Certificate Policy

Test Policy: For the PoC with “Type 2” certificates

Version	1.0
Document name	CP_CTP_e-Certificates_TEST_PoC_Type2_V1_0.docx

1. Document control

Review history

Reviewer	Date	Action	Version	Status
CEPRAC members	31/01/2012	Generation, review and approval	1.0	Approved

2. Index

3. Definitions and Acronyms

Definitions and acronyms have a dynamic nature as they tend to be expanded regularly. A generic document with the definitions and acronyms is available on-line on http://pki.certipost.com

This document is under strict control of the Certipost CErtification PRactices Council (CEPRAC).

For more more information please refer to the Certification Practice Statements (CPS) on http://pki.certipost.com.

(Reference to RFC 3647: 1.6)

4. Introduction

This document describes the applications for which certificates issued by the Certification Service Provider (CSP) under this Certificate Policy (CP), may be used, as well as the procedures to be followed and the responsibilities of the parties involved, in accordance with the Certification Service Provider's Certification Practice Statements (CPS).

This CP is based on RFC 3647. However in format an alternative approach was chosen in order to:

- Increase readability of the user: every piece of essential information that a user needs should be easily findable at one place in a compact form.
- Lower maintenance cost: every change should have a minimal impact on the entire document by making sure the information is not redundant
- Lower operational costs: the mapping between the CP and the actual policy & profile configuration in the underlying systems and procedures should be as straightforward as possible

Though the sequence and format therefore deviates from the proposed format in RFC 3467, a mapping between the RFC 3467 sections and the sections in this CP is included.

5. Overview – General section

The first column references RFC 3467, where applicable.

1.1	Overview	
1.5	Policy Administration	
1.5.1	Organization Administering the Document	Certipost n.v. / s.a.
1.5.2	Contact Person	Contact persons: Certipost n.v./s.a. Certification Practices Council c/o Guy Ramlot Ref.: CPS Administration Muntcentrum B-1000 Brussels Belgium http://www.certipost.com service.desk@certipost.com Fax: +32 (0)70/22.55.01
1.5.3	Person Determining CPS suitability for the Policy	This is determined by the Certipost CErtification PRactices Council (CEPRAC) board. See CPS.
1.5.4	CPS Approval Procedures	This is determined by the Certipost CErtification PRactices Council (CEPRAC) board. See CPS.
2	Publication and Repository Responsibilities	
2.1	Repositories	See CPS.
2.2	Publication of Certification Information	See CPS.
2.3	Time or Frequency of Publication	See CPS.
2.4	Access Controls on Repositories	See CPS.

6. Overview – Specific for this CP section

The basis for this CP is the following base CP. The first column references RFC 3467, where applicable.

The version "number" of this document replaces the last digit of the Certipost CP OID.

1.1	Overview	
1.2	Document Name and Identification	
	Certipost Name= Certificate Policy	**Certificate FOR CERTIPOST USE FOR TESTING ONLY**
7.1.6	Certificate policy object identifier	Not applicable
	Certipost CP OID (of base CP)	1.3.6.1.4.1.3860.1.2.999.1.0
	Policy Issuance date	31/01/2012
1.4	Certificate Usage	
1.4.1	Appropriate Certificate Uses	**Any testing use but this is restricted: a test certificate must never have the appearance of a real life certificate.**
1.4.2	Prohibited Certificate Uses	**All not specified as appropriate**
	Assurance level	None: no relying party should trust this certificate
	Retention period of registration data	No retention guarantee
6.2	Private Key Protection and Cryptographic Module Engineering Controls	Any method of key generation is allowed. The protections, measures and controls are described in the CPS.
6.2.8	Method of activating private key	The private key can only be activated by authorized testers or the service(s) identified in the test specification and policy.
6.2.9	Method of deactivating private key	No restrictions
	Liability	No liability
8.	Compliance audit and other assessments	**No compliance claims**

