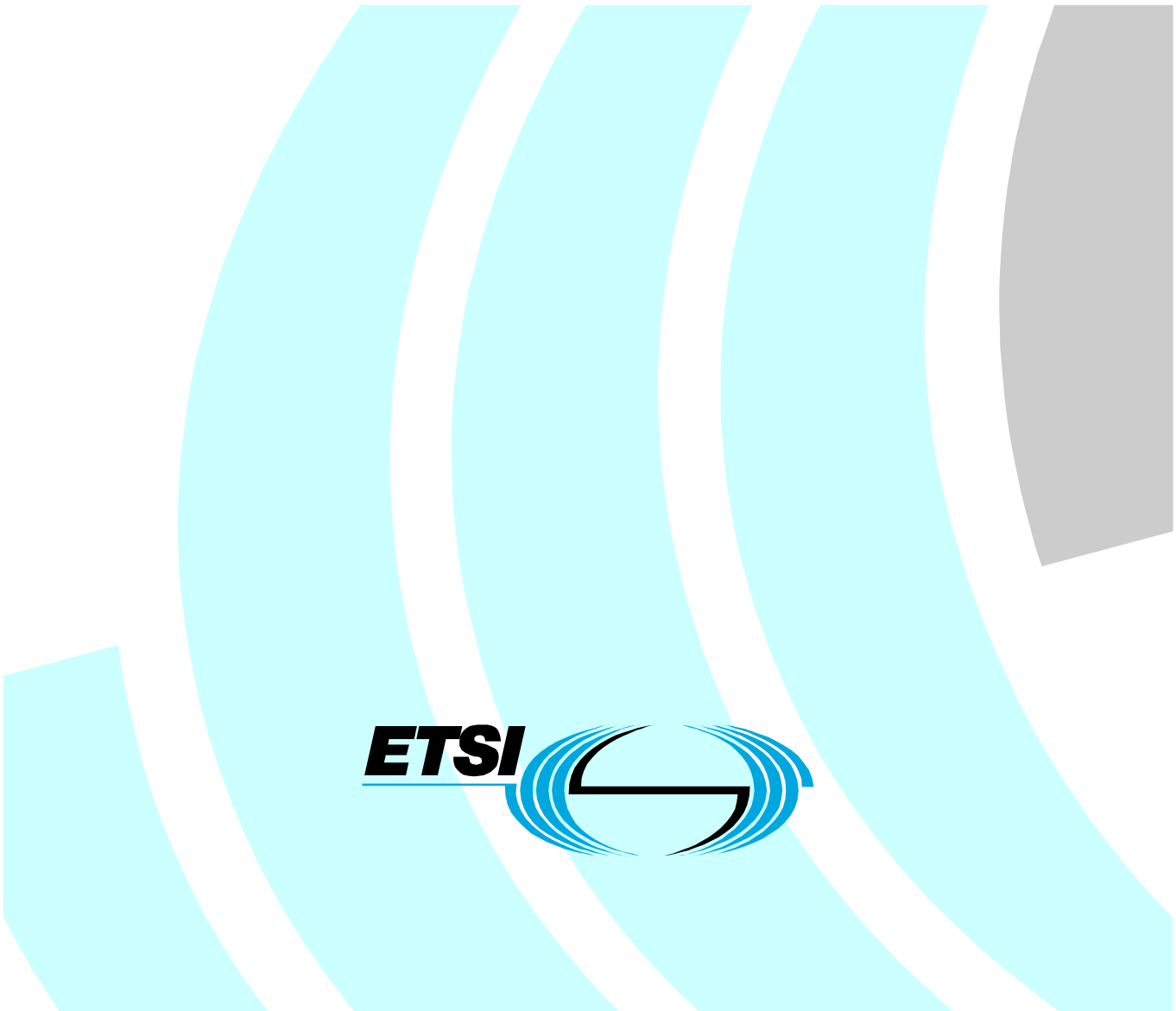
ETSI TR 102 458 V1.1.1 (2006-04)

Technical Report

Electronic Signatures and Infrastructures (ESI); Mapping Comparison Matrix between the US Federal Bridge CA Certificate Policy and the European Qualified Certificate Policy (TS 101 456)



Reference
DTR/ESI-000033

Keywords
authentication, e-commerce, electronic signature, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

Copyright Notification

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Introduction

In Europe ETSI has specified a framework certificate policy for Certification Authorities issuing "Qualified Certificates" [1], commonly referred to as the Qualified Certificate Policy (QCP), which fulfils the requirements of the European Directive on Electronic Signatures 1999/93/EC [1]. This provides a unifying framework for Certification Authorities operating in Europe.

In the United States of America the Federal Bridge Certification Authority (FBCA) has been established as the unifying element to link autonomous Certification Authorities (CAs) into a systematic overall Public Key Infrastructure (PKI). A Certificate Policy has been published for the FBCA specifying requirements for CAs interoperating with the Federal Bridge CA.

The FBCA, with the support of ETSI TC ESI, finalized in early year 2004 a map from the requirements specified in the QCP (TS 101 456 [2] V1.2.1) to the FBCA Certificate Policy (version 1).

The result of this effort was that the Federal Bridge Certification Authority assessed the requirements in TS 101 456 QCP public as "COMPARABLE" to those required to achieve the above mentioned Medium level of assurance. This will greatly facilitate Certification Authorities, conformant with the QCP, that intend to collaborate with CAs abiding by the above FBCA CP with medium level of assurance, to achieve recognition of conformity by FBCA. Since this work was completed new versions of the FBCA Certificate Policy and the ETSI QCP have been issued.

In order to facilitate achieving the opposite recognition, that a CA conformant with the FBCA Certificate Policy requirement is also conformant with the Qualified Certificate Policy, ETSI implemented the opposite mapping that is presented in the present document. The present document is based on the latest releases of the FBCA Certificate Policy and the ETSI Qualified Certificate Policy. The existing QCP to FBCA Certificate Policy mapping document is also being updated by the FBCA using the latest releases of the two policy documents.

1 Scope

The present document compares the United States" The Federal Bridge Certification Authority (FBCA) Certificate Policy [3], and the European Qualified Certificate Policy (QCP) as specified in TS 101 456 [2] in order to identify to what extent which stipulations FBCA CP match those of QCP. This comparison concentrates on requirements at the medium level of assurance as identified in the FBCA Certificate Policy [3] including the option for "medium hardware" (equivalent to SSCD) and "medium - Commercial Best Practices".

The present document gives the current results of the comparison following discussions with FPKI experts up to November 2005. Further consideration on some areas is still ongoing and this mapping is subject to further revision.

The present document is an opposite of the earlier mapping specified by the US Federal PKI mapping from the QCP into the requirements of the FBCA CP.

The purpose of the present document is to facilitate a CA abiding by the QCP to ascertain if QCP requirements, to which it complies, are met by another CA abiding by FBCA CP and therefore to assess if a cross certification can be enacted. It is to be kept in mind that this second CA has to be assessed as compliant by the Federal Bridge Certification Authority.

The present document is structured as follows:

1) BRIEF ASSESSMENT, which provides for each clause of the QCP a one-word assessment of the similarity of the applicable FBCA CP sections, using a set of well-defined evaluation terms, and identifies any points that should specially noted when applying this map to specific CA policies;

2) DETAILED ASSESSMENT, which details the BRIEF ASSESSMENT by breaking down all the relevant requirements in the QCP, grouped by clause, and by listing for each QCP clause the relevant FBCA CP sections and requirements that match to some degree to the corresponding QCP requirements clause; the same one-word assessment used in the BRIEF ASSESSMENT is complemented, where necessary, with explanatory comments. As a result of this comparison, requirements are identified in the FBCA CP that are of particular note and should be especially considered when applying this map to specific CA policies.

2 References

For the purposes of this Technical Report (TR) the following references apply:

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures.

[2] ETSI TS 101 456: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing qualified certificates".

[3] X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA CP) - Version 2, September 13, 2005.

NOTE: This version of the FBCA Certificate Policy replaces earlier version 1 dated September 10, 2002.

[4] ETSI Federal PKI CPWG Mapping Comparison Matrix Between the Federal Bridge Certification Authority (v1) and the European Qualified Certificate Policy (QCP) ETSI TS 101 456 V1.2.1 For Medium Assurance Level Cross Certification.

NOTE: This document is in the process of being revised to use the current versions of the FBCA Certificate Policy and the QCP.j.

[5] Template for use by the U.S. Federal PKI Policy Authority for Cross-Certifying with U.S. Federal Agencies and other U.S. Federal Entities, with U.S. State and Local Governments and U.S. Private Sector Entities, and with Governments of other Nations - Memorandum of Agreement.

[6] US Government Public Key Infrastructure - Cross Certification Criteria and Methodology Version 1.2 June 2005.

[7] ITU-T Recommendation X.509: "Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks".

[8] IETF RFC 3647: "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

certificate policy (CP): named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements (see ITU-T Recommendation X.509 [7])

Entity CA: CA that acts on behalf of an Entity, and is under the operational control of an Entity (FBCA CP)

qualified certificate: certificate which meets the requirements laid down in annex I (of the Directive [1]) and is provided by a certification-service-provider who fulfils the requirements laid down in annex II (of the Directive [1])

Qualified Certificate Policy: QCP public + SSCD: a certificate policy for qualified certificates issued to the public, requiring use of secure signature-creation devices, as defined in TS 101 456 [2]

subject: entity identified in a certificate as the holder of the private key associated with the public key given in the certificate

Subscriber: (1) - the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the certificate policy asserted in the certificate, and who does not itself issue certificates. (FBCA CP [3])

Subscriber: (2) - entity subscribing with a Certification Authority on behalf of one or more subjects (TS 101 456 [2] Policy requirements for certification authorities issuing qualified certificates)

NOTE 1: The subject may be a subscriber acting on its own behalf.

NOTE 2: QCP and FBCA CP assign different meanings to "subscriber". The FBCA CP "subscriber" is not clearly differentiated from the term "subject" whereas the QCP clearly distinguishes the two concepts.

The Directive: Directive 1999/93/EC [1] of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CA	Certification Authority
CP	Certificate Policy
FBCA	Federal Bridge Certification Authority
IETF	Internet Engineering Task Force
MoA	Memorandum of Agreement
OID	Object IDentifier
PKI	Public Key Infrastructure
QCP	Qualified Certificate Policy

4 PKI SUMMARIES

4.1 QCP

The QCP is a certificate policy framework for Qualified Certificates issued to the public in compliance with the requirements laid down in annexes I and II of the European Directive on Electronic Signatures 1999/93/EC [1].

Qualified certificates issued under this policy may be used to support electronic signatures which "satisfy the requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper based data", as specified in article 5.1 of the Electronic Signatures Directive.

It should be noted that the adoption of this policy is not mandatory and that alternative policies could be prepared so as to be conformant with the referenced Directive [1], although a considerably greater investment of time and resource would be required to do so.

It is also worth noting that several Directive compliant CAs have already adopted QCP as of the moment of publication of the present document.

4.2 FBCA CP

Quoted from [3]:

> "This Certificate Policy (CP) defines seven certificate policies for use by the Federal Bridge Certification Authority (FBCA) to facilitate interoperability between the FBCA and other Entity PKI domains. The policies represent five different assurance levels (Rudimentary, Basic, Medium, Medium Hardware, and High) for public key certificates. The level of assurance refers to the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.
>
> The FBCA enables interoperability among Entity PKI domains in a peer-to-peer fashion. The FBCA issues certificates only to those CAs designated by the Entity operating that PKI (called "Principal CAs"). The FBCA may also issue certificates to individuals who operate the FBCA. The FBCA certificates issued to Principal CAs act as a conduit of trust.
>
> Any use of or reference to this FBCA CP outside the purview of the Federal PKI Policy Authority is completely at the using party's risk. An Entity shall not assert the FBCA CP OIDs in any certificates the Entity CA issues, except in the policyMappings extension establishing an equivalency between an FBCA OID and an OID in the Entity CA's CP.
>
> This FBCA CP is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647 [8], Certificate Policy and Certification Practices Framework.
>
> The terms and provisions of this FBCA CP shall be interpreted under and governed by applicable Federal law."

5 Mapping the FBCA CP to the QCP

The mapping detailed in the following clause is built by associating to the requirements of FBCA CP to those of the QCP, as stipulated in its clauses 5, 6 and 7.

5.1 Rating

For an easier comparison the present document adopts the same seven comparative evaluation terms and definitions that were used in the opposite mapping produced by the FBCA [4]. These are:

a) **Exceeds:** The FBCA CP provides a higher level of assurance/security than the QCP requirement.

b) **Equivalent:** The FBCA CP provides exactly the same assurance/security as the QCP requirement.

c) **Comparable:** The FBCA CP provides a comparable level of assurance/security as the QCP requirement.

d) **Partial:** The FBCA CP contains policy that is comparable, but it does not address the entire QCP requirement.

e) **Not Comparable:** The FBCA CP contains dissimilar contents, which provide a lower level of assurance/security than the QCP requirement.

f) **Missing:** The FBCA CP does not contain contents that can be compared to the QCP requirement in any way.

g) **N/A (Not Applicable):** The FBCA implementation is such that mapping the FBCA CP to the QCP requirement in this area is not appropriate.

h) **Shaded:** The QCP does not address this topic.

5.2 Summary Assessment

5.2.1 Overview

The table in this clause summarizes the the degree of alignment between the QCP [2] on the one side and the FBCA CP [3], as detailed in clause 5.3. The assessments specified in the "Comparison Rating" column of the table match the content of the "Overall Match" rows of the corresponding clauses in clause 5.3.

The Summary Assessment table contains three main columns:

- QCP Clause: identifies the QCP clause numbers whose requirements are relevant to this analysis.
- FBCA CP Reference: identifies the [3] sections that were used in this analysis.
- Comparison Rating : provides the evaluation results found in clause 5.3, indicating the overall degree of conformity contained within each CP section.

