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 "IFY e-Signing Automated for scanned invoices", provided by the Certipost e-Signing Automated service. The use of "IFY e-Signing Automated for scanned invoices" is limited to a Certipost invoice scan & capture scheme.

Moreover, the present document sets the roles and obligations of all actors involved in signing actions in this context. These rights and obligations for entities involved in these actions are stated in the form of both contractual obligations and technical requirements.

Finally, the present document gives an overview of the technical standards and operations used to create the electronic signatures through the "Certipost e-Signing Automated" 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

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.

Conforming signature handler: software application, or part of a software application, that knows how to perform digital signature operations (e.g. signing and/or verifying) in conformance with ISO 32000-1 [1] and the requirements of the appropriate profile

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 map to this output
- It is computationally unfeasible to find for a given input a second input which maps to the same output

certipost
a bpost company

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.

PDF Conforming signature handler: software application, or part of a software application, that knows how to perform digital signature operations (e.g. signing and/or verifying) in conformance with ISO 32000-1 [1] and the requirements of the appropriate profile

PDF document creator: entity that creates a PDF document

PDF signature: binary data object based on the CMS (RFC 3852 [4]) or related syntax containing a digital signature placed within a PDF document structure as specified in ISO 32000-1 [1], clause 12.8 with other information about the signature applied when it was first created

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]).

Signer: entity that creates an electronic signature

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

Seed value dictionary: PDF data structure, of type dictionary, as described in ISO 32000-1 [1], clause 12.7.4.5, table 234, that contains information that constrains the properties of a signature that is applied to a specific signature field

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

certipost
a bpost company

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 Time-stamp: A time-stamp (see below) in a container for a time-stamp token over the Signature Value to protect against repudiation in case of a key compromise. This time-stamp is evidence that the signature existed before the asserted time and can be used to prove the signature's validity after the expiration, revocation or compromise of the signing certificate. The process for time-stamping a digital signature is described in RFC 3161.

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.

Verifier: entity that validates an electronic signature

certipost
a bpost company

1.4. IFY e-Signing Automated for scanned invoices Actors

Document Creator: IFY will create electronic images of scanned invoices in PDF format in accordance with [5] and minimally version PDF 1.7. Though this is out of the scope of this signature policy, IFY will perform the process of scanning and signing in accordance with the prevailing laws and regulations (for example see the regulation on Invoice Scan & Capture [10]).

Document Signer: This is IFY. The electronic signing action will take place on the Certipost Signing Service by means of a web service call and a secured access to that web service.

Certipost e-Signing Automated (CEA): This service is integrated with the IFY invoice scanning application. CEA makes use of the Certipost Signing Service (CSS).

Certipost Signing Service (CSS): Certipost Signing Service is the service that helps sign the documents created by the document creator and signed by the document signer.

Client: The eventual receiver of the document is the client to whom the scanned invoice is directed.

Verifier of signature (verifier):

Certipost will act as a signature verifier in order to assure that the received invoice is a scanned invoice from IFY and that its contents have not been changed.

Anybody, including the client, can act as the verifier by making use of a PDF Conforming signature handler, however there are some limitations to this described in the Signature Validation section.

1.5. Supported standard

The scanned invoice will be in a PDF version compatible with ISO 32000-1 see [5] and in conformance with the requirements in ETSI TS 102 778-3 V1.2.1 (2009-07) [4].

The applied signature is a PDF approval signature which also qualifies as a PAdES signature according to the PAdES-BES profile specified in ETSI TS 102 778-3 V1.1.1 (2009-07) [4] and is categorized as an 'approval signature' by ISO 32000-1 [5].

- The signature includes a signature time-stamp which is added during the signing operation.
- The signature includes a Signing Time signed property.
- The signature includes the signer certificate and all intermediary certificates forming a chain between the signer certificate and a CA

- The signature does not include visual representations of the signature in the document as this would change the appearance of the complete document in comparison with the originally scanned document.
- The signature does not include the revocation information in the signature at the time of signing.
- No other optional properties or attributes are included either. This also is in accordance with ISO 32000-1 [5].

