a

Certificate Policy

Qualified certificates for legal persons represented by a physical person on SSCD - QCP+ Public

Version	1.1

1. Document control

Review history

Reviewer	Date	Action	Version	Status
Leslie Goodman	13/01/2012	Generation	1.0	For review (by CEPRAC)
Tim Bracke	13/06/2013	Generation	1.1	Reviewed by CEPRAC

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 Wim Mintiens Ref.: CPS Administration Muntcentrum B-1000 Brussels Belgium http://www.certipost.com trust.services@bpost.be
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	**Qualified certificates for legal persons represented by a physical person on SSCD - QCP+ Public**
7.1.6	Certificate policy object identifier	Itu-t(0) identified-organization(4) etsi(0) Qualified-Certificate-policies(1456) Policy-identifiers(1) qcp-public-with-sscd(1) = [0.4.0.1456.1.1]
	Certipost CP OID (of base CP)	1.3.6.1.4.1.3860.1.2.104.1.0
	Policy Issuance date	1/02/2012
1.4	Certificate Usage	
1.4.1	Appropriate Certificate Uses	**Creation of Qualified Electronic Signatures by means of electronic signing with a SSCD**
1.4.2	Prohibited Certificate Uses	**All not specified as appropriate**
	Assurance level	Qualified: Highest level of assurance provided by a Qualified Trusted Service Provider (supervised/accredited by the referenced Member State for compliance with the relevant provisions laid down in Directive 1999/93/EC). Evidence of the identity is checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence.
	Retention period of registration data	30 years after expiry of certificate
6.2	Private Key Protection and Cryptographic Module Engineering Controls	The key pair of the certificate is generated on a SSCD (no variants); Private Key Protection, Cryptographic Module Engineering Controls and other relevant controls and security measures are such that the certificate complies with the conditions to be a Qualified Certificate on SSCD. The protections, measures and controls are described in the CPS.
6.2.8	Method of activating private key	The private key is activated by means of authentication by the subject.
6.2.9	Method of deactivating private key	Deactivation takes place automatically, immediately after a one-time use.
	Liability	Liability cap for Qualified Certificates: 25.000 EUR
8.	Compliance audit and other assessments	**This policy claims conformance with ETSI TS 101 456 or equivalent. The means to achieve this and other necessary compliance audits are described in the CPS.**

4.5 / 6.1.7	Key usage	see certificate profile
4.5.1	Subscriber private key and certificate usage	The subscriber must discontinue using the private key following the expiration or revocation of the certificate. If the private key was compromised or there is a significant risk of compromise the private key must never use that private key anymore. Otherwise renewal or recertification can allow the continued use of the private key.
4.5.2	Relying party public key and certificate usage	**Relying parties may only use a public key and certificate that is valid and only for the validation of the intended use for which the certificate was utilized.**
6.1.7	Extended Key Usage	see certificate profile
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 3 years after creation. The key pair usage periods of these certificates are only limited by the subscription period and the cryptographic lifetime of the keys and algorithms.
6.4	Activation data	Activation data generation, installation and protection comply with the pertaining standards and best practices for Qualified Certificates on SSCD. The implementation is described in the CPS.
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. Certipost can outsource part of the registration activities but remains the sole RA.
1.3.3	Subscribers	Subscribers are either organizations with subjects (in the form of physical persons adhering to the organization) that are certified or individual subjects with no subscriber organization.
1.3.4	Relying parties	Any party that relies on the Qualified Electronic Signatures created with the certificate.
1.3.5	Others participants	
	Subject	A physical person representing an organization, subject to certification
	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	**The certified entity is a physical person representing an organization as a legal person and linked to the certified public key and whose name consists out of a surname (if the subject has one) and at least a first, and optionally a second and third given name in combination with the name of the organization and organization unique identifier the person is acting for.**
2.3.1-6	Naming	Names are 1) in the form of a X.500 distinguished name, 2) have to be meaningful, 3) are not anonymous or pseudonymous, 4) follow X.500 interpretation, 5) don't have to be unique,6) recognition of trademarks : See CPS
7.1.5	Name constraints	No further name constraints
	Uniqueness of the subject	The surname and given name combination together with the private unique identifier (based on the organization & role and/or the certified person's email domain name and/or a local personnel number (by default)) .
2.3.2	Initial Identity Validation	
2.3.2.1	Method to prove possession of private key	Certificate signing requests (CSR) are signed with the private key (PKCS#10). It must be assured that the origin of the CSR is the SSCD which is in the sole possession of the subject.
2.3.2.2	Authentication of organization identity	Legally signed evidence must be provided of the organization's identity and the physical person(s) mandated to act on behalf of the organization.
2.3.2.3	Authentication of individual identity	Evidence of the identity shall be checked against a physical person either directly or indirectly using means which provides equivalent assurance to physical presence. Evidence of the subject's identity document must have been legally signed by the subject and must still be valid, and provided to the CSP for archiving.
2.3.2.4	Non-verified subscriber information	All information that is not certified (see below: Certificate profile) should be considered as non-verified. No non-verified information should be incorporated in the certificate.
2.3.2.5	Validation of authority	The application must include the authorization from a legal representative (or a mandated person) of the Organization as a legal entity that the applicant can obtain and use the requested legal person's identity and act on behalf of the organization.
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	The initiator of a revocation request should be sufficiently authenticated and authorized to perform the revocation in order to reduce the risk of wrongful revocation. See CPS.

