintsOnTheNumberOfDOTBS=1 (d) Targeted community Any entity that shall be or that choses to be compliant with the eIDAS Regulation Use of PAdES format None (e) Allocation of responsibility for signatures Angenetity that shall be or that choses to be compliant with the eIDAS Regulation Use of PAdES format None (f) Legal type of the signatures (defined by the APP to be one of the legal types; signatures; LuxTrust ORELY based on provisions made by APP as indicated in 9.1.5 and 3.1.5 None (f) Legal type of the signatures (defined by the APP to be one of the legal types; signatures; Parameters in the signatures; APP constraints: • ConstraintsOnCertificateMetadata: ([Signature] QAA level, TSP-Type and TSP-ID] (g) Commitment * Advanced electronic signatures; Parameters in the signatures; • ConstraintsOnCertificateMetadata: ([Signature] QAA level, rSP-Type and TSP-ID] (g) Commitment * Advanced electronic signatures; • Constraints (g) Commitment * proof of opproval" Commitment-type					DOTBSAsAWholeOrInParts:whole
data and signature (s) ata and signature levels: 1) becover signature signature levels: 1) - ConstraintsOn (Enclument-type SignaturePosition:encluped 1) - (d) Targeted community Any entity that shall be compliant with the elDAS Regulation Use of PAdES format None (e) Allocation of responsibility for signatures Managed by the APP, if required, otherwise managed by ORELY signatures; LuxTrust ORELY based on provisions made by APP a sindicated in 9.1.5 and 3.1.5 None (f) Legal type of the signatures (defined by the APP to be one of the legal types: 1. Qualified electronic signatures; Parameters in the signatures; APP constraints: • ConstraintSOnCertificateMetadata: (ISignatures; 2. Advanced electronic signatures; APP constraints: • ConstraintSOnCertificateMetadata: (LegalPersonSignerAllowed:yes EUQualifiedCertificateRequired: (APP-defined: yes/no) EUSSCDRequired: (APP-defined: yes/no) EUAdESigRequired:yes (g) Commitment "proof of approval" Commitment-type APP constraint:	(c)	The relationship	Defined by the APP	Signature levels from [7]	APP constraints :
signature(s) 1 basic signature 1 MandatedSignatureFormattB-B 2) signature with time 3) signature with time 3) MandatedSignatureFormattB-T 3) MandatedSignatureFormattB-T 3) MandatedSignatureFormattB-T 3) (d) Targeted community Any entity that shall be or that choses to be compliant with the elDAS Regulation Use of PAdES format None (e) Allocation of responsibility for signature validation and augmentation Managed by the APP, if required, otherwise managed by ORELY LuxTrust ORELY based on provisions made by APP as indicated in 9.1.5 and 3.1.5 None (f) Legal type of the signatures (defined by the APP to be one of the legal types: signatures; Parameters in the electronic signatures; APP constraints: • ConstraintsOnCertificateMetadata: LegalPersonSignerRequired:no LegalPersonSignerRequired: (APP-defined: yes/no) 2. Advanced electronic signatures 2. Advanced electronic signatures EUAdESigRequired: yes/no) EUAdESigRequired: yes/no) (g) Commitment "proof of approval" Commitment-type APP constraint:		data and	signature levels:		ConstraintsOn i neivumberotDO i BS=1 SignatureRelativePosition:envelopped
(d) Targeted community Any entity that shall be or that choses to be compliant with the eIDAS Regulation Use of PAdES format Use of PAdES format None (e) Allocation of required, otherwise validation and augmentation MandatedSignatureFormat:B-LT None (f) Legal type of the signature MandatedSignatureFormat:B-LT None (f) Legal type of the signatures MandatedSignatureFormat:B-LT None (f) Legal type of the signatures (defined by the APP to be one of the legal types: signatures Parameters in the be one of the legal types: signatures APP constraints: (Signature?QAA level, TSP-Type and TSP-ID) APP constraints: LegalPersonSignerRequired: (APP-defined: yes/no) EUSCDRequired: (APP-defined: yes/no) EUSCDRequired: (APP-defined: yes/no) EUAdESigRequired: yes/ a qualified certificate; (g) Commitment "proof of approval" Commitment-type APP constraint:		signature(s)	1) basic signature		1) MandatedSignatureFormat:B-B