1.6. Signature creation

The signer can create a signature according to this Signature Policy using the Certipost e-Signing Automated (CEA) service.
The rules that apply are defined in the section 3 (Signature Policy Information)

1.7. Signature verification

The verifier can use any means to verify the signatures created according to this Signature Policy.
However, the detailed rules and conditions that must be met in order that the signature verification process is compliant with the present Signature Policy are specified in section 3 (Signature Policy Information).

2. Signature policy information

2.1. General

Following ETSI requirements[1], this Signature Policy includes the following data:

2.1.1. Signature Policy Identifier:

- Signature Policy Name: IFY e-Signing Automated for scanned invoices
- Signature Policy OID: 0.3.2062.7.2.1.13.1.0
- Signature Policy URL: http://www.certipost.com/download/trust/SP_CTP_CEA_IFY_Scanned_invoices_v1_0.pdf

2.1.2. Date of issue

31/01/2012

2.1.3. Signature Policy Issuer name:

Certipost sa/nv
- Contact details:

Registered office: Certipost s.a/n.v. • Centre Monnaie / MuntCentrum • B-1000 Bruxelles / Brussel

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

certipost
a bpost company

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

2.2. Signature Policy validity period

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

2.3. Signature creation and verification rules

2.3.1. Rules for the document creator

2.3.1.1. Absence of time-based dynamic content

The document creator is responsible for ensuring 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 document creator must not include such dynamic content in any file it creates that will be subject to use of the Certipost e-Signing Automated Service.

2.3.2. Rules for the signer

2.3.2.1. Signature / Signing Certificate

The signing will be done on the CSS server at Certipost with a normalized certificate. IFY will be the certificate holder, with the rights, responsibilities and obligations of the Certificate Holder.

2.3.2.2. Commitment type is “authorship and attribution”

The commitment type is not explicitly specified in the the signature. Making use of the IFY application and via this application the Certipost e-Signing Automated Service implies that the signer (the entity representing IFY) makes a certain commitment when signing the files. Because of this, only the IFY application in this form should make use of the Certipost e-Signing Automated Service with the same context and signing certificate. The commitment type is implied by the signing certificate and the timestamp which indicates the time before which the signing took place.
The assumed commitment is: “authorship and attribution” as specified in [8]
For IFY this means that the electronic signature certifies:

- the integity of the scanned invoices in the PDF file after the time indicated by the timestamp
- that the “author” of the document is IFY and IFY states that this document was created in accordance with the relevant legal requirements and regulations.
- that the electronically signed document containing the scanned invoices can be used as evidence solely in the context of scanned inbound invoices as long as it complies with the legal requirements and regulations.

certipost
a bpost company

- that IFY makes no further commitment with the signature and the legality of the signature is non-existant for other purposes

2.3.2.3. Revocation Information

Revocation information is not included in the ***adbe-revocationInfoArchival*** attribute at the time of signing. Since this information is collected at the time of signing a verifier should not rely on this information.

2.3.2.4. Location of signing

The location of signing is not explicitly stated in the signature, but is assumed that this at any location within the Belgian legal jurisdiction.

2.3.2.5. Role or authority of the signer

This is not explicitly specified in the the signature. In order to assume that the signature was created by an entity that has the authority to create the signature, it needs to conform with the signature validation rules.

2.3.2.6. Time of signing

The time of signing is asserted by the signed property "Signing Time". This is a claimed time of the application. The signature time-stamp does assure that the signing took place before the indicated time in the signature time-stamp. Provided that the signing and time-stamping took place immediately after the scanning of the document, this time is a reliable approximation of the scanning time.

2.3.2.7. Signature-policy-identifier Attribute

This attribute is not used. However, the signature policy is implied by the signing certificate, the contents of the signed object, and the timestamp which indicates the time before which the signing took place.

2.3.2.8. Signed attributes (and Seed Values)

The following values are used:

- Name (Contact info of the signatory): Input for You sa/nv
- Location (Description of the location of signing): "Belgium"
- Reason: "Scanid = "*scanid reference*"This signature certifies the integrity of the electronic invoice from the time indicated in the time-stamp. The authenticity of the scanning party that scanned the invoice and converted it into this digital format is also certified "

2.3.2.9. Unsigned attributes

No other optional unsigned attributes will be provided in this context.