QCP Clause	FBCA CP Reference Section	Comparison Rating
5. Introduction to QCP		
5.3 Applicability	1.4.1	COMPARABLE
5.4 Conformance	8, 8.5, MoA (IV.A.2)	EQUIVALENT
6. Obligations & Liability		
6.1 Certification authority obligations	MoA (IV.D)	COMPARABLE
6.2 Subscriber obligations	6.1.1.2, 7.1.3, 9.6.3	COMPARABLE
6.3 Information for Relying parties	4.9.6, 4.5.2	COMPARABLE
6.4 Liability	9.8	Point of note 1
7. Requirements on CA Practice		
7.1 Certification practice statement	1.5.3	COMPARABLE
7.2 PKI - Key management life-cycle		
7.2.1 Certification authority key generation	5.1.1, 5.1.2.1, 6.1.1.1, 6.1.5, 6.1.6, 6.3.2	Point of note 2
7.2.2 Certification authority key storage, backup and recovery	6.2.1, 6.2.4.1	Point of note 2
7.2.3 Certification authority public key distribution	6.1.4	EQUIVALENT
7.2.4 Key escrow	6.2.3.1, 6.2.3.3	EQUIVALENT
7.2.5 Certification authority key usage	6.1.7, 5.1.2.1	EQUIVALENT
7.2.6 End of CA key life cycle	6.2.9, 6.2.10	Point of note 3
7.2.7 Life cycle management of cryptographic hardware used to sign certificates	5.1.2.1, 6.2.9	COMPARABLE
7.2.8 CA provided subject key management services	6.1.1.2, 6.1.1.3, 6.1.5, 6.1.6	COMPARABLE
7.2.9 Secure-signature-creation device preparation	6.1.1.2, 6.1.2, 6.2.8, 6.2.9, 6.2.10	COMPARABLE
7.3 PKI - Certificate management lifecycle		
7.3.1 Subject registration	3.2.1, 3.2.3.1, 3.2.3.2, 3.2.3.3, 9.6.3	EQUIVALENT
7.3.2 Certificate renewal, rekey and update	4.6, 4.7, 4.8, 3.3.1	COMPARABLE
7.3.3 Certificate generation	7.1, 4.3, 3.2.1, 6.1.2, 3.1.5, 9.4, 3.2.3.1, 6.7	COMPARABLE
7.3.4 Dissemination of Terms and Conditions	9.6.3	COMPARABLE Point of note 4
7.3.5 Certificate dissemination	2.2.1, 2.2.2, 2.3, 2.4	COMPARABLE Point of note 4
7.3.6 Certificate revocation and suspension	2.2.1, 2.4, 3.4, 4.9, 4.9.1, 4.9.2, 4.9.3, 4.9.5, 4.9.7, 4.9.9, 4.9.13, 5.7.4	COMPARABLE Point of note 4, 8 and 9
7.4 CA Management and operation		
7.4.1 Security management	1.3.1.6, 1.3.2, 1.3.5, 1.4.1, 1.5.1, 6.6.2, 8, 8.3	COMPARABLE Point of note 5
7.4.2 Asset classification and management	General - policy requirements targeted at specific information needs	COMPARABLE Point of note 5
7.4.3 Personnel security	5.2.1, 5.2.4, 5.3.1, 5.3.3, 5.3.4, 5.3.7, 5.3.8	COMPARABLE
7.4.4 Physical and environmental security	5.1	COMPARABLE
7.4.5 Operations management	6.6.1, 5.4.2, 5.4.8, 5.1.2.1, 5.2.1, 5.1.6, 5.5.3, 6.2.4, 4.8.4, 5.4.2, 5.4.8, 5.7.1, MoA, 5.4.6	COMPARABLE Point of note 4 and 10
7.4.6 System Access Management	6.7, 6.5.1, 5.1.2.1, 6.6.2, 2.4	COMPARABLE
7.4.7 Trustworthy Systems Deployment and Maintenance (Table 27)	6.6.1, 6.6.2	EQUIVALENT
7.4.8 Business continuity management and incident handling (Table 28)	5.7.4, 5.1.8, 5.7.3	COMPARABLE
7.4.9 CA termination	5.8	Point of note 6
7.4.10 Compliance with Legal Requirements	9.4	COMPARABLE Point of note 5 and 8
7.4.11 Recording of Information Concerning Qualified Certificates	5.5, 4.6.2	COMPARABLE
7.5 Organizational	1.1.5, cross cert criteria [6], 1.3.1.1, 1.3.1.2, 9.6.1, 9.1.3, 5.2.1	COMPARABLE

5.2.2 Points of Note

The following specific point should be considered when cross certifying with a Certification Authority through the Bridge CA:

1) Specific legal advise should be sought regarding liability under article 6 of the EU Directive 1999/93/EC [1] and US commercial and governmental liability.

2) Currently, in the FBCA for medium level assurance FIPS 140-1 level 2 is required, and for high level assurance FIPS level 3 is required. Whereas, FIPS 140 level 3 is required in QCP. However, the FBCA policy committee are putting in place a strategy for moving Medium Assurance to Level 3 CA Crypto-modules. Already, most Entity CAs at medium assurance use FIPA level 3.

3) Currently, the FBCA does not address requirements for key destruction at the end of the CA key life cycle. The Federal PKI will investigate adding requirements in this area for the FBCA.

4) The FBCA does not directly address issues relating to levels of service to the subscribers and relying party where this does not affect the security of the certificate (e.g. no requirement to make subscriber aware of change of revocation status). The US are working the E-Authentication programme office in this area and may have additional references that could be added towards the end of this area.

5) Whilst FBCA CP does not require security management and asset classification as in the QCP, the development of the FBCA CP and the audit of the CAs against this CP are considered sufficient to ensure a comparable level of security.

6) The FBCA current does not include requirements for maintaining revocation information on CA termination. It is assumed that Federal PKI users will maintain the information on the status of a certificates used for signing. The Federal PKI will investigate further requirements regarding termination of CA.

7) EU Data Protection Legislation is not applicable to US. However, it is not considered necessary to exchange personal information other than that held in certificates for interoperability.

8) The Federal PKI will investigate notification of the subscriber in the case of revocation.

9) Handling of suspension for Entity CAs is unspecified.

10) FBCA require review of logs at least two months but it is unclear what specific measures are available to enable "timely response to incidents".

5.3 Detailed Assessment

This clause of the report presents the detailed results of the comparison of the QCP to the FBCA CP at the Medium Assurance level. The mapping comparison is characterized using the same evaluation terms listed in the preceding clause.

The detailed results that follow provide the QCP clauses and requirements to be mapped in tabular form, the FBCA CP section(s) and appropriate applicable text, the evaluation result for each requirement element addressed by the FBCA CP, as well as the evaluation comments. By default, the evaluation results listed in the "Overall Match" field indicates the *lowest* result when multiple sections from the FBCA CP are mapped to a particular QCP requirement.

NOTE: Informative notes have been removed from text in following mapping tables.

Table No.	CP reference	Mapping Clause
1	**Applicability**	
	QCP clause 5.3.1	The certificate policy QCP public + SSCD is for certificates: a) which meet the requirements laid down in annex I of the Directive 1999/93/EC [1]; b) are issued by a CA who fulfils the requirements laid down in annex II of the Directive; c) which are for use only with secure-signature-creation devices which meet the requirements laid down in annex III of the Directive; d) are issued to the public. Qualified certificates issued under this policy may be used to support electronic signatures which "satisfy the requirements of a signature in relation to data in electronic form in the same manner as a hand-written signature satisfies those requirements in relation to paper based data", as specified in article 5.1 of the Directive [1].
	QCP clause 5.3.2	The certificate policy QCP Public is for certificates: a) which meet the requirements laid down in annex I of the Directive; b) are issued by a CA who fulfils the requirements laid down in annex II of the Directive; c) are issued to the public. Qualified certificates issued under this policy may be used to support electronic signatures which "are not denied legal effectiveness and admissibility as evidence in legal proceedings", as specified in article 5.2 of the Directive.
	FBCA CP section 1.4.1	….. The FBCA is intended to support applications involving unclassified information, which can include sensitive unclassified data protected pursuant to Federal statues and regulations. …… Medium - This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. Medium Hardware - This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.

Table No.	CP reference	Mapping Clause
Overall Match: COMPARABLE		The scope of the FBCA CP is broader as it includes the range of services provided by a PKI whereas the QCP is specific to electronic signatures as per the Directive [1]. NOTE: The Electronic Signature Directive 1999/93/EC [1] Article 7 covers rules for legal equivalence.
		Conformance
2	QCP clause 5.4	5.4.1 General The CA shall only use the identifier for either of the qualified certificate policies as given in clause 5.2: a) if the CA claims conformance to the identified qualified certificate policy and makes available to subscribers and relying parties on request the evidence to support the claim of conformance; or b) if the CA has a current assessment of conformance to the identified qualified certificate policy by a competent independent party. The results of the assessment shall be made available to subscribers and relying parties on request. c) If the CA is later shown to be non-conformant in a way that significantly affects its ability to meet the requirements for qualified certificates identified in the Directive it shall cease issuing certificates using the identifiers in clause 5.2 until it has demonstrated or been assessed as conformant, otherwise the CA shall take steps to remedy the non-conformance within a reasonable period. d) The CA compliance shall be checked on a regular basis and whenever major change is made to the CA operations. 5.4.2 QCP public + SSCD A conformant CA must demonstrate that: a) it meets its obligations as defined in clause 6.1; b) it has implemented controls which meet all the requirements specified in clause 7. 5.4.3 QCP public A conformant CA must demonstrate that: a) it meets its obligations as defined in clause 6.1; b) it has implemented controls which meet the requirements specified in clause 7, excluding those specified in clause 7.2.9 and excluding the subscriber obligation given in clause 6.2 e) and f).
	FBCA CP clause 8	The FPKI Operational Authority shall have a compliance audit mechanism in place to ensure that the requirements of this CP and the FBCA CPS are being implemented and enforced. Entity CAs shall have a compliance audit mechanism in place to ensure that the requirements of their CP/CPS are being implemented and enforced.
	FBCA CP section 8.5	When the Entity compliance auditor finds a discrepancy between how the Entity CA is designed or is being operated or maintained, and the requirements of the Entity CP, any applicable MOAs, or the applicable CPS, the following actions shall be performed: • The compliance auditor shall document the discrepancy; • The compliance auditor shall notify the responsible party promptly; • The Entity PKI shall determine what further notifications or actions are necessary to meet the requirements of the Entity CP, CPS, and any relevant MOA provisions. The Entity PKI shall proceed to make such notifications and take such actions without delay. When the Federal PKI Policy Authority receives a report of audit deficiency from an Entity PKI, the Federal PKI Policy Authority may direct the FPKI Operational Authority to take additional actions to protect the level of trust in the infrastructure.
	FBCA MoA	IV. Rights and Obligations of the Parties A. Rights of the Federal PKI Policy Authority. 2. If at any time the Federal PKI Policy Authority determines that the Entity is not operating at the Level of Assurance specified in this MOA, the Policy Authority shall notify the Entity and may unilaterally reduce the Level of Assurance expressed in the certificate issued to the Entity or may revoke the certificate. The Policy Authority shall provide the Entity an opportunity to cure the assurance issues and regain its original Level of Assurance.

Table No.	CP reference	Mapping Clause
Overall Match: EQUIVALENT		NOTE: Any "voluntary accreditation" scheme which assesses the requirements defined in the QCP is outside the scope of ETSI, whereas acceptance or otherwise of an external CA is directly under the control of the FPKI. It is not explicitly required that a FBCA Entity CA ceases operations in case of significant discrepancy but it is required that necessary actions are taken.
3		**CA Obligations**
	QCP clause 6.1	The CA shall ensure that all requirements on CA, as detailed in clause 7, are implemented as applicable to the selected qualified certificate policy (see clauses 5.4.2, 5.4.3, 8.4). The CA has the responsibility for conformance with the procedures prescribed in this policy, even when the CA functionality is undertaken by sub-contractors. The CA shall provide all its certification services consistent with its certification practice statement.
	FBCA MoA	IV. Rights and Obligations of the Parties …. D. By entering into this agreement, the Entity [CA] agrees that it will do the following: 1. Comply with the applicable requirements of the FBCA CP, its own CP and CPS and such other requirements (e.g., laws, regulations, data center requirements) as govern the operation of the Entity PKI. [Additional obligations listed beyond those required by QCP]
Overall Match: COMPARABLE		Requirements of sub-contractors not explicitly addressed but overall obligation still holds.
4		**Subscriber Obligations**
	QCP clause 6.2	The CA shall oblige through agreement (see 7.3.1 i) the subscriber to address all the following obligations. If the subject and subscriber are separate entities, the subscriber shall make the subject aware of those obligations applicable to the subject (as listed below): a) submit accurate and complete information to the CA in accordance with the requirements of this policy, particularly with regards to registration; b) only use the key pair for electronic signatures and in accordance with any other limitations notified to the subscriber (see clause 7.3.4); c) exercise reasonable care to avoid unauthorized use of the subject's private key; d) if the subscriber or subject generates the subject's keys: i) generate subject's keys using an algorithm recognized as being fit for the purposes of qualified electronic signatures; ii) use a key length and algorithm which is recognized as being fit for the purposes of qualified electronic signatures during the validity time of the certificate; iii) the subject's private key can be maintained under the subject's sole control. e) if the certificate policy requires use of an SSCD (i.e. QCP public + SSCD), only use the certificate with electronic signatures created using such a device; f) if the certificate is issued by the CA under certificate policy QCP public + SSCD and the subject's keys are generated under control of the subscriber or subject, generate the subject's keys within the SSCD to be used for signing; g) notify the CA without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the certificate: i) the subject's private key has been lost (e.g. by forgetting the PIN number needed to use the key), stolen, potentially compromised; or ii) control over the subjects private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons; and/or iii) inaccuracy or changes to the certificate content, as notified to the subscriber or to the subject. h) following compromise, the use of the subject's private key is immediately and permanently discontinued. i) in the case of being informed that the CA which issued the subject's certificate has been compromised, ensure that the certificate is not used by the subject.

Table No.	CP reference	Mapping Clause
	FBCA CP section 6.1.1.2	Subscriber key pair generation may be performed by the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2 must also be met. Key generation shall be performed using a FIPS approved method or equivalent international standard. At the High and Medium Hardware assurance levels, subscriber key generation must be performed using a hardware cryptographic module. For all other assurance levels, either software or hardware cryptographic modules may be used for key generation
	FBCA CP section 6.2.10	Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a "zeroize" command. Physical destruction of hardware should not be required.
	FBCA CP section 6.1.5	clause 6.1.5 Key sizes All FIPS-approved signature algorithms shall be considered acceptable; additional restrictions on key sizes are detailed below. …. End-entity certificates that expire before 12/31/08 shall contain public keys that are at least 1024 bit for RSA, DSA, or Diffie-Hellman, or 160 bits for elliptic curve algorithms. End-entity certificates that expire on or after 12/31/08 shall contain public keys that are at least 2048 bit for RSA or Diffie-Hellman, or 224 bits for elliptic curve algorithms. [Note: See also memo given in Annex A regarding algorithm compromise.]
	FBCA CP section 4.5.1	"4.5.1 Subscriber Private Key and Certificate Usage For High, Medium Hardware, Medium, and Basic Assurance, subscribers shall protect their private keys from access by other parties."
	FBCA CP section 9.6.3	For Medium, Medium Hardware, and High Assurance levels, a Subscriber shall be required to sign a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. For Basic Assurance level, the Subscriber shall be required to acknowledge his or her obligations respecting protection of the private key and use of the certificate before being issued the certificate. Subscribers of Entity CAs at Basic, Medium, and High Assurance Levels shall agree to the following: • Accurately represent themselves in all communications with the PKI authorities. • Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures. • Promptly notify the appropriate CA upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS. • Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.
Overall Match: COMPARABLE		The following requirements are not directly addressed in the FBCA CP: d) iii) the subject's private key can be maintained under the subject's sole control.: For the policy QCP + SSCD this requirement is addressed by FBCA CP section 4.5.1 (medium hardware). However, there is no equivalent for the basic QCP. h) following compromise, the use of the subject's private key is immediately and permanently discontinued. i) in the case of being informed that the CA which issued the subject's certificate has been compromised, ensure that the certificate is not used by the subject. However, the general intent is considered to be comparable.
5		**Relying Party Obligations**
	QCP clause 6.3	The terms and conditions made available to relying parties (see clause 7.3.4) shall include a notice that if it is to reasonably rely upon a certificate, it shall: a) verify the validity, suspension or revocation of the certificate using current revocation status information as indicated to the relying party (see clause 7.3.4); and b) take account of any limitations on the usage of the certificate indicated to the relying party either in the certificate or the terms and conditions supplied as required in clause 7.3.4; and c) take any other precautions prescribed in agreements or elsewhere.