	Certificate Life-Cycle	
4.1	Certificate Application	
4.1.1	Who can submit a certificate application	Only the certificate holder (subject) can submit a certificate application from his / her SSCD
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 accurate. See CPS.
4.2	Certificate application processing	The application is required to be strongly authenticated. This can happen either explicitly or implicitly. Applications can be based on accurate information sources. But these must be verified by the applicant and then accepted or rejected.
4.3	Certificate issuance	Certificate issuance takes place in real-time and in an automated way from within the SSCD. (See CPS)
6.1.1	Key pair generation	Key generation will happen directly in the SSCD (hardware). The CSP is responsible to assure that this will happen securely, by assigning a particular SSCD to the physical person who will act on behalf of the organization, which can then be used to generate key pairs.
6.1.2	Private key delivery to subscriber	The private key is generated on the subject's SSCD and thus does not need to be delivered.
6.1.3	Public key delivery to certificate issuer	The public key is delivered in a secure connection and signed by the private key according to PKCS#10
6.1.4	CA public key delivery to relying parties	Not applicable
4.4	Certificate acceptance	
4.4.1	Conduct constituting certificate acceptance	Certificate is deemed accepted as a result of the issuance process. (See CPS)
4.4.2	Publication of the certificate by the CA	Certificates are not 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 not allowed in this policy: Certificate re-key is mandated
4.6.1	Circumstance for certificate renewal	Not applicable
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 reasons for this can include any change in the certified data (including the CP) and the CA hierarchy, any action or event (such as certificate expiration or revocation), any evolution which necessitates a new key length and/or algorithm change. Furthermore, the subscriber must still have a contractual agreement with Certipost that is valid in the new validity interval of the certificate or must agree to a new one that covers the extended period. The new validity interval must be in accordance with the limitations imposed by this CP.
4.8	Certificate modification	Certificate modification is not allowed in this policy: Certificate re-key is mandated
4.8.1	Circumstance for certificate modification	Not applicable
4.6.2 / 4.7.2 / 4.8.2	Who may request renewal, re-key and modification (re-certification)	The subject, subscriber, RA, and CSP can only request a re-key. The process is similar to (initial) certificate issuance and initiated from the SSCD.
4.6.3 / 4.7.3 / 4.8.3	Processing certificate renewal, re-key and modification (re-certification) requests	Re-key follows the 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	Certificates are not published in a public directory.
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 certified information is not valid any more or the content has changed. (including the end of existence of the subject) • There is a significant risk of private key compromise or the private key has already been compromised. o Note: previous certificates of the same key that have not expired and have not yet been revoked must also be revoked in this case. • The security of algorithms and key lengths employed in the certificate risks to become below the standard of acceptability in the near future • The certificate has been delivered from wrong or falsified information. • The subscriber has violated or otherwise ended the contractual provisions and agreement (e.g. the subscription to the certificate service has not been paid in respect with the purchase agreement.) • The certified entity does not exist anymore as an entity associated with the subscriber • The CA stops its activities without another CA taking over its activities. • The issuing CA certificate’s private key has been compromised. • The previous certificate of a renewed certificate in use has not yet expired
4.9.2	Who can request revocation	Depending on the circumstances leading to the revocation the revocation request can be made by: • The certificate holder (subject) • A mandated person of the subscriber’s organization • A RA or LRA having taken part in the registration of the concerned certificate • 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	A relying party must use a CRL check in order to check the status of certificates
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 the suspension request can be made by: • The certificate holder (subject) • A mandated person of the subscriber's organization • A RA or LRA having taken part in the registration of the concerned certificate • 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 subject or a person authorized by the subject or subscriber 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	If the end of subscription occurs before the certificate has been revoked, the certificate will be revoked as soon as the subscription is being ended. If the end of subscription is after this, and no new certificate has been produced, the certificate does not need to be revoked.
4.12	Key escrow and recovery	Key escrow and recovery is not allowed in this policy

