certipost	**Certipost e-Signing Services**	Document OID: **0.3.2062.7.2.1.1.1.1**	Version: **1.1**
Handwritten Equivalent Signature Policy		Approval Status: **Approved**	Page #: 1 of 12

Rev	Description of Change	Author	Date
1.0	First Version	Wim Coulier	15/06/2007
1.1	Clarifications to enable this policy to be used for more products	Wim Coulier	23/08/2007

1. Introduction

1.1. Scope

This document covers the policy rules that are used to state under which conditions an electronic signature generation and validation methods are valid when used within the context of the Certipost *e-Signing* service of Handwritten Equivalent level.

Moreover, the present document sets the roles and obligations of all actors involved in the *e-Signing Handwritten Equivalent* transactions. These rights and obligations for entities involved in *e-Signing Handwritten Equivalent* transactions are stated in the form of both contract obligations and technical requirements.

Finally, the present document oversees the technical standards and operations used to create the electronic signatures through the Certipost *e-Signing Handwritten Equivalent* service.

1.2. Organization of the document

The organization of this document is based on the signature policy framework as defined in ETSI TR 102 041 v1.1.1: “Signature policy report”.

1.3. Preceding language version

This document is translated in several languages. In case of conflicting content between the different languages, the English version precedes. The different language versions can be found in the following location:

English version: https://connect.e-signing.be/documents/e-Signing_HandwrittenEquivalentSignaturePolicy_EN_v1.1.pdf

Dutch version (Nederlandstalige versie): https://connect.e-signing.be/documents/e-Signing_HandwrittenEquivalentSignaturePolicy_NL_v1.1.pdf

French version (version francophone): https://connect.e-signing.be/documents/e-Signing_HandwrittenEquivalentSignaturePolicy_FR_v1.1.pdf

1.4. Definitions

Advanced Electronic Signature: means an electronic signature that meets the following requirements:

- It is uniquely linked to the signatory;
- It is capable of identifying the signatory;
- It is created using means that the signatory can maintain under his sole control; and
- It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

Certification Authority (CA): An authority trusted by one or more users to create and assign certificates. Optionally the certification authority may create the users’ keys.

Certificate identifier: a unique identifier of a Certificate consisting of the name of the CA and of the certificate serial number assigned by the CA.

Certificate Policy: A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

Certificate Validity period: The time interval during which the CA warrants that it will maintain information about the status of the certificate.

Certificate revocation list: a list containing the serial numbers of revoked certificates from a given CA, together with other revocation information.

Certification path: A chain of multiple certificates, comprising a certificate of the public key owner (the end entity) signed by one CA, and zero or more additional certificates of CAs signed by other CAs.

Certification Service Provider: an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures; [EC 1999/93]

CRL distribution point: A directory entry or other distribution source for CRLs; a CRL distributed through a CRL distribution point may contain revocation entries for only a subset of the full set of certificates issued by one CA or may contain revocation entries for multiple CAs.

Data to be signed (DTBS): the complete electronic data to be signed (including both Signer's Document and Signature Attributes)

Digital signature: data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery, e.g. by the recipient.

e-Signing Framework: The Certipost e-Signing framework is the whole of the Certipost e-Signing signature policies and the component enforcing compliance to the policy in question for creating and verifying e-Signing signatures. This framework can be used by different front-end applications as part of a Certipost product or service.

e-Signing Handwritten Equivalent Service: e-Signing Service that is limited to the creation of signatures according to the present Signature Policy (Handwritten Equivalent signatures).

e-Signing Service: Any product or service that makes use of the Certipost e-Signing Framework to create electronic signatures for the user of the service. Since this document is limited to the Handwritten Equivalent type of signature, when this term is mentioned further in this document this means the e-Signing Handwritten Equivalent Service.

End entity: A certificate subject that uses its public key for purposes other than for signing certificates.

Electronic signature: means data in electronic form that are attached to or logically associated with other electronic data

Hash function: A function that maps string of bits to fixed-length strings of bits, satisfying the following two properties:
- It is computationally unfeasible to find for a given output an input that maps to this output
- It is computationally unfeasible to find for a given input a second input which maps to the same output

Initial verification: a process performed by a Verifier that must be done soon after a signature is generated in order to capture the information that will make it valid for long term verification.

Object identifier: a sequence of numbers that uniquely and permanently references an object.

OCSP: see Online Certificate Status Protocol

Online certificate status protocol: real time on line trusted source of certificate status information.