Table No.	CP reference	Mapping Clause
	FBCA CP section 4.9.6	**Revocation Checking Requirements for Relying Parties** Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.
	FBCA CP section 4.5.2	FBCA-issued certificates specify restrictions on use through critical certificate extensions, including the basic constraints and key usage extensions. The FBCA issues CRLs specifying the current status of all unexpired FBCA certificates. It is recommended that relying parties process and comply with this information whenever using FBCA issued certificates in a transaction.
Overall Match: COMPARABLE		
6		**Liability**
	QCP clause 6.4	CAs issuing qualified certificates to the public are liable as specified in article 6 of the Directive (see annex A for further guidance on liability).
	FBCA section 9.8	The U.S. Government shall not be liable to any party, except as determined pursuant to the Federal Tort Claims Act (FTCA), 28 U.S.C. 2671-2680, or as determined through a valid express written contract between the Government and another party.
Overall Match: POINT OF NOTE		Specific legal advise should be sought on the issue of liability
7		**Certification Practice Statement**
	QCP clause 7.1	The CA shall ensure that it demonstrates the reliability necessary for providing certification services (see the Directive , annex II (a)). In particular: a) The CA shall have a statement of the practices and procedures used to address all the requirements identified in the qualified certificate policy. b) The CA's certification practice statement shall identify the obligations of all external organizations supporting the CA services including the applicable policies and practices. c) The CA shall make available to subscribers and relying parties its certification practice statement, and other relevant documentation, as necessary to assess conformance to the qualified certificate policy. d) The CA shall disclose to all subscribers and potential relying parties the terms and conditions regarding use of the certificate as specified in clause 7.3.4. e) The CA shall have a high level management body with final authority and responsibility for approving the certification practice statement. f) The senior management of the CA is responsible for ensuring that the certification practices established to meet the applicable requirements specified in the current document are properly implemented. g) The CA shall define a review process for certification practices including responsibilities for maintaining the certification practice statement. h) The CA shall give due notice of changes it intends to make in its Certification Practice Statement (CPS) and shall, following approval as in (e) above, make the revised Certification Practice Statement immediately available as required under (c) above. i) The CA shall document the signature algorithms and parameters employed.
	FBCA section 5.4.1	Types of Events Recorded … Detailed audit requirements are listed … below according to the level of assurance. Medium (All policies) Violations of Certification Practice Statement
	FBCA CP section 1.5.3	The Certification Practices Statement must conform to the corresponding Certificate Policy. The Federal PKI Policy Authority is responsible for asserting whether the FBCA CPS conforms to the FBCA CP. Entities must designate the person or organization that asserts that their CPS(s) conforms to their CP(s). In each case, the determination of suitability shall be based on an independent compliance auditor's results and recommendations.

Table No.	CP reference	Mapping Clause
Overall Match: COMPARABLE		1. FPKI is less explicit in requirements of CPS. 2. even if no procedure is specifically requested for the Entity CA to approve modifications to its CPS, periodic audits by the FBCA ensure that the practices in force match the published CPS, so if the FBCA finds the CPS has changed it may complain. It is up to the CA as to whether the CPS is made public. Given the FBCA requirements for security audit against the CPS it is considered sufficient to meet the QCP objective "The CA shall ensure that it demonstrates the reliability necessary for providing certification services (see the Directive , annex II (a))"
8		**Certification authority key generation**
	QCP clause 7.2.1 a)	The CA shall ensure that CA keys are generated in controlled circumstances (see the Directive, annex II (g) and annex II (f)). In particular: a) Certification authority key generation shall be undertaken in a physically secure environment (see clause 7.4.4) by personnel in trusted roles (see clause 7.4.3) under, at least, dual control. The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.
	FBCA CP section 5.1.1	The location and construction of the facility housing the FBCA and Entity CA equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the FBCA and Entity CA equipment and records.
	FBCAv2 clause 5.1.2.1	The FBCA and Entity CA equipment shall always be protected from unauthorized access. The security mechanisms shall be commensurate with the level of threat in the equipment environment. Since the FBCA must plan to issue certificates at all levels of assurance, it shall be operated and controlled on the presumption that it will be issuing at least one High Assurance certificate. The physical security requirements pertaining to CAs that issue Basic Assurance certificates are: • Ensure no unauthorized access to the hardware is permitted • Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers In addition to those requirements, the following requirements shall apply to CAs that issue Medium, Medium Hardware, or High assurance certificates: • Ensure manual or electronic monitoring for unauthorized intrusion at all times • Ensure an access log is maintained and inspected periodically • Require two person physical access control to both the cryptographic module and computer system
	Match: Equivalent	
	QCP clause 7.2.1 b)	b) CA key generation shall be carried out within a device which either: - meets the requirements identified in FIPS PUB 140-1, or FIPS 140-2 [6], level 3 or higher; or - meets the requirements identified in one of the following CEN Workshop Agreement 14167-2 [10], CWA 16167-3 [11] or CWA 14167-4 [12]; or - is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [8], or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.

Table No.	CP reference	Mapping Clause
	FBCA CP section 6.1.1.1	Cryptographic keying material used to sign certificates, CRLs or status information by the FBCA shall be generated in FIPS 140 validated cryptographic modules. Cryptographic keying material used to sign certificates, CRLs or status information by Entity CAs shall be generated in FIPS 140 validated cryptographic modules or modules validated under equivalent international standards. For the FBCA, the modules shall meet or exceed Security Level 3. For Entity CAs, the modules shall meet or exceed Security Level 1 (for Rudimentary), Security Level 2 (for Basic, Medium, or Medium Hardware), or Security Level 3 (for High). Multiparty control is required for CA key pair generation for the FBCA and for Entity CAs operating at the Medium, Medium Hardware, or High levels of assurance, as specified in Section 5.2.2.
	Match: **Point of note**	For Medium level only FIPS 140 level 2 is required. However, the FBCA policy committee are putting in place a strategy for moving Medium Assurance to Level 3 CA Crypto-modules. Already most Entity CAs at medium assurance use FIPA level 3.
	QCP clause 7.2.1 c)	c) Certification authority key generation shall be performed using an algorithm recognized as being fit for the purposes of qualified certificates.
	FBCA CP section 6.1.5	All FIPS-approved signature algorithms shall be considered acceptable; …
	FBCA CP section 6.1.6	Public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186. Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186; additional tests may be specified by the Federal PKI Policy Authority.
	Match: **Equivalent**	In the case of compromise or weakness found in the cryptographic algorithm employed the Federal PKI will update it's policy (see Annex A)
	QCP clause 7.2.1 d)	d) The selected key length and algorithm for CA signing key shall be one which is recognized as being fit for the purposes of qualified certificates as issued by the CA.
	FBCA CP section 6.1.5	All FIPS-approved signature algorithms shall be considered acceptable; acceptable; additional restrictions on key sizes are detailed below. For CAs that distribute self-signed certificates to relying parties, the CA's subject public keys in such certificates shall be at least 2048 bits for RSA, or at least 224 bits for ECDSA. CAs that generate certificates and CRLs under this policy shall use signature keys of at least 1024 bits for RSA or DSA, and at least 160 bits for ECDSA. Certificates that expire after 12/31/08 shall be generated with at least 2048 bit RSA key, or at least 224 bits for ECDSA. CAs that generate certificates and CRLs under this policy shall use SHA-1, SHA-224, SHA-256, SHA-384, or SHA-512 hash algorithm when generating digital signatures. Signatures on certificates and CRLs that are issued after 12/31/08 shall be generated using, at a minimum, SHA-256.
	Match: **Equivalent**	Also, in the case of compromise or weakness found in the cryptographic algorithm employed the Federal PKI will update it's policy (see Annex A)
	QCP clause 7.2.1 e)	e) A suitable time before expiration of its CA signing key (for example as indicated by expiration of CA certificate), the CA shall generate a new certificate-signing key pair and shall apply all necessary actions to avoid disruption to the operations of any entity that may rely on the CA key. The new CA key shall also be generated and distributed in accordance with this policy.
	FBCA CP section 6.3.2	The usage period for an FBCA key pair is a maximum of six years. The FBCA private key may be used to generate certificates for the first half of the usage period (3 years), and the public key may be used to validate certificates for the entire usage period. If the FBCA private key is used to sign CRLs, it may be used to sign CRLs for the entire usage period.
	Match: **Comparable**	No requirements specified for Entity CAs.

<table>
<tr><th>Table No.</th><th>CP reference</th><th>Mapping Clause</th></tr>
<tr><td colspan="2">OVERALL MATCH:
POINT OF NOTE</td><td>Currently, in the FBCA for medium level assurance FIPS 140-1 level 2 is required, and for high level assurance FIPS level 3 is required. Whereas, FIPS 140 level 3 is required in QCP. However, the FBCA policy committee are putting in place a strategy for moving Medium Assurance to Level 3 CA Crypto-modules. Already most Entity CAs at medium assurance use FIPA level 3.</td></tr>
<tr><td rowspan="11">9</td><td></td><td>Certification authority key storage, backup and recovery</td></tr>
<tr><td>QCP
clause 7.2.2 a)</td><td>a) The CA private signing key shall be held and used within a secure cryptographic device which:
- meets the requirements identified in FIPS PUB 140-1, or FIPS 140-2 [6], level 3 or higher; or
- meets the requirements identified in one of the following CEN Workshop Agreement 14167-2 [10], 14167-3 [11], CWA 14167-4 [12]; or
- is a trustworthy system which is assured to EAL 4 or higher in accordance to ISO/IEC 15408 [8], or equivalent security criteria. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures.</td></tr>
<tr><td>FBCA CP
section 6.2.1</td><td>Cryptographic modules shall be validated to the FIPS 140 level identified in this section. Additionally, the Federal PKI Policy Authority reserves the right to review technical documentation associated with any cryptographic modules under consideration for use by the FBCA.
<table><tr><th>Assurance Level</th><th>CA</th></tr><tr><td>Medium</td><td>Level 2 (Hardware)</td></tr><tr><td>Medium Hardware</td><td>Level 2 (Hardware)</td></tr><tr><td>High</td><td>Level 3 (Hardware)</td></tr></table></td></tr>
<tr><td>Match:
Point of note</td><td>Currently, in the FBCA for medium level assurance FIPS 140-1 level 2 is required, and for high level assurance FIPS level 3 is required. Whereas, FIPS 140 level 3 is required in QCP. However, the FBCA policy committee are putting in place a strategy for moving Medium Assurance to Level 3 CA Crypto-modules. Already most Entity CAs at medium assurance use FIPA level 3.</td></tr>
<tr><td>QCP
clause 7.2.2 b)</td><td>b) When outside the secure cryptographic device (see (a) above) the CA private signing key shall be protected in a way that ensures the same level of protection as provided by the secure cryptographic device.</td></tr>
<tr><td>FBCA CP
section 6.2.1</td><td>Cryptographic modules shall be validated to the FIPS 140 level identified in this section.</td></tr>
<tr><td>Match:
Comparable</td><td>The FBCA policy committee are putting in place a strategy for moving Medium Assurance to FIPS 140-2 Level 3 CA Crypto-modules. For this FIPS 140-2 level it is required that "Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.</td></tr>
<tr><td>QCP
clause 7.2.2
c) d) e)</td><td>c) The CA private signing key shall be backed up, stored and recovered only by personnel in trusted roles using, at least, dual control in a physically secure environment. (see clause 7.4.4). The number of personnel authorized to carry out this function shall be kept to a minimum and be consistent with the CA's practices.
d) Backup copies of the CA private signing keys shall be subject to the same or greater level of security controls as keys currently in use.
e) Where the keys are stored in a dedicated key processing hardware module, access controls shall be in place to ensure that the keys are not accessible outside the hardware module.</td></tr>
<tr><td>FBCA CP
section 6.2.4.1</td><td>FBCA private signature keys shall be backed up under multi-person control, as specified in Section 5.2.2.
Backup of Entity CA private signature keys is required to facilitate disaster recovery. Where required by Section 5.2.2, Entity CA private signature keys shall be backed up under multi-person control.
No more than a single copy of the signature key shall be stored at the FBCA or Entity CA location. Additional copies may exist off-site provided that accountability for them is maintained.</td></tr>
<tr><td>Match:
Comparable</td><td></td></tr>
</table>

Table No.	CP reference	Mapping Clause
Overall Match: POINT OF NOTE		Currently, in the FBCA for medium level assurance FIPS 140-1 level 2 is required, and for high level assurance FIPS level 3 is required. Whereas, FIPS 140 level 3 is required in QCP. However, the FBCA policy committee are putting in place a strategy for moving Medium Assurance to Level 3 CA Crypto-modules. Already, most Entity CAs at medium assurance use FIPA level 3.
10		**Certification authority public key distribution**
	QCP clause 7.2.3	The CA shall ensure that the integrity and authenticity of the CA signature verification (public) key and any associated parameters are maintained during its distribution to relying parties (see the Directive [1], annex II (g) and annex II (f)). In particular: a) CA signature verification (public) keys shall be made available to relying parties in a manner that assures the integrity of the CA public key and authenticates its origin.
	FBCA CP section 6.1.4	When a CA updates its signature key pair, the CA shall distribute the new public key in a secure fashion. The new public key may be distributed in a self-signed certificate, in a key rollover certificate, or in a new CA (e.g., cross-) certificate obtained from the issuer(s) of the current CA certificate(s). Self-signed certificates shall be conveyed to relying parties in a secure fashion to preclude substitution attacks.
Overall Match: EQUIVALENT		
11		**Key Escrow**
	QCP clause 7.2.4	Subject private signing keys shall not be held in a way which provides a backup decryption capability, allowing authorized entities under certain conditions to decrypt data using information supplied by one or more parties (commonly called key escrow) (see the Directive , annex II (j)).
	FBCA CP section 6.2.3.1	Under no circumstances shall an FBCA or Entity CA signature key used to sign certificates or CRLs be escrowed.
	FBCA 6.2.3.3	Subscriber private signature keys shall not be escrowed.
Overall Match: EQUIVALENT		
12	QCP clause 7.2.5	**Certification authority key usage** The CA shall ensure that CA private signing keys are not used inappropriately. In particular: a) CA signing key(s) used for generating certificates, as defined in clause 7.3.3, may also be used to sign other types of certificates, as well as revocation status information, as long as operational requirements for the CA environment, as specified in 7.2.1 to 7.2.3, in 7.2.5 to 7.2.7 and in 7.4, are not violated; b) The certificate signing keys shall only be used within physically secure premises.
	FBCA CP section 6.1.7	The use of a specific key is determined by the key usage extension in the X.509 certificate. FBCA issued certificates and CA certificates issued by Entity CAs shall set two key usage bits: *cRLSign* and/or *keyCertSign*. Where the subject signs OCSP responses, the certificate may also set the *digitalSignature* and/or *nonRepudiation* bits.
	FBCA CP section 5.1.2.1	The FBCA and Entity CA equipment shall always be protected from unauthorized access. The security mechanisms shall be commensurate with the level of threat in the equipment environment. Since the FBCA must plan to issue certificates at all levels of assurance, it shall be operated and controlled on the presumption that it will be issuing at least one High Assurance certificate.
Overall Match: EQUIVALENT		
13		**End of CA key life cycle**
	QCP clause 7.2.6	The CA shall ensure that CA private signing keys are not used beyond the end of their life cycle (see the Directive [1], annex II (g) and annex II (f)). In particular: a) all copies of the CA private signing keys shall be destroyed or put beyond use.