(d) Targeted community Any entity that shall be or that choses to be compliant with the elDAS Regulation Use of PAdES format None (e) Allocation of responsibility for signature validation and augmentation Managed by the APP, if required, otherwise managed by ORELY LuxTrust ORELY based on provisions made by APP as indicated in 9.1.5 and 3.1.5 None (f) Legal type of the signatures (defined by the APP to be one of the legal types: signatures; Parameters in the signature (Signature) signatures; APP constraints: 1. Qualified electronic signatures; 1. Qualified electronic signatures; Formaters in the signatures; APP constraints: 2. Advanced electronic signatures; 1. Qualified certificate; Formaters; • 3. Advanced electronic signatures; 3. Advanced electronic signatures; • Commitment-type (g) Commitment "proof of approval" Commitment-type APP constraint:			2) signature with time		2) MandatedSignatureFormat:B-T
(d) Targeted community Any entity that shall be or that choses to be compliant with the eIDAS Regulation Use of PAdES format None (e) Allocation of responsibility for signature validation and augmentation Managed by the APP, if required, otherwise managed by ORELY LuxTrust ORELY based on provisions made by APP as indicated in 9.1.5 and 3.1.5 None (f) Legal type of the signatures (defined by the APP to be one of the legal types: 1. Qualified electronic signatures; Parameters in the signatures APP constraints: • ConstraintsOnCertificateMetadata: LegalPersonSignerRequired: (APP-defined: yes/no) (f) Legal type of the signatures 2. Advanced electronic signatures; Parameters in the signatures APP constraints: 1. Qualified certificate; 2. Advanced electronic signatures EUQualifiedCertificateRequired: (APP-defined: yes/no) 2. Advanced electronic signatures 3. Advanced electronic signatures EUAdESigRequired: yes/no) 3. Advanced electronic signatures S. Advanced electronic signatures APP constraint:			3) Signature with Iona-term		3) MandatedSignatureFormat:B-LT
(d) Targeted community Any entity that shall be or that choses to be compliant with the eIDAS Regulation Use of PAdES format None (e) Allocation of responsibility for signature validation and augmentation Managed by the APP, if required, otherwise managed by ORELY LuxTrust ORELY based on provisions made by APP as indicated in 9.1.5 and 3.1.5 None (f) Legal type of the signatures (defined by the APP to be one of the legal types: 1. Qualified electronic signatures; Parameters in the signatures; APP constraints: (ISignature] QAA level, TSP-Type and TSP-ID) • ConstraintsOnCertificateMetadata: LegalPersonSignerRequired:no LegalPersonSignerRequired: (APP-defined: yes/no) 2. Advanced electronic signatures; 2. Advanced electronic signatures; EUSCDRequired: (APP-defined: yes/no) EUSCDRequired: (APP-defined: yes/no) 3. Advanced electronic signatures; 3. Advanced electronic signatures; EUAdESigRequired: yes 3. Advanced electronic signatures; 3. Advanced electronic signatures; Advanced electronic signatures; Advanced electronic signatures; 3. Advanced electronic signatures; Commitment-type APP constraint:			validation data		
community of rhat choses to be compliant with the elDAS Regulation (e) Allocation of responsibility for signature validation and augmentation Managed by the APP, if required, otherwise managed by ORELY LuxTrust ORELY based on provisions made by APP as indicated in 9.1.5 and 3.1.5 None (f) Legal type of the signatures (defined by the APP to be one of the legal type: 1. Qualified electronic signatures; Parameters in the signature; (ISignature] QAA level, TSP-Type and TSP-ID) APP constraintsOnCertificateMetadata: (g) Commitment "proof of approval" Commitment-type APP constraints	(d)	Targeted	Any entity that shall be	Use of PAdES format	None
(e) Allocation of responsibility for signature validation and augmentation Managed by the APP, if required, otherwise managed by ORELY LuxTrust ORELY based on provisions made by APP as indicated in 9.1.5 and 3.1.5 None (f) Legal type of the signatures (defined by the APP to be one of the legal types: 1. Qualified electronic signatures; Parameters in the signature; 2. Advanced electronic signatures APP constraints: • ConstraintsOnCertificateMetadata: LegalPersonSignerRequired:no LegalPersonSignerAllowed:yes 2. Advanced electronic signatures Parameters supported by a qualified certificate; Supported by a qualified certificate; Avanced electronic signatures (g) Commitment "proof of approval" Commitment-type APP constraint:		community	or that choses to be compliant with the		
