	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy		Approval status: Released

REVISION HISTORY			
Rev	Description of Change	Author	Effective Date
1.0	First released version	ODO, MBH	04/03/2003
1.1	New Certificate Policy supported	ODO	27/03/2003
1.2	Extension validity EID supported	BCL	30/06/2003
2.0	Extension validity Adaptation of Certificate Policies supported Hybrid Registered Mail supported	BCL	1/1/2004
2.1	Adaptation of Certificate Policies supported	BCL	4/5/2004

1 Introduction

1.1 Scope

This document is intended to cover policy rules that can be used to state under which conditions an electronic signature generation and validation methods are valid when used within the context of a Certipost electronic Registered Mail (REM) transaction.

Moreover, the present document sets the roles and obligations of all actors involved in a REM transaction. These rights and obligations for entities involved in a REM transaction 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 digital signatures that are used within the context of a REM transaction.

1.2 Organisation of the document


The organization of this document is based on from the signature policy framework as defined in ETSI TR 102 041 v1.1.1: "Signature policy report" and ETSI TR 102 045: "Signature Policy for Extended Business Model".

1.3 References

- [1]: ETSI TR 102 041 (v1.1.1): "Signature policy report".
- [2]: ETSI TS 101 733 (v1.2.2): "Electronic signature formats".
- [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

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy		Approval status: Released

- [5]: ETSI TR 102 045: "Signature Policy for Extended Business Model".
- [6]: The 9th of July 2001 Belgian Law about electronic signatures.

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy	Approval status: Released	Page #: 3 of 21

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]

Commitment Type: a signer-selected indication of the exact intent of an electronic signature.


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.

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

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

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy	Approval status: Released	Page #: 4 of 21

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 which 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.

Online Certificate Status Provider: an on line trusted source of certificate status information.

Parallel signatures: 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.

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy	Approval status: Released	Page #: 5 of 21

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.

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 integer for each newly generated time stamp, an identifier to uniquely indicate the security 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 Stamping Authority: An authority trusted by one or more users to provide a Time Stamping Service.


Time Stamping 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. This may be either a relying party or a third party interested in the validity of an electronic signature.

What Is Presented is What Is Signed (WIPIWIS): a description of the required qualities of the interface able to unambiguously present the signer's document to the verifier according to the content format of the signer's document.

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy	Approval status: Released	Page #: 6 of 21

2 Certipost Registered Mail (REM) Service

2.1 Certipost REM actors

MyCertipost subscribers: The creation and the sending of an electronic registered mail is only accessible to MyCertipost subscribers. A MyCertipost subscriber can send and receive electronic registered mails. Someone who is not a MyCertipost subscriber can only receive paper based registered mail. A MyCertipost subscriber is someone who has a MyCertipost account, who is correctly identified and who has performed a first login on the MyCertipost platform

MyCertipost account: A secure identified electronic communication account, obtained after a registration process, guaranteeing the identity of the user.

MyCertipost REM senders: It is a MyCertipost subscriber who creates and sends an electronic registered mail, sent to a MyCertipost REM recipient (see below).

MyCertipost HREM senders: It is a MyCertipost subscriber who creates and sends an electronic registered mail, intended for a MyCertipost HREM recipient (see below).


MyCertipost REM recipients: It is a MyCertipost subscriber who is the recipient of an electronic registered mail.

MyCertipost HREM recipients: It is not a MyCertipost subscriber. It can only receive paper based registered mail.

Certipost REM service provider: Certipost REM service provider acts as a delivery channel guaranteeing the fair and secure REM transaction execution between either a REM sender and a (multiple) REM recipient(s), either a HREM sender and a (multiple) HREM recipient(s), either a combination of both. Remark that the service Certipost delivers does not include the paper based delivery of an electronic sent registered mail. This paper based registered mail service is delivered by the De Post/La Poste and is subject to the general conditions of the De Post/La Poste.

2.2 REM operations summary (REM Sequence Diagram)

This chapter describes the REM operations.