Parallel signature: the application of separate independent signatures to the same Signer’s document

Public key: That key of an entity’s asymmetric key pair that can be made public

Private key: That key of an entity's asymmetric key pair that should only be used by that entity.

Qualified certificate: a certificate which meets the requirements laid down in Annex I of the Directive and is provided by a certification-service-provider who fulfils the requirements laid down in Annex II of the Directive [EC 1999/93]

Qualified electronic signature: an advanced electronic signature which is based on a qualified certificate and which is created by a secure-signature-creation device (Note: Definition of Art. 5.1 signature taken from the Directive [4]).

Secure Signature Creation Device: means a signature creation device that meets the requirements laid down in [4], Annex III.

Signature attributes: Additional information that is signed together with the Signer's Document.

Signature creation data: means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.

Signature creation device: means configured software or hardware used to implement the signature creation data.

Signature policy: a set of technical and procedural requirements for the creation and verification of an electronic signature, under which the signature can be determined to be valid.

Signature policy identifier: Object Identifier that unambiguously identifies a Signature Policy.

Signature policy issuer: An organization that creates, maintains and publishes a signature policy.

Signature policy issuer name: A name of a Signature Policy Issuer.

Signature verification: a process performed by a Verifier either soon after the creation of an electronic signature or later to determine if an electronic signature is valid against a signature policy implicitly or explicitly referenced.

Signature verification data: data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature; [EC 1999/93]

Signature verification device: configured software or hardware used to implement the signature verification-data [EC 1999/93]

Signer: Entity that creates an (electronic) signature (physical or legal person).

Signer’s identity: the registered name of the Signer (i.e. as registered by the CSP supplying the Signer’s certificate).

Signer's document: The electronic data to which the electronic signature is attached to or logically associated with.

Time-Mark: A proof-of-existence for a datum at a particular point in time, in the form of a record in a secure audit trail, which includes at least a trustworthy time value and a hash representation of the datum.

Time stamp: A proof-of-existence for a date at a particular point in time, in the form of a data structure signed by a Time Stamping Authority, which includes at least a trustworthy time value, a unique identifier for each newly generated time stamp, an identifier to uniquely indicate the time-stamp policy under which the time stamp was created, a hash representation of the datum, i.e. a data imprint associated with a one-way collision resistant uniquely identified hash-function.

Time stamp authority: An authority trusted by one or more users to provide a Time Stamping Service.

Time stamp service: A service that provides a trusted association between a date and a particular point in time, in order to establish reliable evidence indicating the time at which the datum existed.

Usual verification: a process performed by a Verifier that may be done years after the electronic signature was produced, does not need to capture more data than the data that was captured at the time of initial verification.

Validation data: additional data, collected by the Signer and/or a Verifier, needed to verify the electronic signature in order to meet the requirements of the signature policy. It may include: certificates, revocation status information, time-stamps or Time-Marks.

Verifier: An entity that validates or verifies an electronic signature (physical or legal person). This may be either a relying party or a third party interested in the validity of an electronic signature.

2. Certipost *e-Signing* Service

2.1. Certipost e-Signing actors

Signer: see above

Verifier: see above

Certipost e-Signing service provider: Certipost e-Signing service provider helps the Signer to create a signature according to the present signature policy, in order to ensure that the signature generated has a legal value equivalent to a handwritten signature as per the Directive [4] implemented in the Belgian law on electronic signature [6]. Certipost e-Signing service provider helps the Verifier to assess whether a signature was compliant to the present signature policy, and thus that the signature verified has a legal value equivalent to a handwritten signature as per the Directive [4] implemented in the Belgian law on electronic signature [6].

2.2. Certipost e-Signing service description

The goal of the Certipost e-Signing Service is to lower the barrier for electronic document signing dramatically by taking the legal and technical complexity of this signing away from the Signer who applies the signature and Verifier who trusts the signature.

The Certipost e-Signing Service is a service that will help users to create and verify Qualified Electronic Signatures with long term value. Qualified Electronic Signatures are electronic signatures that comply with the requirements from the European Directive [1] and Belgian law [2] concerning electronic signatures in such a way that from a legal point of view they are automatically accepted as equivalent to a handwritten signature. As the requirements from the European Directive and Belgian law are complex for the general public, Certipost has created this service to take this complexity away from the Signer and the Verifier. By simply using the Certipost e-Signing service, both the Signer and Verifier can be assured of compliance of their signature and verification method to the European Directive and Belgian law. In addition, the Certipost e-Signing service offers a number of supplementary measures to make sure that the conditions for long term non-repudiation of signatures are met.