Table No.	CP reference	Mapping Clause
	FBCAv1 clause 4.5.1	Types of Events Recorded All security auditing capabilities of the FBCA or Entity CA operating system and PKI CA applications required by this CP shall be enabled. … Destruction of cryptographic modules [for Medium level assurance]
	FBCA section 6.2.9	After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. Hardware cryptographic modules shall be removed and stored in a secure container when not in use.
	FBCA CP section 6.2.10	Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a "zeroize" command. Physical destruction of hardware should not be required.
Overall Match: **POINT OF NOTE**		Comment: a specific stipulation regarding CA Key destruction is not included in the FBCA CP, although this is provided for in subscriber keys.. The US FPKI will investigate adding this to the FBCA CP.
14		**Life cycle management of cryptographic hardware used to sign certificates**
	QCP clause 7.2.7	The CA shall ensure the security of cryptographic hardware throughout its lifecycle (see the Directive [1], annex II (f)). In particular the CA shall ensure that: a) certificate and revocation status information signing cryptographic hardware is not tampered with during shipment; b) certificate and revocation status information signing cryptographic hardware is not tampered with while stored; c) the installation, activation, back-up and recovery of the CA's signing keys in cryptographic hardware shall require simultaneous control of at least of two trusted employees; d) certificate and revocation status information signing cryptographic hardware is functioning correctly; and e) CA private signing keys stored on CA cryptographic hardware are destroyed upon device retirement.
	FBCA CP section 5.1.2.1	The FBCA and Entity CA equipment shall always be protected from unauthorized access. The security mechanisms shall be commensurate with the level of threat in the equipment environment. … In addition to those requirements, the following requirements shall apply to CAs that issue Medium, Medium Hardware, or High assurance certificates: • … • Require two person physical access control to both the cryptographic module and computer system Removable cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive CA equipment shall be placed in secure containers when not in use.
	FBCA section 6.2.9	After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. Hardware cryptographic modules shall be removed and stored in a secure container when not in use.

Table No.	CP reference	Mapping Clause
Overall Match: COMPARABLE		Comment: even though there is no requirement equivalent to the QCP requirement to destroy the CA private keys upon device retirement, its deactivation and its secure storage make the two specifications comparable.
15		**CA provided subject key management services**
	QCP clause 7.2.8	The CA shall ensure that any subject keys, that it generates, are generated securely and the secrecy of the subject's private key is assured (see the Directive [1], annex II (f) and (j)). If the CA generates the subject keys: a) CA-generated subject keys shall be generated using an algorithm recognized as being fit for the purposes of qualified electronic signatures during the validity time of the certificate. b) CA-generated subject keys shall be of a key length and for use with a public key algorithm which is recognized as being fit for the purposes of qualified electronic signatures during the validity time of the certificate. NOTE: See ETSI TS giving guidance on algorithms and their parameters to be published as TS 102 176-1 shortly after the current document has been published. c) CA-generated subject keys shall be generated and stored securely before delivery to the subject. d) The subject's private key shall be delivered to the subject, if required via the subscriber, in a manner such that the secrecy and the integrity of the key is not compromised and, once delivered to the subject, the private key can be maintained under the subject's sole control. e) Once delivered to the subject any copies of the subject's private key held by the CA shall be destroyed.
	FBCA CP section 6.1.1.2	Subscriber key pair generation may be performed by the subscriber, CA, or RA. If the CA or RA generates subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2 must also be met. Key generation shall be performed using a FIPS approved method or equivalent international standard.
	FBCA CP section 6.1.1.3	When CAs or RAs generate keys on behalf of the Subscriber, then the private key must be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met: • Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber. • The private key must be protected from activation, compromise, or modification during the delivery process. • The Subscriber shall acknowledge receipt of the private key(s). • Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers. o For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it. o For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel. o For shared key applications, organizational identities, and network devices, see also Section 3.2. The FBCA (or Entity CA) must maintain a record of the subscriber acknowledgement of receipt of the token.
	FBCA CP section 6.1.5	All FIPS-approved signature algorithms shall be considered acceptable additional restrictions on key sizes are detailed below. [detailed requirements on key size not copied] [See also memo regarding algorithm compromise in Annex A]
	FBCA CP section 6.1.6	Public key parameters for signature algorithms defined in the Digital Signature Standard (DSS) shall be generated in accordance with FIPS 186. Parameter quality checking (including primarily testing for prime numbers) shall be performed in accordance with FIPS 186; additional tests may be specified by the Federal PKI Policy Authority.

Table No.	CP reference	Mapping Clause
Overall Match: EQUIVALENT		
16	QCP clause 7.2.9	**Secure-signature-creation device preparation** The CA shall ensure that if it issues SSCD this is carried out securely (see the Directive, annex III). In particular, if the CA issues a SSCD: a) secure-signature-creation device preparation shall be securely controlled by the service provider; b) secure-signature-creation device shall be securely stored and distributed; c) secure-signature-creation device deactivation and reactivation shall be securely controlled; d) where the secure-signature device has associated user activation data (e.g. PIN code), the activation data shall be securely prepared and distributed separately from the secure signature-creation device.
	FBCA CP section 6.1.1.2	At the High and Medium Hardware assurance levels, subscriber key generation must be performed using a hardware cryptographic module.
	FBCA CP section 6.1.2	When CAs or RAs generate keys on behalf of the Subscriber, then the private key must be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met: • Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber. • The private key must be protected from activation, compromise, or modification during the delivery process. • The Subscriber shall acknowledge receipt of the private key(s). • Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers. o For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it. o For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel. o For shared key applications, organizational identities, and network devices, see also Section 3.2.
	FBCA CP section 6.2.8	The Subscriber must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).
	FBCA CP section 6.2.9	After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure, or automatically after a period of inactivity as defined in the applicable CPS. Hardware cryptographic modules shall be removed and stored in a secure container when not in use. If cryptographic modules are used to store subscriber private keys, then the cryptographic modules that have been activated shall not be left unattended or otherwise available to unauthorized access.
	FBCA CP section 6.2.10	Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a "zeroize" command. Physical destruction of hardware should not be required.

Table No.	CP reference	Mapping Clause
Overall Match: COMPARABLE		Comment: even if there is no specific requirements such as QCP 7.2.9.a, all the other requirements stipulate for the entire CA environment to be securely controlled, including the subscribers" key pairs generation in the subscribers" tokens on behalf of the subscribers
17		**Subject registration**
	QCP clause 7.3.1 a), b)	The CA shall ensure that subjects are properly identified and authenticated; and that subject certificate requests are complete, accurate and duly authorized (see the Directive [1], annex II (d)). In particular: a) Before entering into a contractual relationship with a subscriber, the CA shall inform the subscriber of the terms and conditions regarding use of the certificate as given in clause 7.3.4 (see the Directive, annex II (k)). b) The CA shall communicate this information through a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language.
	FBCA CP section 9.6.3	For Medium, Medium Hardware, and High Assurance levels, a Subscriber shall be required to sign a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate.
	Match Equivalent	
	QCP clause 7.3.1 c), d), e)	c) The service provider shall verify at time of registration by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued. Evidence of the identity shall be checked against a physical person either directly or shall have been checked indirectly using means which provides equivalent assurance to physical presence (see note 3). Submitted evidence may be in the form of either paper or electronic documentation. d) Where the subject is a person evidence shall be provided of: - full name (including surname and given names consistent with the applicable law and national identification practices); - date and place of birth, a nationally recognized identity number, or other attributes which may be used to, as far as possible, distinguish the person from others with the same name. e) Where the subject is a person who is identified in association with a legal person, or other organizational entity, evidence shall be provided of: - full name (including surname and given names) of the subject; - date and place of birth, a nationally recognized identity number, or other attributes of the subject which may be used to, as far as possible, distinguish the person from others with the same name; - full name and legal status of the associated legal person or other organizational entity; - any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity; - evidence that the subject is associated with the legal person or other organizational entity.

<table>
<tr><th>Table No.</th><th>CP reference</th><th>Mapping Clause</th></tr>
<tr><td></td><td>FBCA CP section 3.2.3.1</td><td>For Subscribers, the FPKI Operational Authority or Entity CA, and/or associated RAs shall ensure that the applicant's identity information is verified in accordance with the process established by the applicable CP and CPS. Process information shall depend upon the certificate level of assurance and shall be addressed in the FBCA or Entity CPS. The documentation and authentication requirements shall vary depending upon the level of assurance.

….

For All Levels: If an applicant is unable to perform face-to-face registration (e.g., a network device), the applicant may be represented by a trusted person already issued a digital certificate by the Entity. The trusted person will present information sufficient for registration at the level of the certificate being requested, for both himself/herself and the applicant who the trusted person is representing.

For the Basic and Medium Assurance Levels: An entity certified by a State or Federal Entity as being authorized to confirm identities may perform in-person authentication on behalf of the RA. The certified entity forwards the information collected from the applicant directly to the RA in a secure manner. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement; other secure methods are also acceptable. Such authentication does not relieve the RA of its responsibility to verify the presented data.

…
<table>
<tr><td>Medium (all policies)</td><td>Identity shall be established by in-person proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License)</td></tr>
</table>
</td></tr>
</table>

Table No.	CP reference	Mapping Clause
	Match: Equivalent	
	QCP Clause 7.3.1 f) – j)	f) The CA shall record all the information used to verify the subjects' identity and, if applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity. g) If an entity other than the subject is subscribing to the CA services (i.e. the subscriber and subject are separate entities – see 4.4) then evidence shall be provided that the subscriber is authorized to act for the subscriber as identified (e.g. is authorized for all members of the identified organization). h) The subscriber shall provide a physical address, or other attributes, which describe how the subscriber may be contacted. i) The CA shall record the signed agreement with the subscriber including: - agreement to the subscriber's obligations (see clause 6.2); - if required by the CA, agreement to use a SSCD; - consent to the keeping of a record by the CA of information used in registration (see clause 7.4.11 h), i), j)), subject device provision (see clause 7.4.11 items m), n) and any subsequent revocation (see clause 7.4.11 o)), identity and any specific attributes of the subject placed in the certificate, and the passing of this information to third parties under the same conditions as required by this policy in the case of the CA terminating its services; - whether, and under what conditions, the subscriber requires and the subject's consents to the publication of the certificate; - confirmation that the information held in the certificate is correct. j) The records identified above shall be retained for the period of time as indicated to the subscriber (see a) and b) above) and as necessary for the purposes for providing evidence of certification in legal proceedings according to the applicable law.
	FBCA CP section 3.2.3.1	**Authentication of Human Subscribers** The FPKI Operational Authority, Entity CAs and/or RAs shall record the information set forth below for issuance of each certificate: • The identity of the person performing the identification; • A signed declaration by that person that he or she verified the identity of the applicant as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law; • If in-person identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s); • The date of the verification; and • A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.
	FBCA CP section 3.3.2	Requests for FBCA or Entity CA certificates in the name of an organization shall include the organization name, address, and documentation of the existence of the organization. The FPKI Operational Authority or Entity RA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

Table No.	CP reference	Mapping Clause
	FBCA CP section 9.6.3	For Medium, Medium Hardware, and High Assurance levels, a Subscriber shall be required to sign a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. …. Subscribers of Entity CAs at Basic, Medium, and High Assurance Levels shall agree to the following: • Accurately represent themselves in all communications with the PKI authorities. • Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures. • Promptly notify the appropriate CA upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS. • Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.
	Match: Comparable	
	QCP clause 7.3.1 k) l)	k) If the subject's key pair is not generated by the CA, the certificate request process shall ensure that the subject has possession of the private key associated with the public key presented for certification. l) If the subject's key pair is not generated by the CA and the certificate policy requires use of an SSCD (i.e. QCP public + SSCD), the certificate request process shall ensure that the public key to be certified is from a key pair effectively generated by a SSCD.
	FBCA CP section 3.2.1	In all cases where the party named in a certificate generates its own keys that party shall be required to prove possession of the private key that corresponds to the public key in the certificate request.
	FBCA CP section 6.1.1.2	**Subscriber Key Pair Generation** … Key generation shall be performed using a FIPS approved method or equivalent international standard. At the High and Medium Hardware assurance levels, subscriber key generation must be performed using a hardware cryptographic module
	Match: Comparable	
Overall match: COMPARABLE		
18		**Certificate renewal, rekey and update**
	QCP clause 7.3.2	The CA shall ensure that requests for certificates issued to a subject who has already previously been registered are complete, accurate and duly authorized. This includes certificate renewals, rekey following revocation or prior to expiration, or update due to change to the subject's attributes (see the Directive [1], annex II (g)). In particular: a) The CA shall check the existence and validity of the certificate to be renewed and that the information used to verify the identity and attributes of the subject is still valid. b) If any of the CA terms and conditions have changed, these shall be communicated to the subscriber and agreed to in accordance with clause 7.3.1 a), b) and i). c) If any certified names or attributes have changed, or the previous certificate has been revoked, the registration information is verified, recorded, agreed to by the subscriber in accordance with clause 7.3.1 c) to g). d) The CA shall issue a new certificate using the subject's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's validity period and no indications exist that the subject's private key has been compromised.

<table>
<tr><th>Table No.</th><th>CP reference</th><th>Mapping Clause</th></tr>
<tr><td></td><td>FBCA CP
section 3.3.1</td><td>Identification and Authentication for Routine Re-key
In the event that a Principal CA re-key is required, a new certificate will be issued to Principal CAs by the FBCA. Before issuance, the Principal CA shall identify itself through use of its current signature key or the initial registration process. If it has been more than three years since a Principal CA was identified as required in Section 3.2, identity shall be re-established through the initial registration process.