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
		Title: Certipost Registered Mail Signature Policy	Approval status: Released

2.2.1 In case of a MyCertipost REM recipient

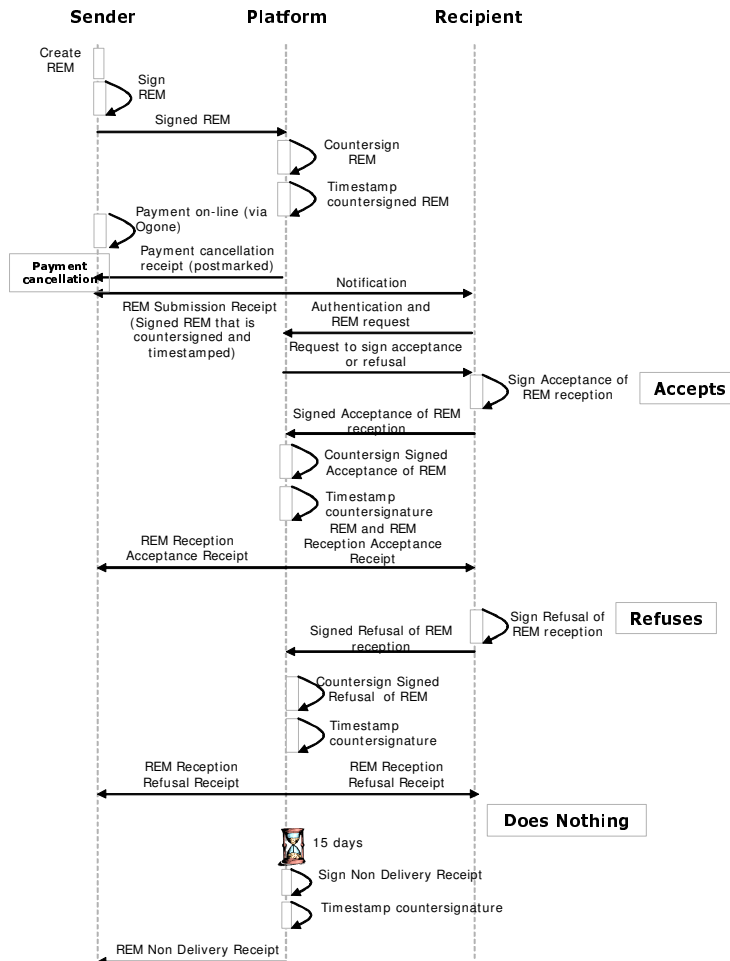



Figure 1: Certipost Registered Mail (REM) Sequence Diagram.

Course of events:


Sender creates its Registered Mail (REM). He then signs this REM and submits this signed REM to the Platform. The Platform countersigns this signed REM and proceeds to the Timestamping of this countersignature. The sender performs an on-line payment for the sending of the REM (via ogone). In case the sender cancels the payment, a payment cancellation receipt is sent to the sender. If not, the Platform sends a notification to the recipient(s). The recipient authenticates and requests access to the received REM. Three possibilities are offered to the recipient:

1. The recipient accepts the download of the received REM: He then has to sign the acceptance of download, which is submitted to the Platform that countersigns and proceed to the Timestamping of this countersignature. This results in a "REM electronic Reception Acceptance Receipt" that is provided to the sender and the signing recipient. The REM is made available to the signing recipient.