4.5 / 6.1.7	Key usage	Any
4.5.1	Subscriber private key and certificate usage	The subscriber must only use the private key and certificate for testing
4.5.2	Relying party public key and certificate usage	**There are no relying parties as they must NOT trust this public key and certificate.**
6.1.7	Extended Key Usage	Any
6.3.1	Public key archival	Public keys and certificates are not archived by the CSP.
6.3.2	Certificate operational periods and key pair usage periods	Certificate operational periods of active (un-revoked) certificates are maximum 2 months after creation and are further restricted by the test period.
6.4	Activation data	Any
1.3	PKI Participants	
1.3.1	Certification Authorities	Only Certipost acts as a Certificate Authority for this CP. For the issuing CA: please see the "issuer" in the Certificate Profile.
1.3.2	Registration Authorities	Only Certipost can act as the Registration Authority.
1.3.3	Subscribers	Certipost only
1.3.4	Relying parties	There are no relying parties as they must NOT trust this public key and certificate.
1.3.5	Others participants	
	Subject	Any test entity
	Certificate Service Provider	Certipost n.v. / s.a.
	Subject device provision service	If a subject device is used : Certipost n.v. / s.a.

2.3	Identification and Authentication	
	Certified entity	**Any test entity**
2.3.1-6	Naming	Any test entity
7.1.5	Name constraints	Names must always be such as to make clear that the certificate is for testing only by starting the CN with "TESTING ONLY!"
	Uniqueness of the subject	Not guaranteed.
2.3.2	Initial Identity Validation	
2.3.2.1	Method to prove possession of private key	Any
2.3.2.2	Authentication of organization identity	No evidence must be provided of the certified entity.
2.3.2.3	Authentication of individual identity	Not applicable
2.3.2.4	Non-verified subscriber information	All information is not certified and should be considered as non-verified.
2.3.2.5	Validation of authority	A Certipost established body authorizes the persons who may request this certificate
2.3.2.6	Criteria for interoperation	Not applicable
2.3.3 (.1-2)	Identification and authentication for re-key requests	This must be on the same level of trust as the initial identity validation. See CPS
2.3.4	Identification and authentication for revocation request	Any means are allowed

	Certificate Life-Cycle	
4.1	Certificate Application	
4.1.1	Who can submit a certificate application	An authorized person of Certipost or authorized by Certipost only
4.1.2	Enrollment process and responsibilities	The enrollment of subjects takes place via the RA which is responsible for ensuring that the information is permissible. See CPS.
4.2	Certificate application processing	Either explicitly or implicitly, the application is authenticated and the processing is largely automated. Applications based on accurate information sources must be verified by the applicant and then accepted or rejected.
4.3	Certificate issuance	Any means are allowed
6.1.1	Key pair generation	Any means are allowed
6.1.2	Private key delivery to subscriber	Any means are allowed
6.1.3	Public key delivery to certificate issuer	Any means are allowed
6.1.4	CA public key delivery to relying parties	Not applicable
4.4	Certificate acceptance	
4.4.1	Conduct constituting certificate acceptance	Not applicable: there is no value associated with the certificate
4.4.2	Publication of the certificate by the CA	Certificates must not be published in a public directory.
4.4.3	Notification of certificate issuance by the CA to other entities	Subscribers can be notified about the issuance of certificates by means of reporting.
4.6	Certificate renewal	Certificate renewal is allowed.
4.6.1	Circumstance for certificate renewal	Certificate renewal is only allowed as far as it is part of the test scenarios.
4.7	Certificate re-key	Certificate re-key is allowed.
4.7.1	Circumstance for certificate re-key	Re-key can take place whenever a new certificate is needed due to the invalidity of the previous certificate. The new validity interval must be in accordance with the limitations imposed by this CP.