2.3.2.10. Access to the service

Access to the CEA service is secured and controlled by SSL with mutual authentication and an additional context parameter configuration.
The client certificates used for the SSL connections are subject to the relevant Certificate Policies and the appropriate Certificate Practice Statement. IFY is required to fulfill the responsibilities and obligations of the Certificate Holder.
The accepted client certificate will be identified with:

- LP Normalized Certificate without SSCD with key generation by the owner (OID= 0.3.2062.7.1.1.211.x)

certipost
a bpost company

cn = Input for You n.v. KBO 0473 984 560 – (Access)
c=Belgium
l= Sint-Agatha-Berchem
o= Input for You n.v.

IFY is also expected to exercise due diligence in securing the application and access to the server it is hosted on in order to protect the second layer of access control to CEA.
Any suspensions or revocations of the SSL client certificates will be logged by the Certification Service Provider (CSP).
During the time a particular SSL client certificate is invalid (suspended, revoked, expired…) no signature requests for qualified signatures will be accepted for the associated context. As soon as a revocation or suspension request has been made for a certain SSL client certificate, IFY should not attempt to use the service for signing with a connection where the client side is authenticated with that certificate until the suspension or revocation has come into effect or a un-suspension request has been approved. The signing certificate itself is not affected by this.

2.3.3. Rules for the verifier of signature (further on called 'verifier')

There are two methods for the verification of this signature: one relies on CEA and the second on a PDF conforming signature handler (like Acrobat Reader from a sufficiently high software version, namely Adobe Reader X). The verification in CEA follows the general rules below. For verification in a PDF conforming signature handler additional steps are given in the next section.

The general rules for the verification of the signature are:

1. Step 1: Follow the general guidelines in "4.6 Signature Validation" in [4] which means for this policy that the validation shall:

   a) Compare the hash value of signer's certificate, with the hash value given in the ESS signing-certificate-v2 attribute. If the hash value does not match the value in the attribute, the verifier should return an incomplete validation response. The validation rules found in RFC 5035 [7] clause 2 and clause 8 apply.
   b) Verify that the document digest matches that in the signature as specified in ISO 32000-1 [5], clause 12.8.1.
   c) Validate the path of certificates used to verify the binding between the subject distinguished name and subject public key as specified in RFC 3280 [6].
   The validity checks shall be carried out at the time indicated by the time-stamp applied as per clause 4.5.2. The revocation status shall be checked as specified in clause 4.6.4 of [4] but ignoring any embedded revocation information in favor of the Certificate Revocation List (CRL) method.

2. Step 2: Successful verification of the validity of the certificate at the time of the validity check: certificate not revoked or suspended, certificate not expired and already valid, full certificate chain validation (including validation of all certificates in the chain).

a. This validation requires the availability of revocation information which renders the true status of the certificate. Because there can be a delay between the reporting of a certificate that needs to be revoked or suspended and the actual availability of this information, the revocation checking is subject to a 'grace period'.

   i. If the revocation checking takes place before the end of that grace period then the status cannot be guaranteed with certainty. When the verifier cannot obtain such status information the verification is incomplete and should be tried again at a later time.

   ii. If the revocation checking takes place later after the "grace period":

      1. When performing verification before expiration of the signature certificate: In case this verification shows the certificate being revoked or suspended, the verifier should not trust the signature.

      2. Performing verification after expiration of the signature certificate: This is not to be accepted in this context. The verification cannot be executed with a sufficient degree of certainty.

3. Step 3: Successful verification of the certificate used to sign is issued under an accepted Certificate Policy (see section 2.3.4.1.1 Certificate requirements).