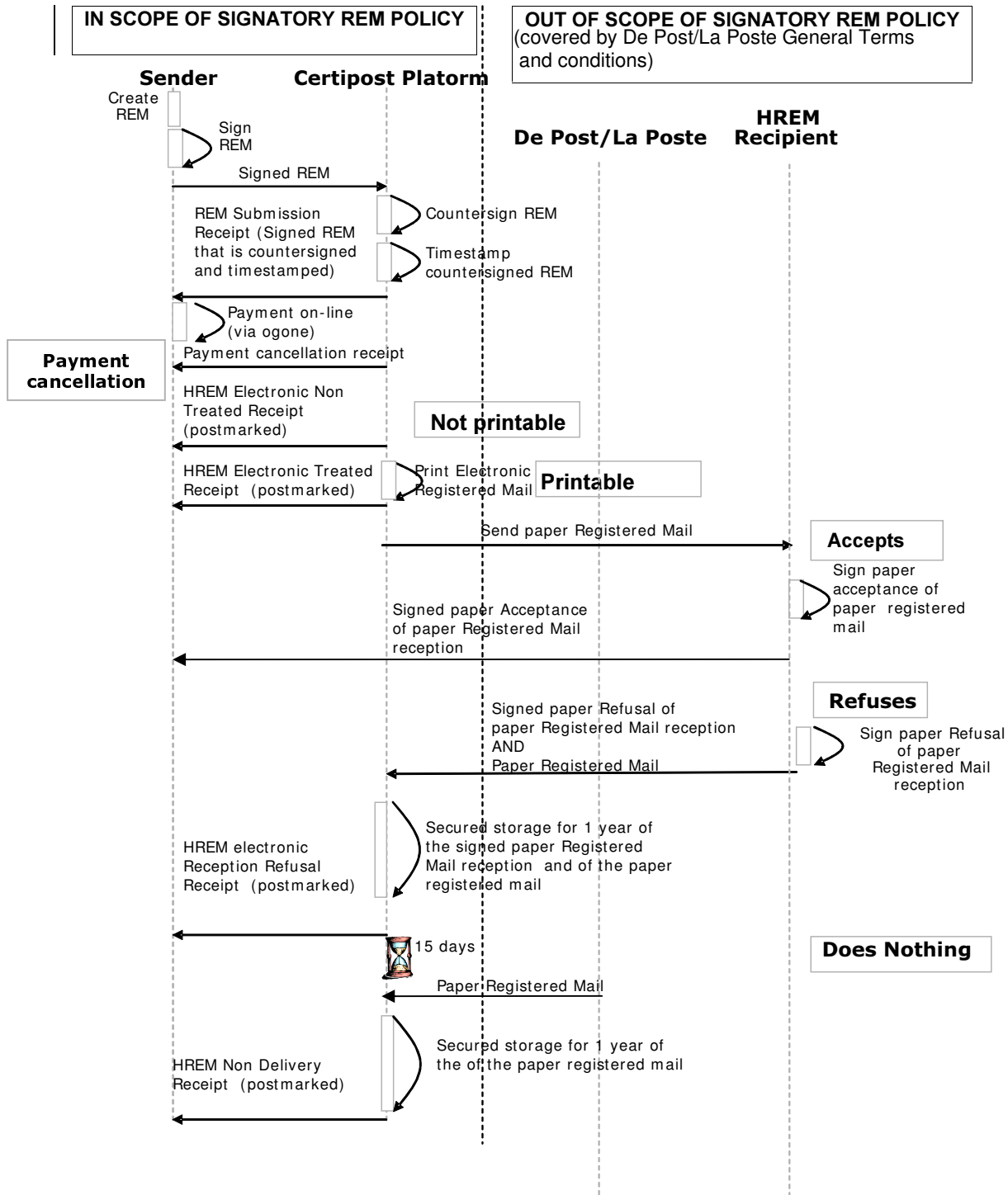
	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy	Approval status: Released	Page #: 8 of 21


2. The recipient refuses the download of the received REM: He then has to sign the refusal of download, which is submitted to the Platform that countersigns and proceed to the Timestamping of this countersignature. This results in a “REM electronic Reception Refusal Receipt” that is provided to the sender and the signing recipient.

3. The recipient does nothing regarding the received REM: After the retention period of 15 days, the Platform will then create a “Non Delivery Receipt”, sign it and proceed to the Timestamping of this signed receipt. This results in the provision of a “REM electronic Non Delivery Receipt” to the sender.

