Policy for Packaging of E-Signatures for Long-Term Validation

1 Policy information

Name	Policy for Packaging of E-Signatures for Long-Term Validation
Policy ID	urn:signicat:packagingpolicy:ltv:1.6
Policy OID	2.16.578.1.46.1.10.1.6
As part of combined policy ID[1]	urn:signicat:packagingpolicy:ltv:[signature packaging policy name]:1.6:[signature packaging policy version]
Policy owner	Signicat
Version	1.6
Publish date	2020-12-01
Working period	2020-12-01 ->

2 Version

Date	Specification version	Change
2020-11-05	1.6	Aligned with new XAdES specification 319 132-1 and added support for B-LTA format. Fixed typos.
2019-09-09	1.5	Added Commfides CA as trust anchor.
2017-04-06	1.4	Added signer's date of birth, issued date and expiry date for signer's certificate. Revised to conform to Signicat policies.
2015-03-31	1.3	- Chapter 6: Now requires that seal is on XAdES Baseline-B form. - Chapter 1: Correction of the name. - References: Specified that XAdES is version 1.4.1
2014-10-16	1.2	- Extracted the non-signature specific rules from the combined packaging policy document for urn:signicat:packagingpolicy:ltv:bankidse:1.1:1.2, into a separate policy document for the LTV policy. - Added *General LTV-SDO Profile* - *Removed URL, as this is not stable enough for policy.*

[1] This policy needs to be accompanied by a signature packaging policy, and they may be referenced together using a combined Policy ID.

3 Introduction

This packaging service policy defines requirements for packaging of e-signatures, in the context of signature creation and initial verification, for the purpose of implementing long-term validation support.

This policy needs to be accompanied by a signature packaging policy.

3.1 About Packaging Policies

The purpose of a packaging policy is to specify requirements for the packaging process, and high-level requirements for the prior signature creation and verification process.

The primary users of this policy will be e-signature users (relying parties). The policy will help e-signature users to better understand the information contained in a package, and on what basis it can be trusted and used.

The policy will also be useful for implementers of the packaging service.

3.2 The relation to a signature packaging policy

This is the general policy for packaging of e-signatures for long-term validation, referred to as the *LTV packaging policy.* It defines general requirements that are not specific to the signature type.

It needs to be accompanied by a *signature packaging policy*. The signature packaging policy will define requirements that are specific to the type of signature that is subject to packaging.

3.3 Scope

This packaging policy defines requirements for packaging of e-signatures for long-term validation in context of with the signature creation and initial verification.

Requirements for the creation and verification processes, including collection of data needed by the packaging process will be set by the accompanying signature packaging policy.

3.4 Structure

The normative parts of the policy are:

1. **General process requirement** defines high-level requirements for the overall packaging process.
2. **Package formatting requirements** defines requirements for the format used for the package
3. **Sealing requirements** defines requirements for the TSP signature on the package
4. **General LTV-SDO profile** defines a general LTV-SDO profile
5. **Trust anchors** for validation of the seal

3.5 Versioning and backwards compatibility

Packaging policy version numbers consists of a major and a minor number, denoting major and minor versions.

A change of minor version is always backwards compatible, and the new policy may be brought into effect without notifying relying parties.

A change of major version may introduce non-backwards compatible changes.

3.6 Contents

1Policy information..... 1
2Version..... 1
3Introduction 2
4General process requirements (normative)..... 3
5Package formatting requirements (normative) 4
6Sealing requirements (normative)..... 4
7General LTV-SDO Profile (normative) 4
8Appendix A (normative): Trust anchors used in validation of the seal 7

3.7 Terms and acronyms

Term	Explanation
TSP	Trust Service Provider - the entity implementing this policy by packaging the signature.
Long-term validation	The concept of validating an e-signature long time (months, and sometimes years) after it was created.
Native signature	The e-signature that is to be packaged for long-term validation
Original document	The document signed with the native signature
Seal	This is the Trust Service Provider's signature on the package. It is commonly referred to as the *Seal*.