2.3. Supported standard

The signature will be formatted in the standard XML Advanced Electronic Signature standard (XAdES)[i], to allow all measures to be applied for long term non-repudiation. XAdES defines several different signature profiles. Each profile adds additional verification information on top of the encapsulated profile. The range goes from the basic XAdES profile, which is only sufficient for very short-term proof of non-repudiation up to XAdES-A which offers enough non-repudiation proof elements for archiving. For more information see the ETSI standard.

The electronic signature applied according to the present Signature Policy must be formatted in at least the XAdES-T profile. This profile contains as well a timestamp that can proof at what time the signature was posed. Another XAdES profile that encapsulates a XAdES-T such as XAdES-X-L is of course accepted as well. For signatures that have to be proven beyond the expiration date of the certificate, the XAdES-X-L should be used (the XAdES-X-L also contains the certificate status information). The signature itself will be created with the Signer's SSCD, the formatting of the XAdES-T or XAdES-X-L signature document (and inclusion of timestamp(s) and possibly certificate status information) will be performed on the Certipost e-Signing server. At any moment, any party in possession of the XAdES-T signature can add revocation status information and timestamps to form a XAdES-X-L. At any moment, any party in possession of the XAdES-X-L can add a new timestamp to form a XAdES-A format for a long term archiving version of the signature.

All signatures created under this signature policy will as well include within the XAdES format references to the present Signature Policy in the form of OID, hash and URL of the present Signature Policy.

2.4. e-Signing creation

The Signer can create a signature according to this Signature Policy using the Certipost e-Signing service. Multiple presentation environments can use the Certipost e-Signing Framework. It is possible that the Certipost e-Signing service will at a certain moment implement other signature policies than the present one. The implementations based on the Certipost e-Signing Handwritten Equivalent Signature Policy will have the following in common:

1. The user can select a file to be signed
2. The Certipost e-Signing service will perform a number of verifications (not necessarily in this order):
    a. Whether the signature is valid for the specified signed file
    b. Certificate issued under an accepted Certificate Policy (see section 3.3.3.1.1 Certificate requirements).
    c. Validity of the certificate: certificate not revoked or suspended, certificate within validity period (between valid from and valid to dates), full certificate chain validation (including validation of all certificates in the chain)

    When one of the verifications fails, the signature process will be aborted.
3. The Certipost e-Signing service will create the XAdES-T file. This includes the collection of a timestamp. In case the e-Signing server creates a XAdES-X-L file, this includes the collection and inclusion of Certificate status information and timestamps.

2.5. e-Signing verification

The Verifier can use any means to verify the signature created according to this policy. However, following conditions must be met. The Certipost e-Signing verification service implementation meets all these criteria, and is open for use to any Verifier.

[i] ETSI TS 101 903

1. Assurance that the signature is valid for the specified signed file.
2. Validity of the certificate at the time of signing: certificate not revoked or suspended, certificate not expired and already valid, full certificate chain validation (including validation of all certificates in the chain). This may include the construction of a XAdES-X-L from the XAdES-T or a XAdES-A from the XAdES-X-L.
3. Certificate issued under an accepted Certificate Policy (see section 3.3.3.1.1 Certificate requirements).
4. Verification of all the timestamps in the XAdES-T, XAdES-X-L or XAdES-A (in case additional timestamps have been added for long term non-repudiation assurance), including the verification that the timestamp validity periods overlap (at any point in time at least one of the timestamps should be valid to assure in case of algorithm breach that never the non-repudiation value might have been compromised).

3. Signature policy information

3.1. General Certipost e-Signing Handwritten Equivalent Signature Policy information

Following ETSI requirements[ii], the Certipost *e-Signing Handwritten Equivalent* signature policy includes the following data:

3.1.1. Signature Policy Identifier:

- Signature Policy Name: Certipost e-Signing Handwritten Equivalent Signature Policy
- Signature Policy OID: 0.3.2062.7.2.1.1.1.0 (the last two digits define the major and minor versions of the signature policy respectively)
- Signature Policy URL: https://connect.e-signing.be/documents/e-Signing_HandwrittenEquivalentSignaturePolicy_EN_v1.0.pdf

3.1.2. Date of issue

15 June 2007

3.1.3. Signature Policy Issuer name:

Certipost sa/nv

- contact details:

Registered office: Certipost s.a/n.v. • Centre Monnaie / MuntCentrum • B-1000 Bruxelles / Brussel
TVA – B.T.W. BE 475.396.406 • RC Bruxelles / HR Brussel 652.060

Operational address: Ninovesteenweg 196, B-9320 Erembodegem
Phone: +32 53 60 11 11 - Fax: +32 53 60 11 01

- Signature Policy Issuer OID: 0.3.2062.7

3.2. Signing Period

The present Signature Policy is valid from the date of issue till it becomes superseded by a next version.