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy		Approval status: Released

2.2.2 In case of a MyCertipost HREM recipient



	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy	Approval status: Released	Page #: 10 of 21

Course of events:

Sender creates its Registered Mail (REM). He then signs this REM and submits this signed REM to the Platform. The Platform countersigns this signed REM and proceeds to the Timestamping of this countersignature. The sender performs an on-line payment for the sending of the REM (via Ogone). In case the sender cancels the payment, a payment cancellation receipt is sent to the sender. If not, Certipost prints the REM. In case the REM is not printable, a HREM electronic Non treated receipt is sent to the HREM sender. If the printing is successful, Certipost sends the paper registered mail via the De Post/La Poste to the HREM recipient(s). The HREM recipient authenticates and requests access to the paper registered mail. Three possibilities are offered to the HREM recipient:

1. The recipient accepts to receive the paper registered mail : He then has to sign the paper acceptance of the paper registered mail, which is submitted via the De Post/La Poste directly to the HREM sender.
2. The recipient refuses to receive the paper registered mail : He then has to sign the paper refusal of the paper registered mail, which is submitted via the De Post/La Poste to Certipost, who proceeds to the secured storage of the paper refusal of the paper registered mail. An electronic reception refusal receipt (postmarked) is delivered to the sender by the Certipost platform.
3. The recipient does nothing regarding the received paper registered mail : After the retention period of 15 days, De Post/La Poste sends the paper registered mail to Certipost. Certipost proceeds to the secured storage of the paper Registered Mail. The Platform will then create a "Non Delivery Receipt", sign it and proceed to the Timestamping of this signed receipt. The electronic Non Delivery Receipt is delivered to the sender by the Certipost platform.

2.3 REM digital receipts summary

2.3.1 Electronic Submission Receipt

A file created by Certipost and transmitted to the sender of a REM as a confirmation that his REM was successfully received.

2.3.2 REM Payment Cancellation Receipt

A file created by Certipost and transmitted to the sender of a REM as a confirmation that the Payment of his REM is cancelled.


2.3.3 REM Electronic Reception Acceptance Receipt

A file created by Certipost and transmitted to the REM sender and REM recipient as a confirmation that the intended REM recipient has successfully accepted to receive the REM.

2.3.4 REM Electronic Reception Refusal Receipt

A file created by Certipost and transmitted to the sender and recipient of a REM as a confirmation that the intended REM recipient has successfully refused to receive the REM.

2.3.5 REM Electronic Non-Delivery Receipt

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy	Approval status: Released	Page #: 11 of 21

A file created by Certipost and transmitted to the sender of a REM as a confirmation that his REM was unsuccessfully delivered to the intended recipient because this latter never performs any action neither to accept nor to refuse the REM.

2.3.6 HREM Electronic Non Treated receipt

A file created by Certipost and transmitted to the sender of a HREM as a confirmation that his HREM was not successfully printed by Certipost.

2.3.7 HREM Electronic Treated Receipt

A file created by Certipost and transmitted to the sender of a HREM as a confirmation that this HREM was successfully printed by Certipost and handed over to De Post/La Poste.

2.3.8 Paper Reception Acceptance Receipt

A paper document created by the De Post/La Poste, signed by the HREM Recipient and transmitted to the HREM sender by the HREM Recipient via the De Post/La Poste as a confirmation to the HREM sender that the intended recipient has successfully accepted to receive the HREM.

2.3.9 Paper Reception Refusal Receipt

A paper document created by the De Post/La Poste, signed by the HREM Recipient and transmitted to Certipost by the HREM Recipient as a confirmation to Certipost that the the intended recipient has successfully refused to receive the HREM.

2.3.10 HREM electronic reception refusal receipt

A file created by Certipost and transmitted to the sender as a confirmation that the intended HREM recipient has successfully refused to receive the HREM.


2.3.11 HREM electronic reception Non-Delivery receipt

A file created by Certipost and transmitted to the sender of a HREM as a confirmation that his HREM was unsuccessfully delivered to the intended HREM recipient because this latter never performed any action neither to accept nor to refuse the HREM.