3.8 References

Short name	Resource
XAdES	ETSI TS 101 903 - "XML Advanced Electronic Signatures (XAdES)
XMLDSIG	W3C XML Signature Syntax and Processing http://www.w3.org/TR/xmldsig-core/
XAdES-BASELINE	ETSI EN 319 132-1 V1.1.1 (2016-05): "XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures"
RFC-3161	IETF RFC 3161: "Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)".

4 General process requirements (normative)

1. Packaging of the native signature is done such that it provides support for long-term validation of the native signature.
2. Packaging is performed immediately following signature creation and initial verification.
3. Packaging is done only if initial verification succeeds.

4. Validation data used in the initial verification are included in the package, to enable re-creation of the validation process at a later point in time

5 Package formatting requirements (normative)

Package formatting is the process of putting all information elements together in a package.

5.1 Format

The package must be formatted according to the following format specification:

Name	LTV-SDO - Long Time Validation extended Signed Data Object
Version *)	1.X
Available at *)	`https://id.signicat.com/definitions/xsd/LtvSdo-1.X`

*) The 'X' means that the minor version number is not specified. It will be replaced by the actual minor version in the URL.

6 Sealing requirements (normative)

This section contains requirements to the TSP signature on the package, also called the *seal.*

1. The seal covers the complete package, such that all information in the package is protected by the signature.
2. The seal is a XAdES [XADES] signature on form Baseline-T [XADES-BASELINE] if an authorized time-stamp provider (TSA) is configured, or on form Baseline-B when no TSA is configured. The seal shall be created using: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256.
3. The seal is validated immediately following creation.
4. Validation of the seal is done according to XMLDSig Core Validation [XMLDSIG]
5. Validation includes certificate validation of the signing certificate, including revocation check. If an authorized time-stamp has been applied then this time-stamp is verified according to [RFC-3161]. Trust anchors used in certificate validation are listed in Appendix B.
6. All certificates and revocation values used in the initial verification of the signature are included in the XAdES structure.
7. If use of archive timestamp is configured then the XAdES structure, including the long term validation material, will be protected by an ArchiveTimeStamp provided by an authorized time-stamp provider (TSA). The resulting seal will then be on form Baseline-LTA – suitable for long-term archiving.
8. The package is sealed according to an explicit signature policy which is available together with this policy.

7 General LTV-SDO Profile (normative)

7.1 Introduction

This chapter defines the general profile for use of LTV-SDO for packaging of E-Signatures for Long-term Validation. The rules here are to be followed by *all* packaging under this policy, regardless of signature type and other signature packaging policy rules.

The signature packaging policy will define a specific profile with additional rules.

7.2 About LTV-SDO profiles

The LTV-SDO format is a generic format for packaging e-signatures for Long-term Validation. An *LTV-SDO Profile* specifies how the LTV-SDO format is used for a specific means, and in a specific context, by defining additional requirements and constraints to which XML Elements and attributes must be present, their possible values, and the semantics of these their values.

7.3 Description/SignerDescription

Element/Attribute	Semantics	Format/possible values	Required
SignerDisplayName	The signer's name	A string with the signer's name.	Yes
SignerUniqueId	An ID that uniquely identifies the signer in the scope of the signature type.	*Defined in the signature packaging policy*	Yes
SignerNationalId	The signer's *national id* identifies the signer by some nation-wide ID-number. This value is tightly connected with *SignerNationality* and *SignerNationalIdType*.	*Defined in the signature packaging policy*	*Defined in the signature packaging policy*
SignerNationality	The nationality for the *SignerNationalId.*	*Defined in the signature packaging policy*	When SignerNationalId is present
SignerNationalIdType	The type of national id given in *SignerNationalId.*	*Defined in the signature packaging policy*	When SignerNationalId is present
SignerDateOfBirth	The date the signer was born.	*yyyy-mm-dd*	No
SignerCertIssueDate	The date the signer's certificate was issued.	*yyyy-mm-dd*	No
SignerCertExpirationDate	The date the signer's certificate will expire.	*yyyy-mm-dd*	No