4.8	Certificate modification	Certificate modification is allowed in this policy: but it comes down to a re-certification.
4.8.1	Circumstance for certificate modification	A precondition for modification is that the key pair can be reused. Certificate renewal may never take place after the certificate has been revoked because of key compromise or a significant risk of key compromise or when the certificate is suspended. The new validity interval must be in accordance with the limitations imposed by this CP. If these conditions are met, modification can take place by means of re-certification. The reasons for this can include any new test that needs to be performed.
4.6.2 / 4.7.2 / 4.8.2	Who may request renewal, re-key and modification (re-certification)	The authorized persons of Certipost or authorized by Certipost. The process is similar to (initial) certificate issuance.
4.6.3 / 4.7.3 / 4.8.3	Processing certificate renewal, re-key and modification (re-certification) requests	Same process as the initial certificate issuance.
4.6.4 / 4.7.4 / 4.8.4	Notification of new certificate issuance to subscriber	Subscribers can be notified about the issuance of certificates by means of reporting.
4.6.5 / 4.7.5 / 4.8.5	Conduct constituting acceptance of a renewed, re-keyed or modified (re-certified) certificate	Same process as the initial certificate issuance.
4.6.6 / 4.7.6 / 4.8.6	Publication of the renewed, re-keyed or modified (re-certified) certificate by the CA	Same process as with the initial certificate issuance.
4.6.7 / 4.7.7 / 4.8.7	Notification of certificate issuance by the CA to other entities	Other entities, when authorized, can be notified about the issuance of certificates by means of reporting.

4.9	Certificate revocation and suspension	
4.9.1	Circumstances for revocation	Revocation of a valid (unexpired) certificate must happen as soon as: • The test has been completed or the test conditions have changed. • There is a significant risk of private key compromise or the private key compromise has already been compromised. • The certificate has been delivered from wrong or falsified information. • The CA stops its activities without another CA taking over its activities. Even though revocation checking should encompass the complete certification path and thus the revocation of the issuing CA should be sufficient to invalidate all issued end-entity certificates, in practice it may be recommended to also revoke each end-entity certificate issued by the CA. Note that in this case the subscribers will be informed at least 12 months before revocation. • The issuing CA certificate's private key has been compromised.
4.9.2	Who can request revocation	Depending on the circumstances leading to the revocation request can be made by: • An authorized person of Certipost or authorized by Certipost • A RA • The CSP • A mandated person representing the CA • An authorized legal authority
4.9.3	Procedure for revocation request	Revocation requests are submitted after adequate authentication and authorization of the requestor.
4.9.4	Revocation request grace period	The revocation request must be made as soon as possible, at maximum after 12 hours if the requestor is not subject to Force Majeure.
4.9.5	Time within which CA must process the revocation request	The CA must process the revocation request in real-time or according to the SLA.
4.9.6	Revocation checking requirement for relying parties	Not applicable
7.2	CRL profile	The CRL profiles are described in the CPS
4.9.7	CRL issuance frequency (if applicable)	6 hours
4.9.8	Maximum latency for CRLs (if applicable)	24 hours

4.9.9	On-line revocation/status checking availability	Not available
4.9.10	On-line revocation checking requirements	Not applicable
4.9.11	Other forms of revocation advertisements available	Not applicable
4.9.12	Special requirements key compromise	Not applicable
4.9.13	Circumstances for suspension	Any circumstance that may lead to the need for revocation and any circumstance in which requester chooses to temporarily suspend the certificate in order to prevent the use of the certificate during a certain time, can be considered as a valid reason for suspension. E.g. the temporary misplacement of the CSP or the suspension of the use of the certificate.
4.9.14	Who can request suspension	Depending on the circumstances leading to the suspension request can be made by: • An authorized person of Certipost • A RA • The CSP • A mandated person representing the CA • An authorized legal authority
4.9.15	Procedure for suspension request	Suspension requests are submitted after adequate authentication and authorization of the requestor.
4.9.16	Limits on suspension period	After 60 days a suspension that is not un-suspended may lead to revocation by the CA.
	Circumstances for un-suspension	The reason for suspension no longer exists and the certificate has not yet been revoked.
	Who can request a un-suspension	The person authorized by Certipost can request an un-suspension.
	Procedure for un-suspension request	Suspension requests are submitted after adequate authentication and authorization of the requestor.
4.10	Certificate status services	These are described in the CPS
4.11	End of subscription	Not applicable
4.12	Key escrow and recovery	Key escrow and recovery are allowed in this policy