2.4 REM digital signature operations summary

2.4.1 Signature generation operations

Acting party	Signature operation
REM Sender	Signature for REM submission
Platform	Countersignature of submitted REM in the context of creation of REM Submission Receipt
REM Recipient	Signature in the context of Reception Acceptance
Platform	Countersignature of recipient signed acceptance in the context of creation of REM Reception Acceptance Receipt
REM Recipient	Signature in the context of Reception Refusal
Platform	Countersignature of recipient signed refusal in the context of creation of

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy	Approval status: Released	Page #: 12 of 21


	REM Reception Refusal Receipt
Platform	Signature in the context of creation of REM Non-Delivery Receipt

2.4.2 Signature verification and validation operations

The signature verification and validation operations include the followings:

- Verify that the certificate is trusted, i.e., the certificate is part of the recognised certificate types as described in section 3.10.1.3.
- Verify the key usage extension: The key usage extension must be present and the NonRepudiation bit set.
- Verify the signature as such
- Validate the certificate chain with regards to possible suspension or revocation. OCSP validation method is used towards the recognised certificate types.

The Signature verification and validation operations, related to the paper registered mail process (HREM) falls beyond the scope of the Certipost Registered Mail. These operations are governed by the De Post/La Poste General Terms and Conditions.

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy		Approval status: Released

3 Signature policy general information

3.1 General contents of Certipost REM signature policy

Following ETSI requirements¹, Certipost REM signature policy includes the following data:

- the name of the issuer of the policy
- the unambiguous unique identifier of the policy
- the date the policy was issued
- the area of application of the policy document
- the signing period of the policy
- the signature validation policy part supplies information that supports a verifier to determine the validity of a signature.

A very important part specifies which certificates from what certification authorities are considered trusted. This includes certificates for signers, certification authorities and for timestamp authorities as well. Certipost REM signature policy (the present document) provides a detailed list of trusted certificates in section 3.10.1. This list will be extended in the future.

The validation policy specifies the information about which revocation information a verifier must collect when checking the status of certificates. Certipost REM signature policy (the present document) provides a detailed list of trusted Certification Authorities in section 3.10.1.1.

A certificate policy can additionally hold a list of allowed commitment types. A signer has the option to sign data and to give a special type of commitment. A commitment type may for instance express that the signer received the content, which he took note of the content or that he approves of the content. Certipost REM signature policy (the present document) provides a detailed list of Signature Commitment Types in section 3.10.2.

In addition, the policy can state rules for the use of timing information like timestamps or it might set constraints on admissible algorithms.

The whole signature policy must be authentic; the issuer can achieve this by signing his policy or he can provide access via secure and authenticated connections using TLS or SSL for instance.


3.2 Title / identification of the signature policy

- Issuer name: Certipost sa/nv
- Issuer contact details:
s.a. Certipost n.v. • Centre Monnaie / MuntCentrum • B-1000 Bruxelles / Brussel
Tel: +32 2 209 99 00 • Fax: +32 2 209 99 01
TVA – B.T.W. BE 475.396.406 • RC Bruxelles / HR Brussel 652.060
- Issuer OID: 0.3.2062.9.6.10 (*temporary OID as subsidiary of Belgacom s.a.*)
- Policy OID: 0.3.2062.9.6.10.1.1.1.2.1
- Available from: www.certipost.be

Paper or Hard copy is available from: feedback.nl@contact.certipost.be or feedback.fr@contact.certipost.be .

3.3 Area of application, Business Application domain, transactional context

¹ Specified in reference document [1]: ETSI TR 102 041 (v1.1.1): "Signature policy report.

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy		Approval status: Released

This signature policy applies to the context of a Certipost electronic Registered Mail (REM) transaction.

3.4 Signature policy applicable period

- Date of issue: **4/5/2004**
- Signing period: **no later than 4/11/2004**

3.5 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 will be convenient, if the policy is available in a computer-processible format. However, because it is the signer that gives a commitment under this policy, there must always be a human readable version of the policy. Moreover, the signer must have the option to read the policy before creating a signature under it.

For the reasons we have expressed above, Certipost opted for a human-readable policy.

3.6 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 digital 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 will include the unique identifier of the signature policy and the hash value of the signature policy (and might also include a location (URL)) where a copy of the Signature Policy may be obtained within the signed document.

3.7 REM 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.

3.8 REM signature policy archiving

The archiving period for REM related items is of thirty (30) years. These archived items shall be digitally notarised.