7.4 Description/DocumentDescription

Element/Attribute	Semantics	Format/possible values	Required
DocumentMimeType	Mime Type of the original document	A string with a valid MIME Type. *Example:* "application/pdf".	Yes
DocumentTitle	Short description of the original document, suitable to be used as title.	A relatively short string with a document title. *Example:* "Loan Agreement"	Yes
DocumentDigest	Digest of the original, unsigned document. Algorithm must be SHA-256 or better.	String, containing the Base64-encoded hash of the document.	Yes
DocumentDigest@alg	The actual hash algorithm used to compute the value of DocumentDigest	A String containing the algorithm identifier. Possible values are algorithm identifiers defined by W3C, for example: http://www.w3.org/2001/04/xmlenc#sha256	Yes

7.5 Description/SignatureDescription

Element/Attribute	Semantics	Format/possible values	Required
SignatureTypeFriendlyName	Descriptive name of the e-signature type, suitable to present to the end user	*Defined in the signature packaging policy*	Yes
SignatureFormatFriendlyName	Descriptive name of the e-signature format, suitable to present to the end user.	*Defined in the signature packaging policy*	Yes
SigningTime	An approximation of the time the signature was created. Collected by the verifier from a secure time source immediately after the signature is received from the signature creation client.	xades:signingTime (XML DateTime) value.	Yes

7.6 NativeSignature/NativeSdo

Element/Attribute	Semantics	Format/possible values	Required
(element content)	The e-signature as produced by the native signature system.	String, containing the Base64-encoded signature	Yes

@Format	The format of the signed data object, as a Signicat format identifier.	*Defined in the signature packaging policy*	Yes
@Version	The version of the format of the signed data object.	String containing the version number	Yes
@MimeType	The mime type of the signed data object.	*Defined in the signature packaging policy*	Yes

7.7 NativeSignature/NativeSignatureQualifyingProperties

Element/Attribute	Semantics	Format/possible values	Required
SigningTime	The signing time, as collected by the TSP from a trusted time source.	xades:signingTime (XML DateTime) value.	Yes

8 Appendix A (normative): Trust anchors used in validation of the seal

The following certificates are used as trust anchor in Certificate Path Validation and OCSP Response validation when validating the seal (the TSP signature).

8.1 Buypass Class 3 CA 1

```
-----BEGIN CERTIFICATE-----
MIIDUzCCAjugAwIBAgIBAjANBgkqhkiG9w0BAQUFADBLMQswCQYDVQQGEwJOTzEd
MBsGA1UECgwUQnV5cGFzcyBBUy05ODMxNjMzMjcxHTAbBgNVBAMMFEJ1eXBhc3Mg
Q2xhc3MgMyBDQSAxMB4XDTA1MDUwOTE0MTMwM1oXDTE1MDUwOTE0MTMwM1owSzEL
MAkGA1UEBhMCTk8xHTAbBgNVBAoMFEJ1eXBhc3MgQVMtOTgzMTYzMzI3MR0wGwYD
VQQDDBRCdXlwYXNzIENsYXNzIDMgQ0EgMTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKSO13TZKWTeXx+HgJHqTjnmGcZEC4DVC69TB4sSveZn8AKxifZg
isRbsELRwCGoy+Gb72RRtqfPFfV0gGgEkKBYouZ0plNTVUhjP5JW3SROjvi6K//z
NIqeKNc0n6wv1g/xpC+9UrJJhW05NfBEMJNGJPO251P7vGGvqaMU+8IXF4Rs4HyI
+MkcVyzwPX6UvCWThOiaAJpFBUJXgPROztmuOfbIUxAMZTpHe2DC1vqRycZxbL2R
hzyRhkmr8w+gbCZ2Xhysm3HljbybIR6c1jh+JIAVMYKWsUnTYjdbiAwKYjT+p0h+
mbEwi5A3lRyoH6UsjfRVyNvdWQrCrXig9IsCAwEAAaNCMEAwDwYDVR0TAQH/BAUw
AwEB/zAdBgNVHQ4EFgQUOBTmyPCppAP0Tj4io1vy1uCtQHQwDgYDVR0PAQH/BAQD
AgEGMA0GCSqGSIb3DQEBBQUAA4IBAQABZ6OMySU9E2NdFm/soT4JXJEVKirZgCFP
Bdy7pYmrEzMqnji3jG8CcmPHc3ceCQa6Oyh7pEfJYWsICCD8igWKH7y6xsL+z27s
EzNxZy5p+qksP2bAEllNC1QCkoS72xLvg3BweMhT+t/Gxv/ciC8HwEmdMldg0/L2
mSlf56oBzKwzqBwKu5HEA6BvtjT5htOzdlSY9EqBs1OdTUDs5XcTRa9bqh/YL0yC
e/4qxFi7T/ye/QNlGioOw6UgFpRreaaiErS7GqQjel/wroQk5PMr+4okoyeYZdow
dXb8GZHo2+ubPzK/QJcHJrrM85SFSnonk8+QQtS4Wxam58tAA915
-----END CERTIFICATE-----
```