<table><tr><td>Medium
(all policies)</td><td>Identity may be established through use of current signature key, except that identity shall be established through initial registration process at least once every nine years from the time of initial registration.</td></tr></table>
Identification and Authentication for Re-key after Revocation
After a certificate has been revoked other than during a renewal or update action, the subscriber is required to go through the initial registration process described in Section 3.2 to obtain a new certificate. (This applies to all certificates issued by both Entity CAs and the FBCA.)</td></tr>
<tr><td></td><td>FBCA CP
section 4.6</td><td>Certificate Renewal
Certificate renewal consists of issuing a new certificate with a new validity period and serial number while retaining all other information in the original certificate including the public key. Frequent renewal of certificates may assist in reducing the size of CRLs.
Circumstance for Certificate Renewal
A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged. In addition, the validity period of the certificate must meet the requirements specified in Section 6.3.2.</td></tr>
<tr><td></td><td>FBCA CP
section 4.7</td><td>Certificate Re-Key
Re-keying a certificate consists of creating new certificates with a different public key (and serial number) while retaining the remaining contents of the old certificate that describe the subject. The new certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point, and/or be signed with a different key.
Subscribers of Entity CAs shall identify themselves for the purpose of re-keying as required in Section 3.3.1</td></tr>
<tr><td></td><td>FBCA CP
section 4.8</td><td>Modification
Certificate modification consists of creating new certificates with subject information (e.g., a name or email address) that differs from the old certificate. For example, an Entity CA may perform certificate modification for a Subscriber whose characteristics have changed (e.g., has just received a medical degree). The new certificate may have the same or different subject public key.
…
Processing Certificate Modification Requests
For Entity CAs, proof of all subject information changes must be provided to the RA or other designated agent and verified before the modified certificate is issued.</td></tr>
<tr><td></td><td>FBCA CP
section 6.1.5</td><td>Key Sizes
All FIPS-approved signature algorithms shall be considered acceptable; additional restrictions on key sizes are detailed below.</td></tr>
</table>

Table No.	CP reference	Mapping Clause
Overall Match: COMPARABLE		Comment: No explicit requirement relating to changes in terms and conditions (7.3.2.b) otherwise equivalent.
19		**Certificate generation**
	QCP clause 7.3.3 a)	The CA shall ensure that it issues certificates securely to maintain their authenticity (see the Directive [1], annex II (g)). In particular: a) the certificates are generated and issued in accordance with annexes I of the Directive [1]. Qualified certificates must contain: - an indication that the certificate is issued as a qualified certificate; - the identification of the CA [Certification-Service-Provider] and the State in which it is established; - the name of the signatory or a pseudonym, which shall be identified as such; - provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended; - signature-verification data which correspond to signature-creation data under the control of the signatory; - an indication of the beginning and end of the period of validity of the certificate; - the identity code of the certificate; - the advanced electronic signature of the certification-service-provider issuing it; - limitations on the scope of use of the certificate, if applicable; and - limits on the value of transactions for which the certificate can be used, if applicable.
	FBCA CP section 7.1	The FBCA and Entity CAs shall issue X.509 v3 certificates
	Match: Comparable	Comments: General requirements for certificate met through X.509. Specific requirement to indicate that certificate is qualified is not applicable, although comparable certificate policy identifier is included in the certificate to indicate that the CA complies with the FBCA CP.
	QCP clause 7.3.3 b) to g)	b) The CA shall take measures against forgery of certificates, and, in cases where the CA generates signature-creation data, guarantee confidentiality during the process of generating such data; (see II (g) of the Directive [1]). c) the procedure of issuing the certificate is securely linked to the associated registration, certificate renewal or rekey, including the provision of any subject generated public key. d) if the CA generated the subjects key: - the procedure of issuing the certificate is securely linked to the generation of the key pair by the CA; - the private key (or SSCD - see clause 7.2.9) is securely passed to the registered subject. e) The CA shall ensure over time the uniqueness of the distinguished name assigned to the subject within the domain of the CA. (i.e. over the life time of the CA a distinguished name which has been used in an issued certificate shall never be re-assigned to another entity). f) The confidentiality and integrity of registration data shall be protected especially when exchanged with the subscriber, subject or between distributed CA system components. g) The CA shall verify that registration data is exchanged with recognized registration service providers, whose identity is authenticated, in the event that external registration service providers are used.
	FBCA CP section 4.3	**CA Actions during Certificate Issuance** Entity CAs shall verify the source of a certificate request before issuance.
	FBCA CP section 3.2.1	In all cases where the party named in a certificate generates its own keys that party shall be required to prove possession of the private key that corresponds to the public key in the certificate request.

Table No.	CP reference	Mapping Clause
	FBCA CP section 6.1.2	When CAs or RAs generate keys on behalf of the Subscriber, then the private key must be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements must be met: • Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber. • The private key must be protected from activation, compromise, or modification during the delivery process. • The Subscriber shall acknowledge receipt of the private key(s). • Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers. …
	FBCA CP section 3.1.5	Name uniqueness must be enforced by the FBCA and Entity CAs.
	FBCA CP section 9.4	**Responsibility to Protect Private Information** Sensitive information must be stored securely, and may be released only in accordance with other stipulations in Section 9.4. **Notice and Consent to use Private Information** The FPKI Operational Authority is not required to provide any notice or obtain the consent of the Subscriber or Entity personnel in order to release private information in accordance with the stipulations of Section 9.4. **Disclosure Pursuant to Judicial/Administrative Process** The FPKI Operational Authority shall not disclose private information to any third party unless authorized by this Policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information shall be processed according to 41 CFR 105-60.605.
	FBCA CP section 3.2.3.1	**For the Basic and Medium Assurance Levels:** An entity certified by a State or Federal Entity as being authorized to confirm identities may perform in-person authentication on behalf of the RA. The certified entity forwards the information collected from the applicant directly to the RA in a secure manner. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement; other secure methods are also acceptable. Such authentication does not relieve the RA of its responsibility to verify the presented data.
	FBCA CP section 6.7	**Network Security Controls** Entity CAs and directories shall employ appropriate network security controls. Networking equipment shall turn off unused network ports and services. Any network software present shall be necessary to the functioning of the equipment.

Table No.	CP reference	Mapping Clause
Overall Match: COMPARABLE		No specific requirements relating to security of exchanged information (QCP 7.3.3 f & g), however general requirements for the security of the CA are expected to include distribution.)
20	QCP Clause 7.3.4	**Dissemination of Terms and Conditions** The CA shall ensure that the terms and conditions are made available to subscribers and relying parties (see the Directive 1, annex II (k)). a) The CA shall make available to subscribers and relying parties the terms and conditions regarding the use of the certificate including the Directive [1], annex II (k): - the qualified certificate policy being applied, including a clear statement as to whether the policy is for certificates issued to the public and whether the policy requires uses of a SSCD; - any limitations on its use; - the subscriber's obligations as defined in clause 6.2, including whether the policy requires uses of a SSCD; - information on how to validate the certificate, including requirements to check the revocation status of the certificate, such that the relying party is considered to "reasonably rely" on the certificate (see clause 6.3); - limitations of liability including the purposes/uses for which the CA accepts (or excludes) liability; - the period of time which registration information (see clause 7.3.1) is retained; - the period of time which CA event logs (see clause 7.4.11) are retained; - procedures for complaints and dispute settlement; - the applicable legal system; and - if the CA has been certified to be conformant with the identified qualified certificate policy, and if so through which scheme. b) The information identified in a) above shall be available through a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language.
	FBCA CP section 9.6.3	For Medium, Medium Hardware, and High Assurance levels, a Subscriber shall be required to sign a document containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate. ….. Subscribers of Entity CAs at Basic, Medium, and High Assurance Levels shall agree to the following: • Accurately represent themselves in all communications with the PKI authorities. • Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures. • Promptly notify the appropriate CA upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS. • Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.

Table No.	CP reference	Mapping Clause
Overall Match: COMPARABLE, POINT OF NOTE		Provision of terms and conditions to Relying party is not directly addressed. The FBCA does not directly address issues relating to levels of service to the subscribers and relying party where this does not affect the security of the certificate.
21	QCP clause 7.3.5	**Certificate dissemination** The CA shall ensure that certificates are made available as necessary to subscribers, subjects and relying parties (see the Directive [1], annex II (l)). In particular: a) upon generation, the complete and accurate certificate shall be available to subscriber or subject for whom the certificate is being issued; b) certificates are available for retrieval in only those cases for which the subject's consent has been obtained; c) the CA shall make available to relying parties the terms and conditions regarding the use of the certificate (see clause 7.3.4); d) the applicable terms and conditions shall be readily identifiable for a given a certificate; e) the information identified in b) and c) above shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the CA, the CA shall make best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the certification practice statement; f) The information identified in b) and c) above shall be publicly and internationally available.
	FBCA CP section 2.2.1	**Publication of Certificates and Certificate Status** The FPKI Operational Authority shall publish all CA certificates issued by or to the FBCA and all CRLs issued by the FBCA in the FBCA repository. At a minimum, the Entity repositories shall contain all CA certificates issued by or to the Entity PKI and CRLs issued by the Entity PKI.
	FBCA CP section 2.2.2	**Publication of CA Information** The FPKI Operational Authority shall publish information concerning the FBCA necessary to support its use and operation. The FBCA CP shall be publicly available on the FPKI PA website (see http://www.cio.gov/fpkipa). The FBCA CPS will not be published; a redacted version of the CPS will be publicly available from the FPKI PA website (see http://www.cio.gov/fpkipa). Publication of CA information in the Entity repositories is a local decision.
	FBCA CP section 2.3	This CP and any subsequent changes shall be made publicly available within one week of approval.
	FBCA CP section 2.4	The FPKI Operational Authority shall protect any repository information not intended for public dissemination or modification. Certificates and certificate status information in the FBCA repository shall be publicly available through the Internet. Access to information in Entity CA repositories shall be determined by the Entity pursuant to the rules and statutes that apply to that entity. Certificates and certificate status information in the Entity repository should be publicly available through the Internet wherever reasonable. At a minimum, the Entity repositories shall make CA certificates and CRLs issued by the Entity PKI and CA certificates issued to the Entity PKI available to Federal Relying Parties.
	FBCA CP section 5.7.4	The FBCA directory system shall be deployed so as to provide 24 hour, 365 day per year availability. The FPKI Operational Authority shall implement features to provide high levels of directory reliability.

Table No.	CP reference	Mapping Clause
Overall Match: COMPARABLE POINT OF NOTE		Specific requirements for availability of Entity CA repository not addressed. The FBCA does not directly address issues relating to levels of service to the subscribers and relying party where this does not affect the security of the certificate. This is not seen as a hindrance for mutual recognition.
22		**Certificate revocation and suspension**
	QCP clause 7.3.6 a)	The CA shall ensure that certificates are revoked in a timely manner based on authorized and validated certificate revocation requests (see the Directive [1], annex II (b)). In particular: a) The CA shall document as part of its certification practice statement (see 7.1) the procedures for revocation of certificates including: - who may submit revocation reports and requests; - how they may be submitted; - any requirements for subsequent confirmation of revocation reports and requests; - whether and for what reasons certificates may be suspended; - the mechanism used for distributing revocation status information; - the maximum delay between receipt of a revocation request or report and the change to revocation status information being available to all relying parties. This shall be at most 1 day.
	FBCA CP section 4.9	For High, Medium Hardware, Medium, and Basic Assurance, all CAs shall publish CRLs.
	FBCA CP section 4.9.1	**Circumstances for Revocation** Entity CAs that implement certificate revocation shall, at a minimum, revoke certificates for the reason of key compromise upon receipt of an authenticated request from an appropriate entity. Other circumstances for certificate revocation may be supported by Entity CAs.
	FBCA CP section 4.9.2	**Who Can Request Revocation** Entity CAs that implement certificate revocation shall, at a minimum, accept revocation requests from subscribers. Requests for certificate revocation from other parties may be supported by Entity CAs. Note that an Entity Principal CA may always revoke the certificate it has issued to the FBCA without any Federal PKI Policy Authority action.
	FBCA CP section 4.9.3	Entity CAs that implement certificate revocation shall revoke certificates upon receipt of sufficient evidence of compromise or loss of the subscriber's corresponding private key. A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). Where subscribers use hardware tokens, revocation is optional if all the following conditions are met: • the revocation request was not for key compromise; • the hardware token does not permit the user to export the signature private key; • the Subscriber surrendered the token to the PKI; • the token was zeroized or destroyed promptly upon surrender; • the token has been protected from malicious use between surrender and zeroization or destruction. In all other cases, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates is recommended.

<table>
<tr><th>Table No.</th><th>CP reference</th><th>Mapping Clause</th></tr>
<tr><td></td><td>FBCA CP
section 4.9.7</td><td>CRL Issuance Frequency
For this CP, CRL issuance encompasses both CRL generation and publication. For the FBCA, the interval between CRLs shall not exceed 24 hours. In the case of revocation of a certificate, the FBCA shall issue an emergency CRL within six hours.
For Entity CAs, see the table below for issuing frequency of routine and emergency CRLs. For Basic, Medium, Medium Hardware, and High, Emergency CRLs shall be issued whenever a CA certificate is revoked, or any certificate is revoked because of key compromise. CRLs may be issued more frequently than specified below.
<table>
<tr><th>Assurance Level</th><th>Maximum Interval for Routine CRL Issuance</th><th>Maximum Interval for Emergency CRL Issuance</th></tr>
<tr><td>Medium (all policies)</td><td>24 hours</td><td>18 hours after notification</td></tr>
</table></td></tr>
<tr><td></td><td>FBCA CP
section 4.9.9</td><td>On-line Revocation/Status Checking Availability
If on-line revocation/status checking is supported by an Entity CA, the latency of certificate status information distributed on-line by Entity CAs or their delegated status responders must meet or exceed the requirements for CRL issuance stated in 4.9.7.</td></tr>
<tr><td></td><td>Match:
Comparable</td><td></td></tr>
<tr><td></td><td>QCP
clause 7.3.6 b) to c)</td><td>The CA shall ensure that certificates are revoked in a timely manner based on authorized and validated certificate revocation requests (see the Directive [1], annex II (b)).
In particular:
b) Requests and reports relating to revocation (e.g. due to compromise of subject's private key, death of the subject, unexpected termination of a subscriber's or subject's agreement or business functions, violation of contractual obligations) shall be processed on receipt.
c) Requests and reports relating to revocation shall be authenticated, checked to be from an authorized source. Such reports and requests will be confirmed as required under the CA's practices.</td></tr>
<tr><td></td><td>FBCA CP
section 4.9.5</td><td>Time within which CA must Process the Revocation Request
For the FBCA, all revocation requests must be processed within six hours of receipt of request.
For Entity CAs, revocation request processing time shall be as specified below:
<table>
<tr><td>Medium (all policies)</td><td>Within 18 hours of receipt of request</td></tr>
</table></td></tr>
<tr><td></td><td>FBCA CP
section 3.4</td><td>Revocation requests must be authenticated. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.</td></tr>
<tr><td></td><td>Match:
Comparable</td><td>Given the requirements for CRL issuance in 4.9.7 difference in requirement for processing request is not considered significant.</td></tr>
<tr><td></td><td>QCP clause
7.3.6 d)</td><td>d) A certificate's revocation status may be set to suspended whilst the revocation is being confirmed. The CA shall ensure that a certificate is not kept suspended for longer than is necessary to confirm its status.</td></tr>
<tr><td></td><td>FBCA CP
section 4.9.13</td><td>Suspension shall not be used by the FBCA.