3.9 REM signature policy conformance statements

The present Signature Policy claims conformance to ETSI TS 101 733, ETSI TR 102 041, and ETSI TR 102 045 and to the Belgian Law of 9th July 2001.

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy	Approval status: Released	Page #: 15 of 21

3.10 REM certificate policy in details

3.10.1 End-user supported certificates

3.10.1.1 Supported Certification authorities

Certipost REM service supports end-entity digital certificates issued by the following Certification Authorities :

- **Belgacom E-Trust Primary CA for Qualified Certificates**

DN:

C=be
O=Belgacom
OU=E-Trust
CN=Belgacom E-Trust Primary CA for Qualified Certificates

Signed by:

- **Belgacom E-Trust Root CA for Qualified Certificates**

DN:

C=be
O=Belgacom
OU=E-Trust
CN=Belgacom E-Trust Root CA for Qualified Certificates

- **Belgacom E-Trust Primary CA for Normalised Certificates**

DN:

C=be
O=Belgacom
OU=E-Trust
CN=Belgacom E-Trust Primary CA for Normalised Certificates

Signed by:

- **Belgacom E-Trust Root CA for Normalised Certificates**

DN:

C=be
O=Belgacom
OU=E-Trust
CN=Belgacom E-Trust Root CA for Normalised Certificates

- **Certipost E-Trust Primary CA for Qualified Certificates**

DN:


C=be
O=Certipost
CN=Certipost E-Trust Primary CA for Qualified Certificates

Signed by:

- **Belgacom E-Trust Root CA for Qualified Certificates**

DN:

C=be
O=Belgacom
OU=E-Trust

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy		Approval status: Released

CN=Belgacom E-Trust Root CA for Qualified Certificates

- **Certipost E-Trust Primary CA for Normalised Certificates**

DN:
 C=be
 O=Certipost
 CN=Certipost E-Trust Primary CA for Normalised Certificates

Signed by:

- **Belgacom E-Trust Root CA for Normalised Certificates**

DN:
 C=be
 O=Belgacom
 OU=E-Trust
 CN=Belgacom E-Trust Root CA for Normalised Certificates

- **Citizen CA**

DN:
 C=be
 CN=Citizen CA

3.10.1.2 Supported Certificate Profiles


Certipost REM service supports end-entity digital certificates having the following profile:

- Standard X.509 v3 certificates
- Certificate issued under a face-to-face procedure
- The key-usage extension field shall be present having its NR bit set
- Certificate issued under a recognised Certificate Policy (CP)


3.10.1.3 List of Recognised and Accepted Certificate Policies / Certificate Types

This list of recognised and accepted Certificate Policies or Certificate types is limited to the following:

- **Belgacom E-Trust FRNB Qualified Certificate for Qualified Digital Signature Only**
 - Qualified Certificate with SSCD (OID ETSI 101 456): **0.4.0.1456.1.1**
and Key Generation by CSP: **0.3.2062.9.6.1.26.3.x**
- **Belgacom E-Trust Lawyer's Qualified Certificate for Qualified Digital Signature Only**
 - Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2**
and Key Generation by Owner : **0.3.2062.9.6.1.15.2.x**
 - Qualified Certificate with SSCD (OID ETSI 101 456): **0.4.0.1456.1.1**
and Key Generation by CSP: **0.3.2062.9.6.1.15.3.x**


	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy	Approval status: Released	Page #: 17 of 21

- Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Key Generation by CSP: **0.3.2062.9.6.1.15.4.x**
- **Belgacom E-Trust FRNB Normalised Certificate**
 - Normalised Certificate with SSCD: **0.4.0.2042.1.2** and Key Generation by CSP : **0.3.2062.9.6.1.26.7.x**
- **Belgacom E-Trust Lawyer's Normalised Certificate**
 - Normalised Certificate without SSCD **0.4.0.2042.1.1** and Key Generation by Owner: **0.3.2062.9.6.1.15.6.x**
 - Normalised Certificate with SSCD: **0.4.0.2042.1.2** and Key Generation by CSP : **0.3.2062.9.6.1.15.7.x**
 - Normalised Certificate without SSCD: **0.4.0.2042.1.1** and Key Generation by CSP: **0.3.2062.9.6.1.15.8.x**
- **Belgacom E-Trust Qualified Certificate for Qualified Signature Only**
 - Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Key generation by owner: **0.3.2062.9.6.1.19.2.x**
 - Qualified Certificate with SSCD (OID ETSI 101 456): **0.4.0.1456.1.1** and Key generation by CSP: **0.3.2062.9.6.1.19.3.x**
 - Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Key generation by CSP: **0.3.2062.9.6.1.19.4.x**
 - Qualified Certificate for use within Certipost application only, without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Key generation by CSP: **0.3.2062.9.6.1.23.4.x**
- **Belgacom E-Trust Normalised Certificate**
 - Normalised Certificate without SSCD: **0.4.0.2042.1.1** and Key generation by owner: **0.3.2062.9.6.1.19.6.x**
 - Normalised Certificate with SSCD: **0.4.0.2042.1.2** and Key generation by CSP: **0.3.2062.9.6.1.19.7.x**
 - Normalised Certificate without SSCD: **0.4.0.2042.1.1** and Key generation by CSP: **0.3.2062.9.6.1.19.8.x**
- **Certipost E-Trust FRNB Qualified Certificate for Qualified Digital Signature Only**

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy	Approval status: Released	Page #: 18 of 21

- Qualified Certificate with SSCD (OID ETSI 101 456): **0.4.0.1456.1.1** and Key Generation by CSP: **0.3.2062.7.1.1.5.3.x**
- **Certipost E-Trust FRNB Normalised Certificate**
 - Normalised Certificate with SSCD: **0.4.0.2042.1.2** and Key Generation by CSP : **0.3.2062.7.1.1.5.7.x**
- **Certipost E-Trust Qualified Certificate for Qualified Signature Only**
 - Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Key generation by owner: **0.3.2062.7.1.1.3.2.x**
 - Qualified Certificate with SSCD (OID ETSI 101 456): **0.4.0.1456.1.1** and Key generation by CSP: **0.3.2062.7.1.1.3.3.x**
 - Qualified Certificate without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Key generation by CSP: **0.3.2062.7.1.1.3.4.x**
 - Qualified Certificate for use within MyCertipost application only, without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Key generation by owner: **'0.3.2062.7.1.1.6.2.x**
 - Qualified Certificate for use within MyCertipost application only, with SSCD (OID ETSI 101 456): **0.4.0.1456.1.1** and Key generation by CSP: **'0.3.2062.7.1.1.6.3.x**
 - Qualified Certificate for use within MyCertipost application only, without SSCD (OID ETSI 101 456): **0.4.0.1456.1.2** and Key generation by CSP: **'0.3.2062.7.1.1.6.4.x**
- **Certipost E-Trust Normalised Certificate**
 - Normalised Certificate without SSCD: **0.4.0.2042.1.1** and Key generation by owner: **0.3.2062.7.1.1.3.6.x**
 - Normalised Certificate with SSCD: **0.4.0.2042.1.2** and Key generation by CSP: **0.3.2062.7.1.1.3.7.x**
 - Normalised Certificate without SSCD: **0.4.0.2042.1.1** and Key generation by CSP: **0.3.2062.7.1.1.3.8.x**
- **EID End User Signature Certificate**
 - OID: **2.16.56.1.1.1.2.1**

3.10.2 Signature Commitment types indication

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy		Approval status: Released

A Signature Commitment Type is an action or will be undertaken by a signer in signing a document in the context of a signature policy. A Signature Commitment Type can be either implicit or explicit if the signature policy specifies more than a single Commitment.


REM signature policy specifies the use of explicit commitment types meaning that each time a signature is to be created in the context of this signature policy, a specific commitment type will be added to the message to be signed by the signer.

All signatures performed by the Certipost electronic Registered Mail Platform are timestamped by a Trusted Timestamping Authority as defined in the IETF RFC 3161.


All signatures performed by the Certipost electronic Registered Mail Platform are performed by a FIPS Level 4 accredited HSM (Hardware Security Module) device.