2.3.3.1. Verification in Acrobat Reader: additional steps

As described above, when using a suitable version of Acrobat Reader (Adobe Reader X), the signature can be checked up to the cryptographic validity of the electronic signature (steps 1 and 2).
Additional manual steps to complete the validation are needed.
The step of verification that the certificate used to sign is issued under an accepted Certificate Policy needs to be performed manually, by checking the signature certificate.
Please refer to the "Trust Conditions" in section 2.3.4 for details.
The trust conditions in the native environment are not in accordance with the Trust-service Status List (TSL) published by the national authorities, which is an official list published in accordance with EU recommendations and standards (see [9]). Because of this:

- The Adobe Readers may need to be configured to enable searching the Windows Certificate Store in order for the signature certificate to be trusted
- Further manual steps are needed to verify the additional trust conditions of this signature policy

2.3.4. Trust conditions

2.3.4.1. Signing Certificate

2.3.4.1.1. Certificate requirements

It shall be a normalized certificate hosted by Certipost on HSM with the following specifications:
Certificate Path Length
No limitation on Certificate Path Length applies.

Acceptable Certificate Policies

Only certificate policies are accepted that relate to Normalized Certificates and are used by legal persons. The accepted OID is:

- 0.3.2062.7.1.1.211.x

Naming constraints

The certificate's DN should include:

cn = Input for You n.v. KBO 0473 984 560 – (Sign)
c=Belgium
l= Sint-Agatha-Berchem
o= Input for You n.v.

2.3.4.1.2. 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 via full CRLs.

2.3.4.2. Algorithm Constraints

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

- The **Signing Algorithms:** The signing algorithm shall be minimum RSA / SHA1.
- **Minimum Key Length**: The Key length shall be minimum 2048 bits.

This signature policy does not define other Algorithm Constraints on certificates.

2.3.4.3. Common Extensions

No common extensions have been defined in this signature policy.

2.4. Commitment Rules

Commitments are not explicitly incorporated in the signatures and therefore no commitment rules apply. Instead the commitments are implied by the context (see 3.3.4.1)

2.5. Signature Policy Extensions

Not applicable.

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

Signatures created under this Signature Policy aim exclusively to create an electronically signed document containing scanned invoices that can be used as evidence solely in the context of scanned inbound invoices as long as it complies with the legal requirements and regulations.

The commitment type category of the signature is "authorship and attribution" as specified in [8].

The format of the signature is not a format for long term validity (LTV).

The intrinsic validity of the signatures is limited in time by the expiry of the signing certificate.
The preservation of the document and the electronic signature beyond this time and the other obligations that may exist from a legal perspective in this context are the responsibility of the receiver.

Signatures created under this Signature Policy also do not express or imply Certipost's or document signer'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.

2.7. Explicit vs. implicit signature policy

The reference to a signature policy within a signed document may be either implicit or explicit. In this case there is an implicit reference to the signature policy indicated by the signer's use of the application because explicit policy formats in accordance with ETSI ESI (-EPES) are not yet supported by PDF conforming signature handlers in the scope of the standard ISO 32000-1.

2.8. Signature policy publication

Before signing, the signer should know which security policy will apply. In the same way, when verifying an electronic signature, a verifier needs to make sure to use the correct signature policy.
Certipost issues its own signature policies and makes 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.

IFY ensures that all the participating parties are aware of the relevant signature policy and that they agree with its contents. However, in accordance with legislation that deals with the enforceability of standard contract terms or "small print", and providing the terms are reasonable and the party wishing to rely on the terms draws them to the intention to the party to be bound by them and makes them readily available to read, then they will be binding regardless of whether the signer actually read by them. Therefore IFY is responsible for publishing this signature policy.

2.9. 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.

Versions are indicated by the two last digits in the OID of the signature policy. However, every version constitutes in effect a different signature policy.

certipost
a bpost company

2.10. Signature policy conformance statements

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

3. 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
[4] ETSI TS 102 778-3 V1.1.1 (2009-07): "Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles"
[5] ISO 32000-1:"Document management - Portable document format - Part 1: PDF 1.7".
[6] IETF RFC 3280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".
[7] ETSI TS 102 778-1 V1.1.1 (2009-07): Electronic Signatures and Infrastructures (ESI);PDF Advanced Electronic Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES
[8] ETSI TR 102 045 V1.1.1 (2003-03): Electronic Signatures and Infrastructures (ESI); Signature policy for extended business model
[9] ETSI TS 102 231 V2.1.1 (2006-03): Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information
[10] Circulaire nr. AOIF 16/2008 (E.T.112.081) dd. 13.05.2008