1. Introduction

1.1. Scope

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

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

Finally, the present document oversees the technical standards and operations used to create the electronic signatures through the Certipost *e-Invoicing* 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].

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

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.

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

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.
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 [3]

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 [3]).

Secure Signature Creation Device (SSCD): means a signature creation device that meets the requirements laid down in [3], 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 [3].

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.
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.

2. Certipost AES *e-Invoicing* Service

2.1. Certipost AES e-Invoicing actors

Sender: Entity that owns the invoice data and that issues / sends the electronic invoice (physical or legal person).

Certipost AES e-Invoicing Service Provider: Certipost AES e-Invoicing Service Provider is the entity that enables electronic invoice exchange between Customer organization's suppliers, buyers and other partners. Certipost can be service provider for the sender of the invoice, for the recipient of the invoice or for both parties.

Certipost e-Signing Service: Certipost e-Signing service is the service that signs on request of Certipost AES e-Invoicing Service Provider and validates on request of Certipost AES e-Invoicing Service Provider or on request of the receiver of the electronic invoice.

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.

2.2. Certipost AES e-Invoicing service description

The goal of the Certipost AES e-Invoicing Service is to enable the exchange of legal electronic invoices.

e-Invoicing stands for the automation of invoice processes and the efficient exchange of invoicing data between different applications. CertiONE e-Invoicing provides organizations with a virtual toolkit, making it possible to send invoices to buyers, to receive invoices from suppliers, translate them to any file format available, and to safely archive, search and consult your invoices.

The exchange of electronic invoices is subject to a regulatory framework within the European Union. According to the EU Directive (2006/112/EC of 28 November 2006 on the common system of value added tax), invoices sent by electronic means shall be accepted by Member States provided that the authenticity of the origin and integrity of the content are guaranteed by means of an advanced electronic signature or on the basis of the EDI method or any other method approved by the Member State. Certipost AES e-Invoicing service meets these legal requirements by applying an electronic signature method under this Signature Policy.

As a general rule, Certipost AES does not support the verification if the (external) sender uses an EDI method or any other method approved by the Member State in this context.

2.3. Certipost e-Signing service

The goal of Certipost e-Signing service is:

- to apply an advanced electronic signature on an electronic invoice on request of Certipost AES e-Invoicing Service in order to meet the legal requirements (EU Council Directive 2006/112/EC of 28 November 2006 on the common system of value added tax) in the different supported countries.
- to validate the signature on an electronic invoice The signature that is validated must not be placed by the Certipost e-Signing Service, but it does need to comply with the relevant signature policy.

2.4. Supported standard

The format of the invoices is PDF. The applied signature is a PDF signature using CMS (extended PKCS#7), i.e. a simple PKCS#7 signature with a reference to the signing certificate in the signed attributes. A signature timestamp is also added in the unsigned attributes.

2.5. Signature creation

The Signer can create a signature according to this Signature Policy using the Certipost e-Signing service.

On request of the Certipost AES e-Invoicing service Provider, the electronic invoice is signed with a qualified certificate stored on a Hardware Security Module, including a timestamp.

2.6. Signature verification

The Verifier can use any means to verify the signature created according to this policy. However, the following conditions must be met in order the Signature verification process is compliant with the present AES e-Invoicing Signature Policy:

1. Provide assurance that the signature is valid for the specified signed file.
2. Successful verification of the 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). (see section 3.3.4.2: Cautionary period)
3. Successful verification of the certificate used to sign is issued under an accepted Certificate Policy (see section 3.3.4.1.1 Certificate requirements).
4. Successful verification of the timestamp that was included in the signature

The Certipost e-Signing verification service implementation meets all these criteria, and is open for use to any Verifier. The Certipost e-Signing verification service is accessible via CertiONE interface, via the CertiONE archive, as an independent service or automatically called by the AES e-Invoicing Service.