	"Private key holding device" & user life cycle management	
	Enrollment process and responsibilities	If the certificate makes use of a "private key holding device", then the enrollment of "private key holding device" holders takes place via the RA which is responsible for ensuring that the information is accurate. This can be an automated process fed from an authoritative source.
	Device issuance	If the certificate makes use of a "private key holding device", the device provisioning takes place in such a way and protected by such means as described in the CPS to ensure that a particular "private key holding device" is always under sole control of the holder. This means that it can only be used by the holder for activating the private key associated with a certificate that certifies the holder as the subject.
	Device suspension	If the certificate makes use of a "private key holding device", device suspension (either due to loss or malfunction) is handled in such a way and protected by such means as described in the CPS to ensure that a particular "private key holding device" can only be used to activate the private key associated with a certificate that certifies the holder as the subject by the holder.
	Device replacement	If the certificate makes use of a "private key holding device", device replacement can take place after device termination and takes place in such a way and protected by such means as described in the CPS to ensure that a particular device is in the possession of a particular holder and that this device can only be used to activate the private key associated with a certificate that certifies the holder as the subject by that holder.
	Device termination	If the certificate makes use of a "private key holding device", device termination can take place after permanent loss, compromise or fatal malfunction and takes place in such a way and protected by such means as described in the CPS to ensure that a particular device is always under sole control of the holder. This means that it can only be used by the holder for activating the private key associated with a certificate that certifies the holder as the subject.
	Technical parameters	
6.1.5	Key sizes	Any
	hashing algorithm	Any
	Certificate path to give along	Any "internal use" path or none
	Combining this CP with other CPs	
	general	No combination is allowed

7.1	Certificate profile	
7.1.1	Version number(s): version	Version 3 (value = "2")
	serialNumber	Value provided by the system
7.1.3	Algorithm object identifiers : signature - algorithm parameters	Any
	issuer	CN=Certipost Internal Use CA SHA-256 ,O=Certipost n.v./s.a.,C=BE or CN=Certipost Internal Use CA SHA-1 ,O=Certipost n.v./s.a.,C=BE, or CN=Certipost Internal Use CA Root Signed SHA-256, or O=Certipost n.v./s.a.,C=BE or CN=Certipost Internal Use CARoot Signed SHA-1,O=Certipost n.v./s.a.,C=BE
	validity: notBefore	A time shortly after the initiation of the Certificate installation
	validity: notAfter	Later than validity: notBefore but with a maximum of 2 months
	subject	
	commonName	**Any but restricted: no existing entity may be used except when it can be limited to the test**
	surName	Any but restricted: no existing entity may be used except when it can be limited to the test
	givenName	Any but restricted: no existing entity may be used except when it can be limited to the test
	serialNumber	Any but restricted: no existing entity may be used except when it can be limited to the test
	countryName	Any but restricted: no existing entity may be used except when it can be limited to the test
	stateOrProvinceName	Any but restricted: no existing entity may be used except when it can be limited to the test
	localityName	Any but restricted: no existing entity may be used except when it can be limited to the test
	organizationName	Any but restricted: no existing entity may be used except when it can be limited to the test
	organizationUnitName	Any but restricted: no existing entity may be used except when it can be limited to the test
	title	Any but restricted: no existing entity may be used except when it can be limited to the test
	email address	Any but restricted: no existing entity may be used except when it can be limited to the test
	domainComponent	Any but restricted: no existing entity may be used except when it can be limited to the test
	unstructuredName	Any but restricted: no existing entity may be used except when it can be limited to the test
	jurisdictionOfIncorporation	Any but restricted: no existing entity may be used except when it can be limited to the test
	jurisdictionOfIncorporationState	Any but restricted: no existing entity may be used except when it can be limited to the test
	jurisdictionOfIncorporationCountryName	Any but restricted: no existing entity may be used except when it can be limited to the test
	Initials	Any but restricted: no existing entity may be used except when it can be limited to the test