3.3. Common Rules

[ii] Specified in reference document [1] ETSI TR 102 041 (V1.1.1) : « Signature policy report »

3.3.1. Rules for the Signer

3.3.1.1. Absence of time based dynamic content

The Signer is responsible that the file being signed does not contain any dynamic content that might modify the visualized result of the file during time (e.g. amounts or sentences that change after a certain date). The Signer must not include such dynamic content in any file the Signer creates that will be subject to use of the e-Signing service. In case the Signer wants to sign a document that he did not create himself, he should make sure that such dynamic content is not present. That is why we advice against the signing of documents containing macro's or other executable code. We advice in such a case to convert the file first to a format that does not contain dynamic content such as TIFF, PDF, JPEG, …

3.3.1.2. Documents accepted by law

Although that the Belgian Law [6] lays down the conditions for electronic signatures to be accepted as equivalent to handwritten signatures, other laws sometimes lay down conditions that rule out electronic signatures after all. Additionally, for some transactions, electronic documents and/or electronic signatures may not be allowed according to the applicable contractual conditions (e.g. a certain form of communication was contractually agreed that rules out the use of electronic signatures). The Signer is responsible that the file being signed is accepted by law and applicable contracts to be signed electronically. In the present Signature Policy, no exhaustive list can be provided of types of content that are not allowed by Belgian law to be signed electronically, but particularly the types of content listed below should be investigated by the Signer:

- testament
- “cheque”, “order note” and “bill of exchange”
- unilateral engagement by a non-merchant to pay a certain amount or good of value
- contracts which need to be registered, such as contracts to rent a house (by lack of e-registration)
- authentic acts (“authentieke akten”, "actes authentiques"), such as the contract to buy real estate and donations.
- some kinds of mandate, such as the mandate for authentic acts, the mandate to accept a donation or the mandate to be present at the execution of civil state acts.

Transaction under another country’s legislation might be subject to similar exceptions.

3.3.1.3. Signed attributes

The following set of Signed Attributes will be provided by the Signer:

- Signing time
- Signing Certificate (including the full certificate path)
- Signature Policy (in the form of OID, hash and URL of the current Signature Policy)

3.3.1.4. Unsigned attributes

The following set of Unsigned Attributes should be provided by the Signer. If not added by the Signer, they may be added by the Verifier.

- Timestamps: this must include SignatureTimeStamps (timestamp on the signature itself), this should include SigAndRef TimeStamps (timestamp on the combination of the signature and the references to validation information) an may include ArchiveTimeStamps (timestamps added over time to maintain long term non-repudiation value)
- Countersignature (possibly, not mandatory)
- Certificate values: this must include the CompleteCertificate Refs and should include the Certificate-Values

- Certificate status references: this must include the CompleteRevocationData Refs and should include the RevocationValues

3.3.2. Rules for the Verifier

3.3.2.1. Signed attributes

- Signing time: only to be used as an indication, only a timestamp can give conclusive information about a time reference. The oldest timestamp within the XAdES structure will be used to determine signing time.
- Signing Certificate: Full verification of the signing certificate for the signing time (signing time during the lifetime of the certificate, certificate not revoked or suspended, full verification on the certificate chain)

  Note: Although the XAdES-X-L format contains certificate verification data, this certificate verification data can have been collected not taking a cautionary period in consideration (see cautionary period in the section 3.3.3.2 Timestamping). Performing a new online certificate status verification can only conclusively give the correct status if this new online verification is performed after the cautionary period but before the expiration of the certificate. Often certificate status information services do not keep mention on revocation or suspension on expired certificates. Therefore the way the verification is performed depends on the state of the certificate at verification time.

  - When performing a verification before expiration of the Signature certificate: The Verifier should as well perform a new online certificate status verification. In case this new verification shows the certificate being revoked or suspended, the Verifier should not trust the signature in case the date and time of revocation or suspension is earlier or equal to signing date and time, even if the certificate revocation data included in the XAdES-X-L signature claims the certificate to have been valid at that time. Only when the Verifier can not obtain such new status information, the certificate status information from the XAdES-X-L itself can be used as only certificate status information, implying an acceptance of the resulting risk.
  - When performing a verification after expiration of the Signature certificate: The certificate status information from the XAdES-X-L itself must be used as only certificate status information, implying an acceptance of the resulting risk. A new online certificate status verification cannot be trusted upon to contain correct revocation data about the certificate.
- Signature Policy: The Verifier should check that this is indeed the Signature Policy that was identified in the XAdES structure (by hash comparison).