	"Private key holding device" & user life cycle management	
	Enrollment process and responsibilities	The enrollment of SSCD 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	Device provisioning takes place in such a way and protected by such means as described in the CPS to ensure that a particular SSCD device and the private key in it is always under the sole control of the SSCD holder and subject of the certificate associated with the private key. This means that only the SSCD holder and subject of the certificate can activate and use this private key.
	Device suspension	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 SSCD device and the private key in it is always under the sole control of the SSCD holder and subject of the certificate associated with the private key. This means that only the SSCD holder and subject of the certificate can activate and use this private key.
	Device replacement	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 SSCD device and the private key in it is always under the sole control of the SSCD holder and subject of the certificate associated with the private key. This means that only the SSCD holder and subject of the certificate can activate and use this private key.
	Device termination	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 SSCD device and the private key in it is always under the sole control of the SSCD holder and subject of the certificate associated with the private key. This means that only the SSCD holder and subject of the certificate can activate and use this private key.
	Technical parameters	
6.1.5	Key sizes	minimum 2048 bits (default)
	hashing algorithm	minimum SHA-256 (default) (OID: 2.16.840.1.101.3.4.3.2)
	Certificate path to give along	Either the path leading up to the Baltimore CyberTrust Root for an environment that can support only the SHA-1 root (default) or alternatively the path leading up to the Verizon Global Root CA for an environment that can support full SHA-2 .
	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	SHA-2 256 bits (OID: 2.16.840.1.101.3.4.3.2)
	issuer	CN=Certipost Public CA for Qualified Signatures,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 3 years
	subject	
	commonName	**Family name (surName), first names (giveName)and initials of additional first names of the Subject as it is on his / her identity documents.** **Optionally the intended use of the certificate could be indicated in the common name between brackets: “ - (Sign)”**
	surName	optional, should match (e)ID card if this exists or passport otherwise
	givenName	should match (e)ID card if this exists or passport otherwise
	serialNumber	optional, not used (default), if present includes a unique qualifier (e.g. Personnel number in the identified organization)
	countryName	Name of the country (according to iso-3166-alpha2-code) of the identified organization's registered office. If no organization exists, then the country refers to the location of the professional activity's main practice identified in the subject's Title.
	stateOrProvinceName	optional, if present the full name of the state or province of the identified organization's registered office. If no organization exists, then this field refers to the location of the professional activity's main practice identified in the subject's Title.
	localityName	name of the locality (e.g. city) of the identified organization's registered office. If no organization exists, then the locality refers to the location of the professional activity's main practice identified in the subject's Title.
	organizationName	optional, Name of the subscriber’s organization or an organization subordinate to or associated with the subscriber’s organization – including a country specific unique organization identifier – (according to the bylaws of the organization) associated with the subject (person). It must be demonstrated that organization or the subordinate or associated organization is authorized to act as the subscriber for the subject (person). The unique identifier can be the VAT number if no other more appropriate identifier exists. The following constraint exists: if this field is not present then "title" must be present & visa versa.
	organizationUnitName	optional, name of the organizational unit the subject (person) belongs to
	title	optional, title or role of the person in the organization. The following constraint exists: if this field is not present then "organizationName" must be present & visa versa.
	email address	optional, "Not used" (default) or e-mail address of subject