For Entity CAs, no stipulation.</td></tr>
<tr><td></td><td>Match:
Point of Note</td><td>Handling of suspension for Entity CAs is unspecified.</td></tr>
<tr><td></td><td>QCP
clause 7.3.6 e)</td><td>e) The subject, and where applicable the subscriber, of a revoked or suspended certificate, shall be informed of the change of status of its certificate.</td></tr>
<tr><td></td><td>FBCA CP
section 2.2.1</td><td>Publication of Certificates and Certificate Status
The FPKI Operational Authority shall publish all CA certificates issued by or to the FBCA and all CRLs issued by the FBCA in the FBCA repository.

At a minimum, the Entity repositories shall contain all CA certificates issued by or to the Entity PKI and CRLs issued by the Entity PKI.</td></tr>
<tr><td></td><td>Match:
Comparable</td><td>Information is made available through repositories although not directly to the subscriber. The Federal PKI will investigate notification of the subscriber in the case of revocation.</td></tr>
<tr><td></td><td>QCP
clause 7.3.6 f)</td><td>f) Once a certificate is definitively revoked (i.e. not suspended) it shall not be reinstated.</td></tr>
</table>

<table>
<tr><th>Table No.</th><th>CP reference</th><th>Mapping Clause</th></tr>
<tr><td></td><td>Match:
Comparable</td><td>Implied by meaning of revoked</td></tr>
<tr><td></td><td>QCP
clause 7.3.6 g)</td><td>g) Where Certificate Revocation Lists (CRLs) including any variants (e.g. Delta CRLs) are used, these shall be published at least daily and:
- every CRL shall state a time for next CRL issue; and
- a new CRL may be published before the stated time of the next CRL issue;
- the CRL shall be signed by the certification authority or an entity designated by the CA.</td></tr>
<tr><td></td><td>FBCA CP
section 4.9.7</td><td>CRL Issuance Frequency
For this CP, CRL issuance encompasses both CRL generation and publication. For the FBCA, the interval between CRLs shall not exceed 24 hours. In the case of revocation of a certificate, the FBCA shall issue an emergency CRL within six hours.
For Entity CAs, see the table below for issuing frequency of routine and emergency CRLs. For Basic, Medium, Medium Hardware, and High, Emergency CRLs shall be issued whenever a CA certificate is revoked, or any certificate is revoked because of key compromise. CRLs may be issued more frequently than specified below.
<table>
<tr><th>Assurance Level</th><th>Maximum Interval for Routine CRL Issuance</th><th>Maximum Interval for Emergency CRL Issuance</th></tr>
<tr><td>Medium (all policies)</td><td>24 hours</td><td>18 hours after notification</td></tr>
</table></td></tr>
<tr><td></td><td>Match:
Comparable</td><td>Content of CRL implied through use of X.509 CRLs</td></tr>
<tr><td></td><td>QCP
clause 7.3.6
h),i)</td><td>h) Revocation management services shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which are not under the control of the CA, the CA shall make best endeavours to ensure that this service is not unavailable for longer than a maximum period of time as denoted in the certification practice statement.
i) Revocation status information, shall be available 24 hours per day, 7 days per week. Upon system failure, service or other factors which is not under the control of the CA, the CA shall make best endeavours to ensure that this information service is not unavailable for longer than a maximum period of time as denoted in the certification practice statement.</td></tr>
<tr><td></td><td>FBCA CP
section 4.9.5</td><td>Time within which CA must Process the Revocation Request
For the FBCA, all revocation requests must be processed within six hours of receipt of request.
For Entity CAs, revocation request processing time shall be as specified below:
<table>
<tr><td>Medium (all policies)</td><td>Within 18 hours of receipt of request</td></tr>
</table></td></tr>
<tr><td></td><td>FBCA CP
section 5.7.4</td><td>The FBCA directory system shall be deployed so as to provide 24 hour, 365 day per year availability. The FPKI Operational Authority shall implement features to provide high levels of directory reliability.

The FPKI Operational Authority shall operate a hot backup site, whose purpose is to ensure continuity of operations in the event of failure of the primary site. The FBCA operations shall be designed to restore full service within six (6) hours of primary system failure.</td></tr>
<tr><td></td><td>Match:
Comparable</td><td>Requirements for processing and publishing revocation requests within 18 hours implies high availability.</td></tr>
<tr><td></td><td>QCP
clause 7.3.6 j)</td><td>j) The integrity and authenticity of the status information shall be protected.</td></tr>
<tr><td></td><td>Match:
Comparable</td><td>Comment: CRLs include authenticity and integrity protection.</td></tr>
<tr><td></td><td>QCP
clause 7.3.6 k),</td><td>k) Revocation status information shall be publicly and internationally available.</td></tr>
<tr><td></td><td>FBCA CP
section 2.4</td><td>Access to information in Entity CA repositories shall be determined by the Entity pursuant to the rules and statutes that apply to that entity. Certificates and certificate status information in the Entity repository should be publicly available through the Internet wherever reasonable. At a minimum, the Entity repositories shall make CA certificates and CRLs issued by the Entity PKI and CA certificates issued to the Entity PKI available to Federal Relying Parties.</td></tr>
</table>

Table No.	CP reference	Mapping Clause
	Match: Comparable	Comment: Scope of FBCA is not to provide services to the public although it is required to make the repository publicly available wherever possible.
	QCP clause 7.3.6 l)	l) Revocation status information shall include information on the status of certificates at least until the certificate expires
	FBCA CP section 4.9.1	… Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.
	Match: Equivalent	
Overall Match: COMPARABLE		See 7.6.3 d, e, above. Handling of suspension for Entity CAs is unspecified. The FBCA does not directly address issues relating to levels of service to the subscribers and relying party where this does not effect the security of the certificate. The Federal PKI will investigate notification of the subscriber in the case of revocation.
23		**Security management**
	QCP clause 7.4.1	The CA shall ensure that administrative and management procedures are applied which are adequate and correspond to recognized standards (see the Directive [1], annex II (e), 2nd part). In particular: a) The CA shall carry out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. The risk analysis shall be regularly reviewed and revised if necessary. b) The CA shall retain responsibility for all aspects of the provision of certification services, even if some functions are outsourced to subcontractors. Responsibilities of third parties shall be clearly defined by the CA and appropriate arrangements made to ensure that third parties are bound to implement any controls required by the CA. The CA shall retain responsibility for the disclosure of relevant practices of all parties. c) The CA management shall provide direction on information security through a suitable high level steering forum that is responsible for defining the CA's information security policy and ensuring publication and communication of the policy to all employees who are impacted by the policy. d) The CA shall have a system or systems for quality and information security management appropriate for the certification services it is providing. e) The information security infrastructure necessary to manage the security within the CA shall be maintained at all times. Any changes that will impact on the level of security provided shall be approved by the CA management forum. f) The security controls and operating procedures for CA facilities, systems and information assets providing the certification services shall be documented, implemented and maintained. g) CA shall ensure that the security of information shall be maintained when the responsibility for CA functions has been outsourced to another organization or entity.
	FBCA CP section 1.3.1.6	The FBCA is the entity operated by the FBCA Operational Authority that is authorized by the Federal PKI Policy Authority to create, sign, and issue public key certificates to Principal CAs. As operated by the FBCA Operational Authority, the FBCA is responsible for all aspects of the issuance and management of a certificate including: ….
	FBCA CP section 1.3.2	… The requirements for RAs in the FBCA and Entity PKIs are set forth elsewhere in this document.
	FBCA CP section 1.3 5	The FBCA and Entity CAs may require the services of other security, community, and application authorities. If required, the FBCA or Entity CPS shall identify the parties, define the services, and designate the mechanisms used to support these services.

Table No.	CP reference	Mapping Clause
	FBCA CP section 1.4.1	The sensitivity of the information processed or protected using certificates issued by FBCA or an Entity CA will vary significantly. Relying Parties must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. …. … *Medium*: This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. *Medium Hardware*: This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk..
	FBCA CP section 1.5.1	The Federal PKI Policy Authority is responsible for all aspects of this CP.
	FBCA CP section 1.5.4	**CPS Approval Procedures** The FPKI Operational Authority shall submit the FBCA CPS and the results of a compliance analysis study to the FPKI PA for approval. The FPKI PA shall vote to accept or reject the CPS and accompanying analysis. If rejected, the FPKI Operational Authority shall resolve the identified discrepancies and resubmit to the FPKI PA.
	FBCA CP section 6.6.2	The configuration of the FBCA or Entity CA system as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to the FBCA or Entity CA software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of the FBCA or Entity CA system.
	FBCA CP section 8	The FPKI Operational Authority shall have a compliance audit mechanism in place to ensure that the requirements of this CP and the FBCA CPS are being implemented and enforced. Entity CAs shall have a compliance audit mechanism in place to ensure that the requirements of their CP/CPS are being implemented and enforced. This specification does not impose a requirement for any particular assessment methodology.
	FBCA CP section 8.6	**Communication of Results** Upon completion, an Audit Compliance Report letter shall be provided to the Federal PKI Policy Authority. The report shall identify the versions of the CP and CPS used in the assessment. Additionally, where necessary, the results shall be communicated as set forth in Section 8.5 above.
Overall Match: COMPARABLE		Whilst FBCA CP does not require security management and risk assessment (as described in the QCP), the development of the FBCA CP and the audit of the CAs against this CP are considered sufficient to ensure a comparable level of security.
24	QCP clause 7.4.2	**Asset classification and management** The CA shall ensure that its assets and information receive an appropriate level of protection. (see the Directive 1, annex II (e)). a) The CA shall maintain an inventory of all information assets and shall assign a classification for the protection requirements to those assets consistent with the risk analysis.
Overall Match: COMPARABLE POINT OF NOTE		Whilst FBCA CP does not require formal asset classification, the development of the FBCA CP and the audit of the CAs against this CP are considered sufficient to ensure a comparable level of security.

Table No.	CP reference	Mapping Clause
25	QCP clause 7.4.3	**Personnel security** The CA shall ensure that personnel and hiring practices enhance and support the trustworthiness of the CA's operations (see [1], annex II (e) 1st part). In particular: a) The CA shall employ a sufficient number of personnel which possess the expert knowledge, experience and qualifications necessary for the offered services and as appropriate to the job function. b) Appropriate disciplinary sanctions shall be applied to personnel violating CA policies or procedure. c) Security roles and responsibilities, as specified in the CA's security policy, shall be documented in job descriptions. Trusted roles, on which the security of the CA's operation is dependent, shall be clearly identified. d) CA personnel (both temporary and permanent) shall have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. Where appropriate, these shall differentiate between general functions and CA specific functions. e) Personnel shall exercise administrative and management procedures and processes that are in line with the CA's information security management procedures (see clause 7.4.1). f) Managerial personnel shall be employed who possess experience or training in electronic signature technology and familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions. g) All CA personnel in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the CA operations. h) Trusted roles include roles that involve the following responsibilities: - Security Officers: Overall responsibility for administering the implementation of the security practices. Additionally approve the generation/revocation/suspension of certificates; - System Administrators: Authorized to install, configure and maintain the CA trustworthy systems for registration, certificate generation, subject device provision and revocation management; - System Operators: Responsible for operating the CA trustworthy systems on a day to day basis. Authorized to perform system backup and recovery; - System Auditors: Authorized to view archives and audit logs of the CA trustworthy systems. i) CA personnel shall be formally appointed to trusted roles by senior management responsible for security. j) The CA shall not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position. Personnel shall not have access to the trusted functions until any necessary checks are completed.

Table No.	CP reference	Mapping Clause
	FBCA CP section 5.2.1	A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the FBCA or an Entity CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion. The requirements of this policy are defined in terms of four roles. (Note: the information derives from the Certificate Issuing and Management Components (CIMC) Protection Profile.) 1. *Administrator* – authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys. 2. *Officer* – authorized to request or approve certificates or certificate revocations. 3. *Auditor* – authorized to maintain audit logs. 4. *Operator* – authorized to perform system backup and recovery. Some roles may be combined. The roles required for each level of assurance are identified in Section 5.2.4.
	FBCA CP section 5.2.4	*Medium (all policies):* Individual CA personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume more than one role; however, individuals who assume an Officer role may not assume an Administrator or Auditor role. The CA system shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and an Officer role or an Auditor and an Officer role. No individual shall be assigned more than one identity.
	FBCA CP section 5.3.1	**Background, Qualifications, Experience, & Security Clearance Requirements** Each Entity shall identify at least one individual or group responsible and accountable for the operation of each CA in that Entity. For the FBCA, these are the Federal PKI Policy Authority and the FPKI Operational Authority. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity. For the FBCA and Federal Agency PKIs, regardless of the assurance level, and for state and local government PKIs operated in the U.S. at High Assurance, all trusted roles are required to be held by U.S. citizens. For PKIs operated at Medium Assurance and Medium Hardware, all trusted roles must be held by citizens of the country where the CA is located. For PKIs operated at Medium-CBP and Medium Hardware-CBP, there is no citizenship requirement specified. Where an entity PKI operated at Medium or Medium Hardware Assurance is affiliated with RAs operated overseas, RA personnel holding trusted roles may be local citizens of the country where the RA is located or of the country where the CA is located. FPKI Operational Authority personnel acting in trusted roles shall hold TOP SECRET security clearances.
	FBCA CP section 5.3.2	**Background Check Procedures** Entity CA personnel shall, at a minimum, pass a background investigation covering the following areas: • …
	FBCA CP section 5.3.7	Contractor personnel employed to perform functions pertaining to the FBCA or an Entity CA shall meet the personnel requirements set forth in the FBCA CP or Entity CP, as applicable.
	FBCA CP section 5.3.8	For the FBCA and Entity CAs, documentation sufficient to define duties and procedures for each trusted role shall be provided to the personnel filling that role.