8.2 Buypass Class 3 CA 1 - extended life-time

```
-----BEGIN CERTIFICATE-----
MIIDUzCCAjugAwIBAgIBAzANBgkqhkiG9w0BAQsFADBLMQswCQYDVQQGEwJOTzEd
MBsGA1UECgwUQnV5cGFzcyBBUy05ODMxNjMzMjcxHTAbBgNVBAMMFEJ1eXBhc3Mg
Q2xhc3MgMyBDQSAxMB4XDTA1MDUwOTE0MTMwM1oXDTE2MDUwOTE0MTMwM1owSzEL
MAkGA1UEBhMCTk8xHTAbBgNVBAoMFEJ1eXBhc3MgQVMtOTgzMTYzMzI3MR0wGwYD
VQQDDBRCdXlwYXNzIENsYXNzIDMgQ0EgMTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBAKSO13TZKWTeXx+HgJHqTjnmGcZEC4DVC69TB4sSveZn8AKxifZg
```

```
isRbsELRwCGoy+Gb72RRtqfPFfV0gGgEkKBYouZ0plNTVUhjP5JW3SROjvi6K//z
NIqeKNc0n6wv1g/xpC+9UrJJhW05NfBEMJNGJPO251P7vGGvqaMU+8IXF4Rs4HyI
+MkcVyzwPX6UvCWThOiaAJpFBUJXgPROztmuOfbIUxAMZTpHe2DC1vqRycZxbL2R
hzyRhkmr8w+gbCZ2Xhysm3HljbybIR6c1jh+JIAVMYKWsUnTYjdbiAwKYjT+p0h+
mbEwi5A3lRyoH6UsjfRVyNvdWQrCrXig9IsCAwEAAaNCMEAwDwYDVR0TAQH/BAUw
AwEB/zAdBgNVHQ4EFgQUOBTmyPCppAP0Tj4io1vy1uCtQHQwDgYDVR0PAQH/BAQD
AgEGMA0GCSqGSIb3DQEBCwUAA4IBAQCFpYJ6LryjhPCuxwMa6pdG+o9tLL1AgTUU
WzJzPlbXKRJPkT60DiLptFhhcqu0/hEDz5hAkWXU6gydQlk3lZQodNLWj9Db+WyY
casAxUSacqSuR/RT7G+myQEJ4Bl+4cBFjTY6McWCNifctCsJMhlNm3puHNytqwRy
T2DoICHrURrzfaqnZ0hkNnf26Yhs0BDjWE/R+5SbzqmEVlLGVfZW8QzQMRNEnPkH
Mg3Ah6doPqjO+1+UAJgeI+dC9epf+iQgGlBdzw3NLYtqbs3fsHu2/40bbOum0qfI
Q8MLRyH/421x8g3MeJ7SAUQ8+fU5RzbkZUfnpGLIcH82viL3C9Pg
-----END CERTIFICATE-----
```