3.3.2.2. Unsigned attributes

The following set of Unsigned Attributes should be provided by the Signer. If not added by the Signer, they may be added by the Verifier.

- Timestamps: Several timestamps can have been applied. Except the verification of the validity of the timestamps themselves and the timestamp signing certificates, the Verifier should make sure that timestamps are included in such a way that the timestamp validity periods overlap (at any point in time at least one of the timestamps should be valid to assure in case of algorithm breach that never the non-repudiation value might have been compromised), and this for the period between the Signing time and the moment of the verification.
- Countersignature (possibly, not mandatory): Same checks as on the first signature.
- Certificate values: Used in the verifications above.
- Certificate status references: Used in the verifications above.

3.3.3. Trust conditions

3.3.3.1. Signing Certificate

3.3.3.1.1. Certificate requirements

The trust points that must be used for the start of processing of the Signing Certificate path (the self-signed certificates for the CAs) are limited to:

- Belgium Electronic Identity card (eID) certificates:

  Belgium Root CA

- Certipost E-Trust certificates:
  - Belgacom E-Trust Root CA for qualified certificates
  - Certipost E-Trust TOP Root CA
  - GTE CyberTrust Global Root

Certificate Path Length

No limitation on Certificate Path Length applies.

Acceptable Certificate Policies

Only certificate policies are accepted that apply to Qualified Certificates stored on SSCD.

Naming constraints

No naming constraints apply.

Explicit Indication of the certificate policies

- eID
  - 2.16.56.1.1.1.2.1 (eID Citizen signing certificate)
  - 2.16.56.1.1.1.7.2 (eID Foreigner signing certificate)
- Certipost E-Trust
  - 0.3.2062.7.1.1.3.3.x (Certipost E-Trust qualified for qualified signatures for physical persons)
  - 0.3.2062.7.1.1.4.2.x (Certipost E-Trust qualified for qualified signatures for legal persons)
  - 0.3.2062.7.1.1.101.x (Certipost E-Trust qualified for qualified signatures for physical persons)
  - 0.3.2062.7.1.1.112.x (Certipost E-Trust qualified for qualified signatures for legal persons)
  - 0.3.2062.7.1.1.121.x (Certipost E-Trust qualified for qualified signatures for communities)

3.3.3.1.2. Revocation Requirements

Revocation status information on the Signer certificate should be validated in the following way:

- eID certificates: The OCSP service should be used. When the OCSP service cannot be used for whatever reason, full CRLs should be used.
- Certipost certificates: Full CRLs should be used.

Revocation status information on the CA certificates in the Signer certificate chain should be validated in the following way:

- eID certificates: The OCSP service should be used. When the OCSP service cannot be used for whatever reason, full CRLs should be used.
- Certipost certificates: Full CRLs should be used.

3.3.3.2. Timestamping

Time Stamping Authorities Public Key Rules

The certificate of the time stamping authorities public key should include the timestamping ExtendedKeyUsage (OID: 1.3.6.1.5.5.7.3.8).

Naming constraints

No naming constraints apply.

Cautionary Period

At the time of the creation of the signature XAdES-X-L format by the e-Signing service provider, a validation will be performed on the validity of the certificate used for signing. This includes the verification whether the certificate was not revoked or suspended during at the moment it was used for signing. Such verification is preformed by getting revocation information from the certificate issuer (CRL or OCSP). Some time goes by between the moment that the certificate was requested to be revoked and the time that the revocation services (CRL or OCSP server) publish this status. That means that there is a small risk that the revocation status collected during the creation of the XAdES-X-L is not correct (the certificate being considered valid while it is not). As a result there is a risk that the XAdES-X-L claims a valid signature, while in reality the signature is not valid.

A means to eliminate this risk is by waiting for a certain period (cautionary period or grace period) after the actual signature before creating the XAdES-X-L. If this grace period is larger then the time that it takes for the certificate status service to publish the revocation information the risk is completely mitigated. However in this Signature Policy, it was chosen not to impose such a grace period for the following reasons:

1. The certificates allowed by this Signature Policy are stored on an SSCD, which limits considerably the risk of abuse of a stolen or lost certificate.
2. Including a grace period would in most cases disrupt the normal flow of events in which the signature takes part in such a way that this would more then offset the positive effect of applying such grace period.
3. Even if the XAdES-X-L does not contain verification information from after such grace period, present signature policy requests the Verifier to verify the revocation data online to assess whether the signing certificate was not revoked or suspended at the time of signature.