Table No.	CP reference	Mapping Clause
Overall Match: COMPARABLE		Comments: Requirement regarding conflict of interest (7.4.3 g) not directly addressed. However, the FBCA controls are considered provide equivalent level of personal security.
26	QCP clause 7.4.4	**Physical and environmental security** The CA shall ensure that physical access to critical services is controlled and physical risks to its assets minimized (see Directive 1999/93/EC [1] annex II (f)). In particular: a) Physical access to facilities concerned with certificate generation, subject device preparation, and revocation management services shall be limited to properly authorized individuals. b) Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities; and c) Controls shall be implemented to avoid compromise or theft of information and information processing facilities. d) The facilities concerned with certificate generation, subject device preparation (see 7.2.9) and revocation management shall be operated in an environment which physically protects the services from compromise through unauthorized access to systems or data. e) Any persons entering this physically secure area shall not be left for any significant period without oversight by an authorized person. f) Physical protection shall be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the certificate generation, subject device preparation (see 7.2.9) and revocation management services. Any parts of the premises shared with other organizations shall be outside this perimeter. g) Physical and environmental security controls shall be implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. The CA's physical and environmental security policy for systems concerned with certificate generation, subject device preparation (see 7.2.9) and revocation management services shall address the physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking and entering, and disaster recovery, etc. h) Controls shall be implemented to protect against equipment, information, media and software relating to the CA services being taken off-site without authorization.

Table No.	CP reference	Mapping Clause
	FBCA CP section 5.1	The FBCA and Entity CAs shall impose physical security requirements that provide similar levels of protection as those specified below. All the physical control requirements apply equally to the FBCA and Entity CAs. **Site Location & Construction** The location and construction of the facility housing the FBCA and Entity CA equipment shall be consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the FBCA and Entity CA equipment and records. **Physical Access for CA Equipment** The FBCA and Entity CA equipment shall always be protected from unauthorized access. The security mechanisms shall be commensurate with the level of threat in the equipment environment. Since the FBCA must plan to issue certificates at all levels of assurance, it shall be operated and controlled on the presumption that it will be issuing at least one High Assurance certificate. The physical security requirements pertaining to CAs that issue Basic Assurance certificates are: • Ensure no unauthorized access to the hardware is permitted • Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers In addition to those requirements, the following requirements shall apply to CAs that issue Medium, Medium Hardware, or High assurance certificates: • Ensure manual or electronic monitoring for unauthorized intrusion at all times • Ensure an access log is maintained and inspected periodically • Require two person physical access control to both the cryptographic module and computer system A security check of the facility housing the FBCA or Entity CA equipment (operating at the Basic Assurance level or higher) shall occur if the facility is to be left unattended. …… **Physical Access for RA Equipment** RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment. ……. **Media Storage** FBCA and Entity CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). **Waste Disposal** Sensitive waste material shall be disposed of in a secure fashion.
Overall Match: COMPARABLE		
27	QCP clause 7.4.5	**Operations management** The CA shall ensure that the CA systems are secure and correctly operated, with minimal risk of failure (see the Directive [1], annex II (e)). In particular:
	QCP clause 7.4.5 a)	a) The integrity of CA systems and information shall be protected against viruses, malicious and unauthorized software.
	FBCA CP section 6.6.1	• Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Hardware and software shall be scanned for malicious code on first use and periodically thereafter.
	Match: Equivalent	
	QCP clause 7.4.5 b)	b) Damage from security incidents and malfunctions shall be minimized through the use of incident reporting and response procedures.

Table No.	CP reference	Mapping Clause
	FBCA CP section 5.4.2	Audit logs shall be reviewed in accordance to the table below. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented. For the FBCA, the FPKI Operational Authority shall explain all significant events in an audit log summary. .. Medium (all policies): At least once every two months. Statistically significant set of security audit data generated by Entity CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity
	FBCA CP section 5.4.8	FBCA personnel shall routinely assess whether the CA system or its components have been attacked or breached. For Entity CAs, personnel shall perform routine assessments for evidence of malicious activity.
	Match: Comparable	
	QCP clause 7.4.5 c)	c) Media used within the CA shall be securely handled to protect media from damage, theft and unauthorized access.
	FBCA CP section 5.1.2.1	Removable cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive CA equipment shall be placed in secure containers when not in use. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.
	FBCA CP section 5.1.6	FBCA and Entity CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic).
	Match: Equivalent	
	QCP clause 7.4.5 d)	d) Media management procedures shall protect against obsolescence and deterioration of media within the period of time that records are required to be retained.
	FBCA CP section 5.5.3	If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Alternatively, an Entity may retain data using whatever procedures have been approved by NARA for that category of documents. Applications required to process the archive data shall also be maintained for a period determined by the Federal PKI Policy Authority for the FBCA (or Entity for the Entity CA).
	Match: Equivalent	
	QCP clause 7.4.5 e)	e) Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of certification services.
	FBCA CP section 5.2.1	*This section provides requirements on the procedures for trusted roles.*
	Match: Exceeded	
	QCP clause 7.4.5 f)	**Media handling and security** f) All media shall be handled securely in accordance with requirements of the information classification scheme (see clause 7.4.2). Media containing sensitive data shall be securely disposed of when no longer required.
	FBCA CP section 5.1.2.1	Removable cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive CA equipment shall be placed in secure containers when not in use. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

Table No.	CP reference	Mapping Clause
	FBCA CP section 5.1.6	FBCA and Entity CA media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic).
	FBCA CP section 5.1.7	Sensitive waste material shall be disposed of in a secure fashion.
	FBCA CP section 5.5.3	No unauthorized user shall be permitted to write to or delete the archive. For the FBCA, archived records may be moved to another medium when authorized by the FPKI Operational Authority Administrator. Archive media shall be stored in a safe, secure storage facility separate from the FBCA or Entity CA itself.
	FBCA CP section 6.2.4	*This section describes requirements on procedures for handling CA key including their destruction*
	Match: Comparable	Comment: FBCA Identifies requirements for handling different types of data even though these is no formal classification scheme.
	QCP clause 7.4.5 g)	**System Planning** g) Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.
	FBCA CP section 4.8.4	The FBCA directory system shall be deployed so as to provide 24 hour, 365 day per year availability. The FBCA Operational Authority shall implement features to provide high levels of directory reliability.
	Match: Point of Note	*Whilst there is no specific FBCA requirement in this area, requirements to provide 24/7for critical directory and revocation services within 18 hours implies capacity planning is necessary.* The FBCA does not directly address issues relating to levels of service to the subscribers and relying party where this does not effect the security of the certificate. (e.g. no requirement to make subscriber aware of change of revocation status).
	QCP clause 7.4.5 h)	**Incident reporting and response** h) The CA shall act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security. All incidents shall be reported as soon as possible after the incident.
	FBCA CP section 5.4.2	Audit logs shall be reviewed in accordance to the table below. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented. For the FBCA, the FPKI Operational Authority shall explain all significant events in an audit log summary. .. Medium (all policies): At least once every two months. Statistically significant set of security audit data generated by Entity CAs since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity
	FBCA CP section 5.4.8	FBCA personnel shall routinely assess whether the CA system or its components have been attacked or breached. For Entity CAs, personnel shall perform routine assessments for evidence of malicious activity.
	FBCA CP section 5.7.1	The members of the Federal PKI Policy Authority shall be notified if any of the following cases occur: • suspected or detected compromise of the FBCA systems; • physical or electronic attempts to penetrate FBCA systems; • denial of service attacks on FBCA components; • any incident preventing the FBCA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

Table No.	CP reference	Mapping Clause
	FBCA MoA *D7*	By entering into this agreement, the Entity [CA] agrees that it will do the following: Promptly advise the FBCA Operational Authority and the Federal PKI Policy Authority (1) in the event of any material problem or inability to operate the Principal CA in accordance with the Entity Principal CA CP or Supplemental Requirements, or (2) in the event that the Entity becomes aware of a material non-compliance on the part of any other party that is within the name constraints in the cross-certificate issued by the FBCA and that interoperates with the Principal CA or (3) in the event that the Entity takes any action to terminate or limit such other party's interoperability with the FBCA.
	Match: **Point of Note**	FBCA require review of logs at least two months but it is unclear what specific measures are available to enable "timely response to incidents".
	QCP clause 7.4.5 i)	i) Audit processes, meeting requirements specified in section 7.4.11, shall be invoked at system startup, and cease only at system shutdown.
	FBCA CP section 5.4.6	…. Automated audit processes shall be invoked at system or application startup, and cease only at system or application shutdown. …..
	Match: **Equivalent**	
	QCP clause 7.4.5 j)	j) Audit logs shall be monitored or reviewed regularly to identify evidence of malicious activity.
	FBCA CP section 5.4.2	Audit logs shall be reviewed in accordance to the table below. Such reviews involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented. For the FBCA, the FPKI Operational Authority shall explain all significant events in an audit log summary. .. Medium (all policies): At least once every two months. …
	Match **equivalent**	
	QCP clause 7.4.5 k)	**Operations procedures and responsibilities** k) CA security operations shall be separated from normal operations.
	FBCA CP section 5.2.1	A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the FBCA or an Entity CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.
	FBCA CP section 5.1.1	**Site Location & Construction** … The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to the FBCA and Entity CA equipment and records. **Physical Access for CA Equipment** The FBCA and Entity CA equipment shall always be protected from unauthorized access.
	Match **Comparable**	

Table No.	CP reference	Mapping Clause
Overall Match: COMPARABLE POINT OF NOTE		See 7.4.5 g, h) above
28	QCP clause 7.4.6 a)	**System Access Management** The CA shall ensure that CA system access is limited to properly authorized individuals (see [1], annex II (f)). In particular: a) Controls (e.g. firewalls) shall be implemented to protect the CA's internal network domains from external network domains accessible by third parties.
	FBCA CP section 6.7	Network security controls shall be employed to protect the FBCA and the FBCA Internal Directory. Networking equipment shall turn off unused network ports and services. Any network software installed on the FBCA equipment shall be necessary to the functioning of the FBCA. The FBCA Border Directory shall be connected to the Internet and provide continuous service (except, when necessary, for brief periods of maintenance or backup). Any boundary control devices used to protect the Border directory or FBCA local area network shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network. Entity CAs and directories shall employ appropriate network security controls. Networking equipment shall turn off unused network ports and services. Any network software present shall be necessary to the functioning of the equipment.
	Match Equivalent	
	QCP clause 7.4.6 b)	b) Sensitive data shall be protected against unauthorized access or modification. Sensitive data shall be protected (e.g. using encryption and an integrity mechanism) when exchanged over networks which are not secure.
	FBCA CP 5.1.2.1	**Physical Access for CA Equipment** The FBCA and Entity CA equipment shall always be protected from unauthorized access.
	FBCA CP section 5.2	**Identification and Authentication for Each Role** At all assurance levels other than Rudimentary, an individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity. **Separation of Roles** Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or by both means.
	FBCA CP section 6.7	[As above]
	Match Comparable	
	QCP clause 7.4.6 c)	c) The CA shall ensure effective administration of user (this includes operators, administrators and any users given direct access to the system) access to maintain system security, including user account management, auditing and timely modification or removal of access.
	FBCA CP section 6.5.1	For Entity CAs, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The Entity CA and its ancillary parts shall include the following functionality: • authenticate the identity of users before permitting access to the system or applications; • manage privileges of users to limit users to their assigned roles; • generate and archive audit records for all transactions; (see Section 5.4) • enforce domain integrity boundaries for security critical processes; and • support recovery from key or system failure.
	Match Equivalent	

Table No.	CP reference	Mapping Clause
	QCP clause 7.4.6 d)	The CA shall ensure access to information and application system functions are restricted in accordance with the access control policy and that the CA system provides sufficient computer security controls for the separation of trusted roles identified in CA's practices, including the separation of security administrator and operation functions. Particularly, use of system utility programs shall be restricted and tightly controlled. Access shall be restricted only allowing access to resources as necessary for carrying out the role(s) allocated to a user.
	FBCA CP section 6.5.1	[As above]
	Match Equivalent	
	QCP clause 7.4.6 e)	e) CA personnel shall be successfully identified and authenticated before using critical applications related to certificate management.
	FBCA CP section 6.5.1	• … • Require identification and authentication of PKI roles and associated identities
	Match Equivalent	
	QCP clause 7.4.6 f)	f) CA personnel shall be accountable for their activities, for example by retaining event logs (see clause 7.4.11).
	FBCA CP section 6.5.1	• Archive FBCA history and audit data
	FBCA CP section 5.3.1	**Background, Qualifications, Experience, & Security Clearance Requirements** Each Entity shall identify at least one individual or group responsible and accountable for the operation of each CA in that Entity.
	Match Equivalent	
	QCP clause 7.4.6 g)	g) Sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) being accessible to unauthorized users.
	FBCA CP section 6.5.1	For the FBCA, the computer security functions listed below are required. • Prohibit object re-use or require separation for FBCA random access memory
	Match Comparable	Whilst object re-use is not specifically mentioned for Entity CAs: 1. There are a number of provisions about access authentication that prevent unauthorized users to access assets and data when inside the CA premises. 2. there are specific provisions on securely dispose of sensible waste 3. there are specific provisions on how to handle the cryptographic material.
	QCP clause 7.4.6 h)	h) The CA shall ensure that local network components (e.g. routers) are kept in a physically secure environment and their configurations periodically audited for compliance with the requirements specified by the CA.
	FBCA CP section 5.1.2.1	**Physical Access for CA Equipment** The FBCA and Entity CA equipment shall always be protected from unauthorized access.
	Match Comparable	Whilst CA networking equipment is not specifically mentioned it is considered reasonable that this is included in the FBCA requirement.
	QCP clause 7.4.6 i) & k)	Certificate generation (i) Revocation management (k) Continuous monitoring and alarm facilities shall be provided to enable the CA to detect, register and react in a timely manner upon any unauthorized and/or irregular attempts to access its resources.
	FBCA CP section 5.1.2.1	……. In addition to those requirements, the following requirements shall apply to CAs that issue Medium, Medium Hardware, or High assurance certificates: • Ensure manual or electronic monitoring for unauthorized intrusion at all times
	FBCA CP section 6.6.2	There shall be a mechanism for detecting unauthorized modification to the FBCA or Entity CA software or configuration.
	Match Comparable	

Table No.	CP reference	Mapping Clause
	QCP clause 7.4.6	j) Dissemination application shall enforce access control on attempts to add or delete certificates and modify other associated information.
	FBCA CP section 2.4	The FPKI Operational Authority shall protect any repository information not intended for public dissemination or modification. Certificates and certificate status information in the FBCA repository shall be publicly available through the Internet. Access to information in Entity CA repositories shall be determined by the Entity pursuant to the rules and statutes that apply to that entity. Certificates and certificate status information in the Entity repository should be publicly available through the Internet wherever reasonable. At a minimum, the Entity repositories shall make CA certificates and CRLs issued by the Entity PKI and CA certificates issued to the Entity PKI available to Federal Relying Parties.
	Match Comparable	
	QCP clause 7.4.6 l)	l) Revocation status application shall enforce access control on attempts to modify revocation status information.
	FBCA CP section 2.4	[As above]
	Match Comparable	
Overall Match: COMPARABLE		7.4.6.i & k) It assumed that protection against denial of service and intrusion attacks requires some form of monitoring and alarm facilities.
29	QCP clause 7.4.7	**Trustworthy Systems Deployment and Maintenance** The CA shall use trustworthy systems and products that are protected against modification (see the Directive [1], annex II (f)). a) An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the CA or on behalf of the CA to ensure that security is built into IT systems. b) Change control procedures exist for releases, modifications and emergency software fixes for any operational software.
	FBCA CP section 6.6.1	The System Development Controls for the FBCA and Entity CAs at the Basic Assurance level and above are as follows: • For commercial off-the-shelf software, the software shall be designed and developed under a formal, documented development methodology. • For hardware and software developed specifically for a particular CA, the applicant shall demonstrate that security requirements were achieved through a combination of software verification & validation, structured development approach, and controlled development environment. • Where open source software has been utilized, the applicant shall demonstrate that security requirements were achieved through software verification & validation and structured development/life-cycle management. • Hardware and software procured to operate the CA shall be purchased and shipped in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase). • The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the CA operation. • Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Hardware and software shall be scanned for malicious code on first use and periodically thereafter. • Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.
	FBCA CP section 6.6.2	The configuration of the FBCA or Entity CA system as well as any modifications and upgrades shall be documented and controlled. ….