8.3 Buypass Class 3 Root CA

```
-----BEGIN CERTIFICATE-----
MIIFWTCCA0GgAwIBAgIBAjANBgkqhkiG9w0BAQsFADBOMQswCQYDVQQGEwJOTzEd
MBsGA1UECgwUQnV5cGFzcyBBUy05ODMxNjMzMjcxIDAeBgNVBAMMF0J1eXBhc3Mg
Q2xhc3MgMyBSb290IENBMB4XDTEwMTAyNjA4Mjg1OFoXDTQwMTAyNjA4Mjg1OFow
TjELMAkGA1UEBhMCTk8xHTAbBgNVBAoMFEJ1eXBhc3MgQVMtOTgzMTYzMzI3MSAw
HgYDVQQDDBdCdXlwYXNzIENsYXNzIDMgUm9vdCBDQTCCAiIwDQYJKoZIhvcNAQEB
BQADggIPADCCAgoCggIBAKXaCpUWUOOV8l6ddjEGMnqb8RB2uACatVI2zSRHsJ8Y
ZLya9vrVediQYkwiL944PdbgqOkcLNt4EemOaFEVcsfzM4fkoF0LXOBXByow9c3E
N3coTRiR5r/VUv1xLXA+58bEiuPwKAv0dpihi4dVsjoT/Lc+JzeOIuOoTyrvYLs9
tznDDgFHmV0ST9tD+leh7fmdvhFHJlsTmKtdFoqwNxxXnUX/iJY2v7vKB3tvh2PX
0DJq1l1sDPGzbjniazEuOQAnFN44wOwZZoYS6J1yFhNkUsepNxz9gjDthBgd9K5c
/3ATAOux9TN6S9ZV+AWNS2mw9bMoNlwUxFFzTWsL8TQH2xc519woe2v1n/MuwU8X
KhDzzMro6/1rqy6any2CbgTUUgGTLT2G/H783+9CHaZr77kgxve9oKeV/afmiSTY
zIw0bOIjL9kSGiG5VZFvC5F5GQytQIgLcOJ60g7YaEi7ghM5EFjp2CoHxhLbWNvS
O1UQRwUVZ2J+GGOmRj8JDlQyXr8NYnon74Do29lLBlo3WiXQCBJ31G8JUJc9yB3D
34xFMFbG02SrZvPAXpacw8Tvw3xrizp5f7NJzz3iiZ+gMEuFuZyUJHmPfWupRWgP
K9Dx2hzLabjKSWJtyNBjYt1gD1iqj6G8BaVmos8bdrKEZLFMOVLAMLrwjEsCsLa3
AgMBAAGjQjBAMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFEe4zf/lb+74suwv
Tg75JbCOPGvDMA4GA1UdDwEB/wQEAwIBBjANBgkqhkiG9w0BAQsFAAOCAgEAACAj
QTUEkMJAYmDv4jVM1z+s4jSQuKFvdvoWFqRINyzpkMLyPPgKn9iB5btb2iUspKdV
cSQy9sgL8rxq+JOssgfCX5/bzMiKqr5qb+FJEMwx14C7u8jYog5kV+qi9cKpMRXS
IGrs/CIBKM+GuIAeqcwRpTzyFrNHnfzSgCHEy9BHcEGhyoMZCCxt8l13nIoUE9Q2
HJLw5QY33KbmkJs4j1xrG0aGQ0JfPgEHU1RdZX33inOhmlRaHylDFCfChQ+1iHsa
O5S3HWCntZznKWlXWpuTekMwGwPXYshApqr8ZORK15FTAaggiG6cX0S5y2CBNOxv
033aSF/rtJC8LakcC6wc1aJoIIAE1vyxjy+7SjENSoYc6+I2KSb12tjE8nVhz36u
dmNKekBlk4f4HoCMhuWG1o8O/FMsYOgWYRqiPkN7zTlgVGr18okmAWiDSKIz6MkE
kbIRNBE+6tBDGR8Dk5AM/1E9V/RBbuHLoL7ryWPNbczk+DaqaJ3tvV2XcEQNtg41
3OEMXbugUZTLfhbrES+jkkXITHHZvMmZUldGL1DPvTVp9D0VzgalLA8+9oG6lLvD
u79leNKGef9JOxqDDPDeeOzI8k1MGt6CKfjBWtrt7uYnXuhF0J0cUahoq0Tj0Itq
4/g7u9xN12TyUb7mqqta6THuBrxzvxNiCp/HuZc=
-----END CERTIFICATE-----
```