Maximum Acceptable Time

Not applicable.

3.3.3.2.1. Certificate requirements

Belgacom E-Trust Root CA for Qualified Certificates

Certificate Path Length

No limitation on Certificate Path Length applies.

Acceptable Certificate Policies

There is no specific indication on the acceptable Certificate Policies.

Naming constraints

No naming constraints apply.

3.3.3.2.2. Revocation Requirements

Revocation status information on the timestamping certificate should be validated in the following way:

- Certipost certificates: Full CRLs should be used.

Revocation status information on the CA certificates in the timestamping certificate chain should be validated in the following way:

- Certipost certificates: Full CRLs should be used.

3.3.3.3. Attributes

No attribute signing is part of this signature policy.

3.3.3.4. Algorithm Constraints

Following Signer algorithm constraints apply to signatures created under this Signature Policy:

- The **Signing Algorithms** : One of the following algorithms should be used: RSA / SHA1, RSA/SHA256, RSA/SHA512
- **Minimum Key Length**: The Certificate Policies that are accepted define the minimum key length.

This signature policy does not define Algorithm Constraints on certificates or timestamping authorities.

3.3.3.5. Common Extensions

No common extensions have been defined in this signature policy.

3.4. Commitment Rules

Not applicable.

3.5. Signature Validation Policy Extensions

No Signature Validation Policy Extensions are applicable.

3.6. Area of application, Business Application domain, transactional context

This signature policy applies to the context of a Certipost *e-Signing Handwritten Equivalent* transaction.

3.7. Computer- processible vs. human-readable signature policy

Two formats of signature policies can be implemented: Computer-processible policy and human readable signature policy. From the developers point of view it would be convenient, if the policy is available in a computer-processible format. However, because it is the Signer that gives a commitment with regard to the content of the signed document as per this policy, there must always be a human readable version of the policy. Moreover, the Signer must be able to read the policy before creating a signature under it.
For the reasons we have expressed above, Certipost opted for a human-readable policy.

3.8. Explicit vs. implicit signature policy

The reference to a signature policy within a signed document may be either implicit or explicit. We opted for an explicit reference to the signature policy indicated by the Signer within the electronic signature (and thus protected by the electronic signature from the Signer). In this case, the benefit is to allow a processing of the electronic signatures, even long after they have been generated and outside their original context of use (e.g. in front of a judge).
The Signature Policy is identifiable by a unique identifier, e.g. an OID (Object IDentifier), and verifiable using a hash of the signature policy. So each time an electronic signature is generated, it includes within the signed document the unique identifier of the signature policy, the hash value of the signature policy and a location (URL)) where a copy of the Signature Policy may be obtained.

3.9. Certipost e-Signing Handwritten Equivalent signature policy publication

Before signing, a Signer should be sure which security policy will apply. In the same way, when verifying an electronic signature, a Verifier needs to make sure to use the correct security policy.
Certipost issues its own signature policies and make them available to end-entities by placing them on a secure web site (that can be accessed via SSL). By this way, an end-entity (a Signer or Verifier) has the guarantee that he is in possession of the genuine policy.

3.10. Certipost e-Signing Handwritten Equivalent signature policy archiving

In case the current version of this signature policy is superseded, the next version of the signature policy will identify the repository where the current signature policy version will be archived and how a Verifier can get access. This might be required for the verification of electronic signature created under the current signature policy version.

3.11. Certipost e-Signing Handwritten Equivalent signature policy conformance statements

The present Signature Policy claims conformance to ETSI TS 101 903, ETSI TR 102 041 and to the Belgian Law of 9th July 2001.

4. References

[1]: ETSI TR 102 041 (v1.1.1): “Signature policy report”.

[2]: ETSI TS ETSI TS 101 903 (v1.2.2): “XML Advanced Electronic Signatures (XAdES)”.

[3]: RFC 3280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.

[4]: EC 1999/93: European Community (EC) DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND COUNCIL ON A COMMUNITY FRAMEWORK FOR ELECTRONIC SIGNATURES

[5]: ETSI TR 102 045 (v1.1.1): “Signature Policy for Extended Business Model”.

[6]: The 9th of July 2001 Belgian Law about electronic signatures.