	pseudonym	Any but restricted: no existing entity may be used except when it can be limited to the test
	stateOrProvinceName	Any but restricted: no existing entity may be used except when it can be limited to the test
	homePostalAddress	Any but restricted: no existing entity may be used except when it can be limited to the test
	streetAddress	Any but restricted: no existing entity may be used except when it can be limited to the test
	postalCode	Any but restricted: no existing entity may be used except when it can be limited to the test
	dnQualifier	Any but restricted: no existing entity may be used except when it can be limited to the test
7.1.2	Certificate extensions	
	authorityKeyIdentifier: keyIdentifier	C8:25:51:56:B9:3D:55:D6:CF:21:0D:BE:8B:B8:30:46:07:3E:53:7A OR 56:CB:29:19:0A:5E:91:B1:5E:5E:CA:BC:ED:40:3C:CB:51:D8:CF:DA Or 1B:80:D6:C9:39:10:86:1A:BA:8F:D1:5A:45:06:E9:DA:1B:76:00:30 Or 41:04:B6:B0:E6:1D:78:48:A7:17:3E:C1:CF:26:CA:1E:01:AB:0D:6B
	subjectKeyIdentifier: keyIdentifier	variable: derived from the public key
	keyUsage	Any
7.1.6	Certificate policy object identifier: certificatePolicies: policyIdentifier	see Certipost CP OID
	certificatePolicies: Policy Qualifier Info	Policy Qualifier Id=CPS Qualifier: http://pki.certipost.com
	certificatePolicies: Policy Qualifier Info	Policy Qualifier Id=User Notice Qualifier: Notice Text=Certipost Certificate Policy for testing by Certipost. More detailed information can be found in the Certificate Policy 1.3.6.1.4.1.3860.1.2.999.1.0 on http://pki.certipost.com
	subjectAltName: rfc822Name	Any but restricted: no existing entity may be used except when it can be limited to the test
	subjectAltName: OtherName	Any but restricted: no existing entity may be used except when it can be limited to the test
	subjectAltName: dNSName	Any but restricted: no existing entity may be used except when it can be limited to the test
	subjectAltName: iPAddress	Any but restricted: no existing entity may be used except when it can be limited to the test
	Subject Directory Attributes : dateOfBirth	Any but restricted: no existing entity may be used except when it can be limited to the test
	Subject Directory Attributes : placeOfBirth	Any but restricted: no existing entity may be used except when it can be limited to the test
	Subject Directory Attributes : gender	Any but restricted: no existing entity may be used except when it can be limited to the test
	Subject Directory Attributes : countryOfResidence	Any but restricted: no existing entity may be used except when it can be limited to the test
	Subject Directory Attributes : countryOfCitizenship	Any but restricted: no existing entity may be used except when it can be limited to the test

	basicConstraints: CA	Subject Type=End Entity
	basicConstraints: pathLenConstraint	None
	extendedKeyUsage	Any
	cRLDistributionPoints: distributionPoint	http://crl.pki.certipost.com/IUCA_SHA256.crl or http://crl.pki.certipost.com/IUCA_SHA1.crl or http://crl.pki.certipost.com/IUCA_SHA256_RS.crl or http://crl.pki.certipost.com/IUCA_SHA1_RS.crl
	authorityInfoAccess : (1) accessMethod = [CA issuer]	= CA Issuer
	authorityInfoAccess : (1) accessLocation	http://certs.pki.certipost.com/IUCA_SHA256.crt or http://certs.pki.certipost.com/IUCA_SHA1.crt or http://certs.pki.certipost.com/IUCA_SHA256_RS.crt or http://certs.pki.certipost.com/IUCA_SHA1_RS.crt
	qcStatements: id-etsi-qcs-QcCompliance	Any
	qcStatements: id-etsi-qcs-QcSSCD	Any
	qcStatements: id-etsi-qcs-QcLimitValue	Any
	qcStatements: id-etsi-qcs-QcRetentionPeriod	Any
	Community logotype	Any but restricted: no existing entity may be used
	Subject organization logotype	Any but restricted: no existing entity may be used
	Other logos: Issuer organization logotype	Any but restricted: no existing entity may be used
	id-pe-wlanSSID	Any but restricted: no existing entity may be used
	id-pe-ipAddrBlocks	Any but restricted: no existing entity may be used
	id-pe-autonomousSysIds	Any but restricted: no existing entity may be used
	id-pe-otherCerts	Any but restricted: no existing entity may be used
	biometricInformation	Any but restricted: no existing entity may be used
7.1.7	Usage of Policy Constraints extension	Not used
7.1.8	Policy qualifiers syntax and semantics	Not Applicable
7.1.9	Processing semantics for the critical Certificate Policies extension	Not Applicable