	domainComponent	Not used
	unstructuredName	Not used
	jurisdictionOfIncorporation	Not used
	jurisdictionOfIncorporationState	Not used
	jurisdictionOfIncorporationCountryName	Not used
	Initials	Not used
	pseudonym	Not used
	stateOrProvinceName	Not used
	homePostalAddress	Not used
	streetAddress	Not used
	postalCode	Not used
	dnQualifier	Not used
7.1.2	Certificate extensions	
	authorityKeyIdentifier: keyIdentifier	0E:37:33:C7:28:6E:BF:CE:5F:E6:2A:E6:98:90:8B:AC:C1:E6:28:44
	subjectKeyIdentifier: keyIdentifier	variable: derived from the public key
	keyUsage	(1) contentCommitment (formerly nonRepudiation).
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 Qualified Certificate Policy for Physical Persons with Secure Signature Creation Device (SSCD). More detailed information can be found in the Certificate Policy 1.3.6.1.4.1.3860.1.2.104.1.0 on http://pki.certipost.com
	subjectAltName: rfc822Name	optional, "Not used" (default) or e-mail address of subject
	subjectAltName: OtherName	private unique identifier (default) or "Not used"
	subjectAltName: dNSName	Not used
	subjectAltName: iPAddress	Not used
	Subject Directory Attributes : dateOfBirth	optional, "not used" (default), date of birth of the subject as given in his / her birth certificate
	Subject Directory Attributes : placeOfBirth	optional, "not used" (default), place of birth of the subject as given in his / her birth certificate
	Subject Directory Attributes : gender	optional, "not used" (default), gender at birth of the subject as given in his / her birth certificate
	Subject Directory Attributes : countryOfResidence	optional, "not used" (default), country of residence of the subject as given in his / her identity document
	Subject Directory Attributes : countryOfCitizenship	optional, "not used" (default), country of citizenship at birth or the earliest after birth of the subject as given in his / her identity document

	basicConstraints: CA	Subject Type=End Entity
	basicConstraints: pathLenConstraint	None
	extendedKeyUsage	Not used
	cRLDistributionPoints: distributionPoint	http://crl.pki.certipost.com/PCA_Q.crl
	authorityInfoAccess : (1) accessMethod = [CA issuer]	= CA Issuer
	authorityInfoAccess : (1) accessLocation	http://certs.pki.certipost.com/PCA_Q.crt
	qcStatements: id-etsi-qcs-QcCompliance	Mandatory: to indicate that the certificate is issued as a Qualified Certificate according Annex I and II of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, as implemented in the law of the country specified in the issuer field of this certificate.
	qcStatements: id-etsi-qcs-QcSSCD	optional, OID id-qcs-pkixQCSyntax-v2, indicated that the certificate's private key is on SSCD
	qcStatements: id-etsi-qcs-QcLimitValue	optional, indicates the liability cap, The codes are defined in ISO 4217
	qcStatements: id-etsi-qcs-QcRetentionPeriod	optional, indicates the "Retention period of registration data"
	Community logotype	Not used
	Subject organization logotype	Not used
	Other logos: Issuer organization logotype	Not used
	id-pe-wlanSSID	Not used
	id-pe-ipAddrBlocks	Not used
	id-pe-autonomousSysIds	Not used
	id-pe-otherCerts	Not used
	biometricInformation	Not 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	By accepting the GTC the subscriber and/or subject grants Certipost the right to register and store the e-mail address of the subject for as long as the subject is active. The e-mail address is used for communications in relationship with the administration of certificates and "private key holding devices" (such as secure tokens, smart cards and SSCDs) when applicable
	delivery addresses	By accepting the GTC the subscriber and/or subject grants Certipost the right to register and store (the) delivery address(es) of the subject for as long as the subject is active. T(he) delivery address(es) is/are used for communications in relationship with the administration of certificates and "private key holding devices" (such as secure tokens, smart cards and SSCDs) when applicable
	language preferences	By accepting the GTC the subscriber and/or subject grants Certipost the right to register and store language preferences of the subject for as long as the subject is active. These language preferences are used for communications in relationship with the administration of certificates and "private key holding devices" (such as secure tokens, smart cards and SSCDs) when applicable
	unique identifier	By accepting the GTC the subscriber and/or subject grants Certipost the right to register and store a unique identifier for as long as the subject is active. This unique identifier is used in order help Certipost with identifying the subject in order that there is no or limited uncertainty about the identity of the subject.
	user ID	The user ID is used for communications in relationship with certificate and "private key holding device" administration and self-service access of the certificate holder(s).
	password	An encrypted form of a personal password is stored to enable authentication for the certificate holder(s) to access self-service
	organization name and data for group managed certificates	Not used
	list of mandated certificate requesters, viewers and administrators for group managed certificates	Not used
	Service Entity data for group managed certificates	Not used
	date of birth	Optional, if this data is needed to distinguish the subject.
	place of birth	Optional, if this data is needed to distinguish the subject.

7. Variant

This “Child” CP is a variant of the base CP in above section. The following sections are particular to this CP:
Not Applicable.