8.4 Commfides CPN RootCA SHA256 Class 3

```
-----BEGIN CERTIFICATE-----
MIIEOzCCAyOgAwIBAgIIZGU4FfEKbvowDQYJKoZIhvcNAQELBQAwgZ4xIjAgBgNV
BAMTGUNQTiBSb290Q0EgU0hBMjU2IENsYXNzIDMxQDA+BgNVBAsTN0NvbW1maWRl
cyBUcnVzdCBFbnZpcm9ubWVudCAoYykgMjAxMSBDb21tZmlkZXMgTm9yZ2UgQVMx
KTAnBgNVBAoTIENvbW1maWRlcyBOb3JnZSBBUyAtIDk4OCAzMTIgNDk1MQswCQYD
VQQGEwJOTzAeFw0xMTAyMjgwOTEyMjJaFw0yNTAxMDEwOTEyMjJaMIGeMSIwIAYD
```

```
VQQDExlDUE4gUm9vdENBIFNIQTI1NiBDbGFzcyAzMUAwPgYDVQQLEzdDb21tZmlk
ZXMgVHJ1c3QgRW52aXJvbm1lbnQgKGMpIDIwMTEgQ29tbWZpZGVzIE5vcmdlIEFT
MSkwJwYDVQQKEyBDb21tZmlkZXMgTm9yZ2UgQVMgLSA5ODggMzEyIDQ5NTELMAkG
A1UEBhMCTk8wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDKz5CLVgBq
/7vJvEnTA2Ba046lGu7Lwwwglq/4uiPc/1SEJI/pRr2qpIS2HXi+gq6p/0ig7XQU
2KxRaYKgP4elSJkC7V49yu+UvlAEf1PQ3RmVUoNLsIeT7VbxyUwF/JCPOx7B95Rg
aTHQoAocZ+nsejZcPNenHXTq2EKrXHHuJDD2U7Dg5OGJq9D1/NaRl4/fGdUAZSgl
ArbAAM5gFsT0/p714rC4jTn9eMLrkyfMvBWRvjHQz+ctiElpkvX/GJsOtEFqtedV
fnBoydiKOAsef0ICgt01yYaW5OPQgvg6B27tqFsJEgOltQ6chFvA8FFc++QiH6BX
OJEGm/wmHozxAgMBAAGjezB5MB0GA1UdDgQWBBSWhl/gjBoUw6aC4uOZoWE1ohYY
4TAPBgNVHRMBAf8EBTADAQH/MB8GA1UdIwQYMBaAFJaGX+CMGhTDpoLi45mhYTWi
FhjhMBYGA1UdIAQPMA0wCwYJYIRCAR0KAQEAMA4GA1UdDwEB/wQEAwIBhjANBgkq
hkiG9w0BAQsFAAOCAQEAVneyH1lbUcxaxrfi78cPSeWtSzO/QMsNsczzJmW33uTQ
6lL3KuM5Htw13SzzKlG2UZYTbY+RiWBOpZT30Z9lkMwAC2epbuN9zczdsF8oZYfp
6QQGn/hfSex0S5FuT85h7pEMlcZAGrKq+eojoe/RmTwCEX/0uxl14QDIlmAPNrEJ
P4bg1+SN2ha+P4DX5XMGPfJkYCMmWBe6kmQkQkgJFmqAHJnZ/V72Sowyhinu6UnI
47cVEAeqwOAtF/Cu6IRnvjV1Vse3wjRFy/mpNlbOq9IQBkBdXb2uXzRt78JmNWw0
DGMYnXhJ13mUKFJJrZr6K6rRBFT7lkf0k+QnSkAvNA==
-----END CERTIFICATE-----
```