	Other registration data	
	e-mail address	The e-mail addresses of Certipost employees, or other persons authorized by Certipost, mandated for particular testing purposes with this certificate are used for communications in relationship with certificate administration. If the mandated Certipost employee, or other persons authorized by Certipost, is also a "private key holding device" holder, then the e-mail address is also used for communications in relationship with the administration of "private key holding devices" (such as secure tokens, smart cards and SSCDs) when applicable .
	delivery addresses	Not applicable: delivery happens on the Certipost premises under the supervision of the security officer.
	language preferences	Not applicable: the working language used is English.
	unique identifier	Not applicable: if any identifiers are used they are temporary and for testing purposes only.
	user ID	A list of user IDs is used for communications in relationship with certificate administration and self-service access of the mandated person(s).
	password	A list of encrypted personal passwords is stored to enable authentication for the mandated person(s) to access self-service
	organization name and data for group managed certificates	Certipost (Default)
	list of mandated certificate requesters, viewers and administrators for group managed certificates	This list must be approved by the security officer or a PoC Engagement Manager. These mandated persons will be identified by their user ID, password, e-mail address (see above) and "private key holding device" identification number if applicable.
	Service Entity data for group managed certificates	Not applicable
	date of birth	Not applicable
	place of birth	Not applicable

7. Variant

This "Child" CP is a variant of the base CP in above section. The following sections are particular to this CP:

	Certipost CP OID (of base CP)	1.3.6.1.4.1.3860.1.2.999.3.0
6.2	Private Key Protection and Cryptographic Module Engineering Controls	The key pair is generated on the SUD.
4.12	Key escrow and recovery	Key escrow and recovery are not allowed in this policy
6.1.5	Key sizes	2048 bits
	hashing algorithm	SHA-1 (OID: 1.3.14.3.2.26)
	Certificate path to give along	The path leading up to the Baltimore CyberTrust Root.
7.1.3	Algorithm object identifiers : signature - algorithm parameters	SHA-1 (OID: 1.3.14.3.2.26)
	issuer	CN= Certipost Internal Use CA Root Signed SHA-1
	validity: notBefore	A time shortly after the initiation of the Certificate installation
	validity: notAfter	Later than validity: notBefore but with a maximum of 2 months
	subject	
	commonName	TEST - The (fictional) name of a test person
	surName	TEST - The (fictional) surname of a test person
	givenName	TEST - The (fictional) given name of a test person
	countryName	BE
	organizationName	TEST – Customer Organization Name

	title	TEST - The (fictional) title of a test person
	certificatePolicies: Policy Qualifier Info	Policy Qualifier Id=User Notice Qualifier: Notice Text=Certipost Certificate Policy for testing by Certipost. More detailed information can be found in the Certificate Policy 1.3.6.1.4.1.3860.1.2.999.3.0 on http://pki.certipost.com
	keyUsage	(0) digitalSignature and (1) contentCommitment (formerly nonRepudiation)
	extendedKeyUsage	None
	cRLDistributionPoints: distributionPoint	http://crl.pki.certipost.com/IUCA_SHA1_RS.crl
	authorityInfoAccess : accessLocation	http://certs.pki.certipost.com/IUCA_SHA1_RS.crt