3. Signature policy information

3.1. General

Following ETSI requirements[i], the Certipost AES e-Invoicing Signature Policy includes the following data:

3.1.1. Signature Policy Identifier:

- Signature Policy Name: Certipost AES e-Invoicing Signature Policy
- Signature Policy OID: 0.3.2062.7.2.1.2.1.0 (the last two digits define the major and minor versions of the signature policy respectively)
- Signature Policy URL: http://www.certipost.be/ddsolutions/download/AES_e-Invoicing_Signature_Policy_v1.0.pdf

3.1.2. Date of issue

10 November 2009

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

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

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

3.3.1. Rule for the Sender

3.3.1.1. Absence of time based dynamic content

The Sender is responsible that the file being signed does not contain any dynamic content that might modify the visualized result of the file over time (e.g. amounts or sentences that change after a certain date). The Sender must not include such dynamic content in any file the Sender creates that will be subject to use of the e-Signing service. In case the Sender 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,…

3.3.2. Rules for the Certipost e-Signing Service

3.3.2.1. Signed attributes

The following set of Signed Attributes will be provided by the Certipost e-Signing Service:

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

3.3.2.2. Unsigned attributes

The following set of Unsigned Attributes should be provided by the Certipost e-Signing Service. If not added by the Sender, 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)
- 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

3.3.3. Rules for the Verifier

3.3.3.1. 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 signature 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)
    - 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 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 signature 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 signature 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 signature structure (by hash comparison).

3.3.3.2. Unsigned attributes

The following set of Unsigned Attributes should be provided by the Verifier. If not added by the Sender, 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.
- Certificate values: Used in the verifications above.
- Certificate status references: Used in the verifications above.

3.3.4. Trust conditions

3.3.4.1. Signing Certificate

3.3.4.1.1. Certificate requirements

Depending of the applicable law on the electronic invoice, the acceptable certificate level is different.

Strongest level being a qualified certificate on SSCD.

Certificate Path Length

No limitation on Certificate Path Length applies.

Acceptable Certificate Policies

Depending on the applicable law to be complied with

- Either only certificate policies are accepted that apply to Qualified Certificates stored on SSCD.
- Or certificate policies are accepted that apply to Qualified Certificates.
- Or certificate policies are accepted that apply to non-Qualified Certificates.

Naming constraints

No naming constraints apply.

3.3.4.1.2. Revocation Requirements

Revocation status information on the Sender certificate and revocation status information on the CA certificates in the Sender certificate chain should be validated either via OCSP or via full CRLs.

3.3.4.2. Timestamping

Time Stamping Authorities Public Key Rules

The certificate of the time stamping authority's public key should include the timestamping Extended-KeyUsage (OID: 1.3.6.1.5.5.7.3.8).

The timestamping certificate will be compliant with the country law applicable on the electronic invoice.

Naming constraints

No naming constraints apply.

Cautionary Period

At the time of the creation of the signature by the Certipost e-Signing Service or by another Signature Service, 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 signature is not correct (the certificate being considered valid while it is not). As a result there is a risk that it claims a valid signature, while in reality the signature is not valid.

Maximum Acceptable Time

Not applicable.

3.3.4.2.1. Revocation Requirements

Revocation status information on the timestamping certificate and revocation status information on the CA certificates in the timestamping certificate chain should be validated should be validated either via OCSP or via full CRLs.

3.3.4.3. Attributes

No attribute signing is part of this signature policy.

3.3.4.4. Algorithm Constraints

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

- The **Signing Algorithms** : The signing algorithm shall be derived from applicable law. One of the following algorithms should be used: RSA / SHA1, RSA/SHA256, RSA/SHA512.
- **Minimum Key Length**: The Key length shall be derived from applicable law. The minimum key length is 1024 bits.

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

3.3.4.5. 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

Signatures created under this Signature Policy aim exclusively to ensure compliance with laws requiring integrity and authenticity of electronic invoices.

Signatures created under this Signature Policy do not express or imply Certipost's agreement with or approval of the semantics of the signed data. Certipost accepts no liability, for the accuracy, completeness, legality and compliance with applicable legal requirements concerning the content and format of business data signed under this Signing Policy.

3.7. 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 Sender within the electronic signature (and thus protected by the electronic signature from the Sender). 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.

3.8. Certipost AES e-Invoicing signature policy publication

Before signing, a Sender 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 Sender or Verifier) has the guarantee that he is in possession of the genuine policy.

3.9. Certipost AES e-Invoicing 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.

3.10. Certipost AES e-Invoicing signature policy conformance statements

The present Signature Policy claims conformance to ETSI TR 102 041 [1].

4. References

[1] ETSI TR 102 041 (v1.1.1): “Signature policy report”.
[2] RFC 5280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”.
[3] EC 1999/93: European Community (EC) DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND COUNCIL ON A COMMUNITY FRAMEWORK FOR ELECTRONIC SIGNATURES