The following Signature Commitment Types are defined as follows:

Acting Party	Signature Operation	Signature Commitment	Signature Commitment OID
Sender	Signature for REM submission	By creating this signature, the Sender agrees to the creation and submitting / sending of a REM through the Certipost REM service platform (Platform), on his behalf, to the Recipients that he has indicated and according to the present signature policy and the specific conditions related to Certipost REM service. The REM is being composed of the Sender's and Recipient(s)' information, the subject, the text, and the potential attachments.	0.3.2062.9.6.10.1.1.1.2.1
Platform	Countersignature of submitted REM in the context of creation of REM Submission Receipt	By creating this signature the Certipost REM service Platform confirms: <ul style="list-style-type: none"> • That the REM has been sent by the Sender to the Recipient(s) at the time of deposit as indicated in the timestamp; • That the Platform has notified, at that time, the Recipient(s) that the REM is available for them in protected central repository that is accessible to them provided that they digitally sign a "Reception Acceptance Receipt"(not applicable for HREM); • The integrity of the REM content so that any later alteration of the REM will be detected; • According to the present signature 	0.3.2062.9.6.10.1.1.1.2.2

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy		Approval status: Released

		policy and the specific conditions related to Certipost REM service.	
REM Recipient	Signature in the context of Reception Acceptance	By creating this signature the Recipient indicates his will to approve the reception of the REM and guarantees that he is indeed the correct recipient and accept the full liability to this regard, according to the present signature policy and the specific conditions related to Certipost REM service. The REM is being composed of the Sender's and Recipient(s)' information, the subject, the text, and the potential attachments. (not applicable for HREM)	0.3.2062.9.6.10.1.1.1.2.3
Platform	Countersignature of recipient signed acceptance in the context of creation of REM Reception Acceptance Receipt	By creating this signature the Certipost REM service Platform confirms (not applicable for HREM) : <ul style="list-style-type: none"> • That the REM has been accepted for reception by the Recipient who is identified in the Recipient identification field at the time of creating this signature as indicated in the timestamp; • That this signature covers the REM as signed by the Sender confirming the integrity of the receipt content so that any later alteration of the receipt will be detected; • According to the present signature policy and the specific conditions related to Certipost REM service. 	0.3.2062.9.6.10.1.1.1.2.4
Recipient	Signature in the context of Reception Refusal	By creating this signature the Recipient indicates his will to refuse the reception of the REM, for which he is the addressee, from the Certipost REM service platform (Platform), according to the present signature policy and the specific conditions related to Certipost REM service.(not applicable for HREM)	0.3.2062.9.6.10.1.1.1.2.5
Platform	Countersignature of recipient signed refusal in the context of creation of REM Reception Refusal Receipt	By creating this signature the Certipost REM service Platform confirms (not applicable for HREM) : <ul style="list-style-type: none"> • That the REM has been refused for reception by the Recipient who is identified in the Recipient identification field at the time of creating this signature as indicated in the associated timestamp; • That this signature covers the REM as signed by the Sender confirming the integrity of the receipt content 	0.3.2062.9.6.10.1.1.1.2.6

	Certipost Registered Mail Services	Document OID: 0.3.2062.9.6.10.1.1.1.2.1	Version: 2.1
	Title: Certipost Registered Mail Signature Policy		Approval status: Released

		so that any later alteration of the receipt will be detected; <ul style="list-style-type: none"> According to the present signature policy and the specific conditions related to Certipost REM service. 	
Platform	Signature in the context of creation of REM Non-Delivery Receipt	By creating this signature the Certipost REM service Platform confirms (not applicable for HREM) : <ul style="list-style-type: none"> That the REM has not been delivered to the Recipient who is identified in the Recipient identification field; That this Non-Delivery Receipt has been associated to the time as indicated in the timestamp; That this signature covers the REM as signed by the sender confirming the integrity of the receipt content so that any later alteration of the receipt will be detected; According to the present signature policy and the specific conditions related to Certipost REM service. 	0.3.2062.9.6.10.1.1.1.2.7