(e) Allocation of responsibility for signature validation and augmentation Managed by the APP, if required, otherwise managed by ORLY LuxTrust ORELY based on provisions made by APP as indicated in 9.1.5 and 3.1.5 None (f) Legal type of the signatures (defined by the APP to be one of the legal types: 1. Qualified electronic signatures; Parameters in the signature request [17] ([Signature] QAA level, TSP-Type and TSP-ID) APP constraints: • ConstraintsOnCertificateMetadata: LegalPersonSignerAllowed:yes 2. Advanced electronic signatures supported by a qualified certificate; Parameters in the signatures supported by a qualified certificate; EUQualifiedCertificateRequired: (APP-defined: yes/no) EUSSCDRequired: (APP-defined: yes/no) EUAdESigRequired:yes (g) Commitment "proof of approval" Commitment-type APP constraint:			eIDAS Regulation		
responsibility for signature validation and augmentation required, otherwise managed by ORELY provisions made by APP as indicated in 9.1.5 and 3.1.5 (f) Legal type of the signatures (defined by the APP to be one of the legal types: 1. Parameters in the signature request [17] ([Signature] QAA level, TSP-Type and TSP-ID) APP constraints: • ConstraintsOnCertificateMetadata: LegalPersonSignerRequired:no LegalPersonSignerRequired: (APP-defined: yes/no) 2. Advanced electronic signatures 7SP-Type and TSP-ID) EUQcalifiedCertificateRequired: (APP-defined: yes/no) 2. Advanced electronic signatures supported by a qualified certificate; Advanced electronic signatures) EUQcalifiedCertificateRequired: (APP-defined: yes/no) 3. Advanced electronic signatures) Supported by a qualified certificate; Advanced electronic signatures) Advanced 3. Advanced electronic signatures) Advanced Advanced APP constraint:	(e)	Allocation of	Managed by the APP, if	LuxTrust ORELY based on	None
Image: Synthetic validation and augmentation 3.1.5 (f) Legal type of the signatures (defined by the APP to be one of the legal types: Parameters in the signature request [17] ([Signature] QAA level, TSP-Type and TSP-ID) APP constraints: • ConstraintsOnCertificateMetadata: 1. Qualified electronic signatures; 2. Advanced electronic signatures supported by a qualified certificate; TSP-Type and TSP-ID) EUQualifiedCertificateRequired: (APP-defined: yes/no) EUSSCDRequired: (APP-defined: yes/no) EUAdESigRequired: yes (g) Commitment "proof of approval" Commitment-type APP constraints:		responsibility for	required, otherwise	provisions made by APP as indicated in 9.1.5 and	
augmentation Parameters in the signatures APP constraints: (f) Legal type of the signatures (defined by the APP to be one of the legal types: Parameters in the signature request [17] APP constraints: ConstraintsOnCertificateMetadata: 1. Qualified electronic signatures; ([Signature] QAA level, TSP-Type and TSP-ID) LegalPersonSignerRequired: (APP-defined: yes/no) EUQualifiedCertificateRequired: (APP-defined: yes/no) 2. Advanced electronic signatures supported by a qualified certificate; supported by a qualified electronic signatures) EUAdESigRequired: yes 3. Advanced electronic signatures) Advanced electronic signatures) Advanced electronic signatures (g) Commitment "proof of approval" Commitment-type APP constraint:		validation and	managed by ONEET	3.1.5	
(f)Legal type of the signatures(defined by the APP to be one of the legal types: I.Parameters in the signature request [17] ([Signature] QAA level, TSP-Type and TSP-ID)APP constraints:1.Qualified electronic signatures;I.Qualified electronic signatures;I.Qualified electronic signatures;I.Qualified electronic signaturesLegalPersonSignerRequired:no LegalPersonSignerAllowed:yes2.Advanced electronic signatures supported by a qualified certificate;I.Advanced electronic signatures supported by a qualified certificate;EUQualified certificate;3.Advanced electronic signatures)I.Advanced electronic signaturesEUAdESigRequired:yes(g)Commitment"proof of approval"Commitment-typeAPP constraints:	(4)	augmentation			
1. Qualified electronic signatures; ([Signature]QAA level, TSP-Type and TSP-ID) LegalPersonSignerRequired:no LegalPersonSignerAllowed:yes EUQualifiedCertificateRequired: (APP-defined: yes/no) 2. Advanced electronic signatures supported by a qualified certificate; Supported by a qualified certificate; EUSCDRequired: yes/no) 3. Advanced electronic signatures) EUSconstraintsorteet intraterweatata. (g) Commitment "proof of approval" Commitment-type	(†)	Legal type of the	(defined by the APP to be one of the legal types:	Parameters in the signature request [17]	APP constraints:
Image: Constraint of the electronic signatures; TSP-Type and TSP-ID) LegalPersonSignerAllowed:yes Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures; Image: Constraint of the electronic signatures;		Signatures	1 Qualified	([Signature] QAA level,	LegalPersonSignerRequired:no
image: signatures; image: signatures; image: signatures; image: signatures; image: signatures; image: signatures; image: signatures; image: signatures; image: signatures;<			electronic	TSP-Type and TSP-ID)	LegalPersonSignerAllowed:yes
2. Advanced electronic signatures signatures supported by a qualified certificate; 3. 3. Advanced electronic signatures signatures supported by a qualified certificate; 3. Advanced electronic signatures) (g) Commitment "proof of approval"			signatures;		EUQualifiedCertificateRequired: (APP-defined:
electronic EUAdESigRequired:yes signatures supported by a qualified certificate; 3. Advanced electronic signatures) (g) Commitment "proof of approval"			2. Advanced		EUSSCDRequired: (APP-defined: yes/no)
(g) Commitment "proof of approval" Commitment-type APP constraint:			electronic		EUAdESigRequired:yes
a qualified certificate; 3. Advanced electronic signatures) (g) Commitment "proof of approval" Commitment-type APP constraint:			supported by		
(g) Commitment "proof of approval" Commitment-type APP constraint:			a qualified		
3. Advanced electronic signatures) (g) Commitment "proof of approval" Commitment-type APP constraint:			certificate;		
(g) Commitment "proof of approval" Commitment-type APP constraint:			3. Advanced		
(g) Commitment "proof of approval" Commitment-type APP constraint:			signatures)		
	(g)	Commitment	"proof of approval"	Commitment-type	APP constraint:
assumed by the unless defined by the attribute is mandatory in • CommitmentTypesRequired:		assumed by the	unless defined by the	attribute is mandatory in	CommitmentTypesRequired:
Signatory APP the generated signatures. MandatedSignedQProperties-commitment-type-		Signatory	APP	the generated signatures.	MandatedSignedQProperties-commitment-type- indication:no
parameter of the				parameter of the	Indicationatio
signature request SCA constraint:				signature request	SCA constraint:
CommitmentTypesRequired: MandatadSignedOBrenerties commitment types					CommitmentTypesRequired: MandatedSignedOProperties commitment type
indication:yes					indication:yes
(h) Level of assurance Claimed by signatory for LuxTrust Global (none)	(h)	Level of assurance	Claimed by signatory for	LuxTrust Global	(none)
on timing the basic level, timestamping authority,		on timing	the basic level, timestamp for higher	timestamping authority,	
levels		evidences	levels		

28/29

VERSION 1.1.3

		Business statement	Technical counterpart	
BSP	BSP title	summary	statement	Constraint value at signature creation (SCA or APP)
(i)	Formalities of signing	Partially delegated mode	APP's responsibility and implementation for DTBS; LuxTrust ORELY or alternatively APP enables signature attributes visualization, with the enabling party becoming solely responsible for providing correct and full transparency	APP constraints: WYSIWYSRequired:yes WYSIWHBSRequired:yes ProperAdviceAndInformationRequired:yes UserInterfaceDesignConstraints:yes CorrectValidationAndArchivalProcedures:no
(j)	Longevity and resilience to change	Signing's certificate or timestamp's duration, whichever is higher	Ditto	(none)
(k)	Archival	No requirement		(none)
(I)	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 assurance levels [2].	 Corresponding signature request's parameter Specific trust anchors configuration 	 SCA constraints: X509CertificateValidationConstraints:SetOfTrustAnchors:(APP-defined⁵ or EU Trusted List)
(n)	Signature creation devices	(Optionally defined by the APP among the LuxTrust supported devices)	Signature request's parameters	
(0)	Other information to be associated with the signature	No requirement		
(p)	Cryptographic suites	State-of-art cryptographic suites	Cryptographic libraries	Cf. [14] for cryptographic constraints reference
(q)	Technological environment	LuxTrust specifications [17]. [18]. [21] and [22]	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

9.6.3 Output Constraints to be used for Generating/Augmenting Signatures in The Context of The Identified Signature Policy

No constraint

⁵ APP-defined requires a specific signature policy