Table No.	CP reference	Mapping Clause
Overall Match: EQUIVALENT		
30	QCP clause 7.4.8	**Business continuity management and incident handling** The CA shall ensure in the event of a disaster, including compromise of the CA's private signing key, operations are restored as soon as possible (see the Directive [1], annex II (a)). In particular: a) The CA must define and maintain a continuity plan to enact in case of a disaster. **CA systems data back up and recovery** b) CA systems data necessary to resume CA operations shall be backed up and stored in safe places suitable to allow the CA to timely go back to operations in case of incident / disasters. c) Back-up and restore functions shall be performed by the relevant trusted roles specified in section 7.4.3. **CA key compromise** d) The CA's business continuity plan (or disaster recovery plan) shall address the compromise or suspected compromise of a CA's private signing key as a disaster. e) In the case of compromise the CA shall as a minimum provide the following undertakings: - Inform the following of the compromise: all subscribers and other entities with which the CA has agreements or other form of established relations, among which relying parties and CAs. In addition, this information shall be made available to other relying parties. - indicate that certificates and revocation status information issued using this CA key may no longer be valid. **Algorithm compromise** f) Should any of the algorithms, or associated parameters, used by the CA or its subscribers become insufficient for its remaining intended usage then he CA shall: - Inform all subscribers and relying parties with which the CA has agreement or other form of established relations. In addition, this information shall be made available to other relying parties. - revoke any affected certificate.
	FBCA CP section 5.7.4	The FBCA directory system shall be deployed so as to provide 24 hour, 365 day per year availability. The FPKI Operational Authority shall implement features to provide high levels of directory reliability. The FPKI Operational Authority shall operate a hot backup site, whose purpose is to ensure continuity of operations in the event of failure of the primary site. The FBCA operations shall be designed to restore full service within six (6) hours of primary system failure. The FPKI Operational Authority or Entity Principal CA shall at the earliest feasible time securely advise the Federal PKI Policy Authority and all of its member entities in the event of a disaster where the FBCA or Entity Principal CA installation is physically damaged and all copies of the FBCA or Entity Principal CA signature keys are destroyed.
	FBCA CP section 5.1.8	For the FBCA and Entity CAs operating at the Basic Assurance level or higher, full system backups sufficient to recover from system failure shall be made on a periodic schedule. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy shall be stored at an off-site location separate from the FBCA or Entity CA equipment. Only the latest full backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational FBCA or Entity CA.

Table No.	CP reference	Mapping Clause
	FBCAv2 clause 5.7.3	If the FBCA or Entity CA signature keys are compromised or lost (such that compromise is possible even though not certain): • The Federal PKI Policy Authority and all of its member entities shall be notified so that entities may issue CRLs revoking any cross-certificates issued to the compromised CA; • A new FBCA or Entity CA key pair shall be generated by the FBCA or Entity CA in accordance with procedures set forth in the FBCA or Entity CPS; and • New FBCA or Entity CA certificates shall be issued to Entities also in accordance with the FBCA or Entity CPS. The FPKI Operational Authority or Entity CA governing body shall also investigate and report to the Federal PKI Policy Authority what caused the compromise or loss, and what measures have been taken to preclude recurrence.
Overall Match: COMPARABLE		In the case of compromise or weakness found in the cryptographic algorithm employed the Federal PKI will update it's policy (see Annex A).
31	QCP clause 7.4.9	**CA Termination** The CA shall ensure that potential disruptions to subscribers and relying parties are minimized as a result of the cessation of the CA's services as covered by the certificate policy, and ensure continued maintenance of records required to provide evidence of certification for the purposes of legal proceedings (see the Directive [1], annex II (i)). In particular: a) Before the CA terminates its services the following procedures shall be executed as a minimum: - the CA shall inform the following of the termination: all subscribers and other entities with which the CA has agreements or other form of established relations, among which relying parties and CAs. In addition, this information shall be made available to other relying parties. - the CA shall terminate all authorization of subcontractors to act on behalf of the CA in the performance of any functions related to the process of issuing certificates; - the CA shall perform necessary undertakings to transfer obligations for maintaining registration information (see clause 7.3.1), and event log archives, including revocation status information, (see clause 7.4.11) for their respective period of time as indicated to the subscriber and relying party (see clause 7.3.4); - the CA shall destroy, or withdraw from use, its private keys, as defined in clause 7.2.6. b) The CA shall have an arrangement to cover the costs to fulfil these minimum requirements in case the CA becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy. c) The CA shall state in its practices the provisions made for termination of service. This shall include: - the notification of affected entities; - the transfer of its obligations to other parties; - the handling of the revocation status for unexpired certificates that have been issued.
	FBCA CP section 5.8	In the event of termination of the FBCA operation, certificates signed by the FBCA shall be revoked and the Federal PKI Policy Authority shall advise entities that have entered into MOAs with the Federal PKI Policy Authority that FBCA operation has terminated so they may revoke certificates they have issued to the FBCA. Prior to FBCA termination, the FPKI Operational Authority shall provide all archived data to an archival facility. Entities will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will be sought in the event the FBCA is terminated. In the event that an Entity CA terminates operation, the Entity shall provide notice to the FBCA prior to termination.

Table No.	CP reference	Mapping Clause
Overall Match: POINT OF NOTE		The FBCA current does not include requirements for maintaining revocation information on CA termination. It is assumed that Federal PKI users will maintain the information on the status of a certificates used for signing. The Federal PKI will investigate further requirements regarding termination of CA.
32	QCP clause 7.4.10	**Compliance with Legal Requirement** The CA shall ensure compliance with legal requirements (see the Directive [1], article 8). In particular: a) CA shall ensure it meets all applicable statutory requirements (including requirements of the Data Protection Directive [4] – see next item) for protecting records from loss, destruction and falsification. Some records may need to be securely retained to meet statutory requirements, as well as to support essential business activities (see clause 7.4.11). b) The CA shall ensure that the requirements of the European data protection Directive [4], as implemented through national legislation, are met. c) Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. d) The information that users contribute to the CA shall be completely protected from disclosure without the user's agreement, a court order or other legal authorization.
	FBCA section 9.4	**9.4.1 Privacy Plan** The FPKI Operational Authority shall conduct a Privacy Impact Assessment. If deemed necessary, the FPKI Operational Authority shall have a Privacy Plan to protect personally identifying information from unauthorized disclosure. The Federal PKI Policy Authority shall approve the Privacy Plan. For Entity CAs, no stipulation. **9.4.2 Information treated as Private** The FBCA shall protect all subscriber personally identifying information from unauthorized disclosure. The FBCA shall also protect personally identifying information for Entity personnel collected to support cross-certification and MOA requirements from unauthorized disclosure. For Entity CAs, no stipulation. **9.4.3 Information not deemed Private** Information included in FBCA certificates is not subject to protections outlined in Section 9.4.2. **9.4.3 Responsibility to Protect Private Information** Sensitive information must be stored securely, and may be released only in accordance with other stipulations in Section 9.4. **9.4.4 Notice and Consent to use Private Information** The FPKI Operational Authority is not required to provide any notice or obtain the consent of the Subscriber or Entity personnel in order to release private information in accordance with the stipulations of Section 9.4. **9.4.5 Disclosure Pursuant to Judicial/Administrative Process** The FPKI Operational Authority shall not disclose private information to any third party unless authorized by this Policy, required by law, government rule or regulation, or order of a court of competent jurisdiction. Any request for release of information shall be processed according to 41 CFR 105-60.605.

Table No.	CP reference	Mapping Clause
Overall Match: COMPARABLE POINT OF NOTE		EU Data Protection Legislation not applicable to US. However, it is not considered necessary to exchange personal information other than that held in certificates for interoperability.
33	QCP clause 7.4.11 a-g)	**Recording of Information Concerning Qualified Certificates** The CA shall ensure that all relevant information concerning a qualified certificate is recorded for an appropriate period of time, in particular for the purpose of providing evidence of certification for the purposes of legal proceedings (see the Directive [1], annex II (i)). In particular: a) The confidentiality and integrity of current and archived records concerning qualified certificates shall be maintained. b) Records concerning qualified certificates shall be completely and confidentially archived in accordance with disclosed business practices. c) Records concerning qualified certificates shall be made available if required for the purposes of providing evidence of certification for the purpose of legal proceedings. The subject, and within the constraints of data protection requirements (see clause 7.4.10) the subscriber, shall have access to registration and other information relating to the subject. d) The precise time of significant CA environmental, key management and certificate management events shall be recorded. e) Records concerning qualified certificates shall be held for a period of time as appropriate for providing necessary legal evidence in support of electronic signatures in accordance with applicable legislation. f) The events shall be logged in a way that they cannot be easily deleted or destroyed (except for transfer to long term media) within the period of time that they are required to be held. g) The specific events and data to be logged shall be documented by the CA.

Table No.	CP reference	Mapping Clause
	FBCA CP section 5.5	**5.5.2 Retention Period for Archive** The minimum retention periods for archive data are identified below. Executive branch agencies must follow either the General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable. All other entities shall comply with their respective records retention policies in accordance with whatever laws apply to those entities. Medium (all policies): 10 Years & 6 Months. **5.5.3 Protection of Archive** No unauthorized user shall be permitted to write to or delete the archive. For the FBCA, archived records may be moved to another medium when authorized by the FPKI Operational Authority Administrator. Archive media shall be stored in a safe, secure storage facility separate from the FBCA or Entity CA itself. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. Alternatively, an Entity may retain data using whatever procedures have been approved by NARA for that category of documents. Applications required to process the archive data shall also be maintained for a period determined by the Federal PKI Policy Authority for the FBCA (or Entity for the Entity CA). Prior to the end of the archive retention period, the FPKI Operational Authority shall provide archived data and the applications necessary to read the archives to a Federal PKI Policy Authority approved archival facility, which shall retain the applications necessary to read this archived data. **5.5.4 Archive Backup Procedures** The CPS or a referenced document shall describe how archive records are backed up, and how the archive backups are managed. **5.5.5 Requirements for Time-Stamping of Records** CA archive records shall be automatically time-stamped as they are created. The CPS shall describe how system clocks used for time-stamping are maintained in synchrony with an authoritative time standard. **5.5.6 Archive Collection System (internal or external)** No stipulation. **5.5.7 Procedures to Obtain & Verify Archive Information** Procedures detailing how to create, verify, package, transmit, and store archive information shall be published in the applicable CP or CPS. The contents of the archive shall not be released except as determined by the Federal PKI Policy Authority for the FBCA (or Entity for the Entity CA) or as required by law. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents.

Table No.	CP reference	Mapping Clause
	Match: Comparable	
	QCP clause 7.4.11 h - o)	h) The CA shall ensure all events relating to registration including requests for certificate re-key or renewal, are logged. i) The CA shall ensure that all registration information including the following is recorded: - type of document(s) presented by the applicant to support registration; - record of unique identification data, numbers, or a combination thereof (e.g. applicant's drivers license number) of identification documents, if applicable; - storage location of copies of applications and identification documents, including the signed subscriber agreement (see clause 7.3.1 h)); - any specific choices in the subscriber agreement (e.g. consent to publication of certificate) see 7.3.1 i); - identity of entity accepting the application; - method used to validate identification documents, if any; - name of receiving CA and/or submitting Registration Authority, if applicable. j) The CA shall ensure that privacy of subject information is maintained. k) The CA shall log all events relating to the life-cycle of CA keys. l) The CA shall log all events relating to the life-cycle of certificates. m) The CA shall log all events relating to the life cycle of keys managed by the CA, including any subject keys generated by the CA. n) If applicable, the CA shall log all events relating to the preparation of SSCDs. o) The CA shall ensure that all requests and reports relating to revocation, as well as the resulting action, are logged.
	FBCA CP section 4.6.2	A message from any source received by the FBCA or Entity CA requesting an action related to the operational state of the CA is an auditable event. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event): • The type of event, • The date and time the event occurred, • A success or failure indicator, where appropriate • The identity of the entity and/or operator (of the FBCA or Entity CA) that caused the event, Detailed audit requirements are listed in the table below according to the level of assurance. The FBCA shall record the events identified in the table for High Assurance. All security auditing capabilities of the FBCA or Entity CA operating system and CA applications required by this CP shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. Where events cannot be automatically recorded, the CA shall implement manual procedures to satisfy this requirement. [Table listing auditable events]
Overall Match: COMPARABLE		
34	QCP clause 7.5 a-b)	**Organizational** The CA shall ensure that its organization is reliable (see Directive [1], annex II (a)). In particular that: a) Policies and procedures under which the CA operates shall be non-discriminatory. b) The CA shall make its services accessible to all applicants whose activities fall within its declared field of operation.
	FBCA CP section 1.1.5	The FBCA will extend interoperability with non-federal entities only when it is beneficial to the federal government.
	Match comparable	US legislation required by law to not discriminate on racial, gender or national origin. US Government employees required by law to act ethically.
	QCP clause 7.5 c)	c) The CA is a legal entity according to national law.

Table No.	CP reference	Mapping Clause
	FBCA Cross Cert Criteria [6]	3. If the Applicant PKI is an organization not governed by the Federal Information Processing Standards (FIPS) (i.e., a non-Federal Applicant PKI), it may be asked to provide additional information, such as but not limited to the following: a. Evidence of the current legal status of the organization operating the PKI; b. ...
	FBCA CP section 1.3.1.1	The Federal CIO Council comprises the Chief Information Officers of all cabinet level departments and other independent agencies. The Federal CIO Council has established the framework for the interoperable FPKI, and that includes overseeing the operation of the organizations responsible for governing and promoting its use. In particular, this CP is established under the authority of and with the approval of the Federal CIO Council.
	FBCA CP section 1.3.1.2	The Federal PKI Policy Authority is a group of U.S. Federal Government Agencies (including cabinet-level Departments) established pursuant to the Federal CIO Council. The FPKIPA owns this policy and represents the interest of the Federal CIOs. The Federal PKI Policy Authority is responsible for:
	FBCA CP section 9.6.1	A non-federal entity must determine whether that entity's certificate policy meets its legal and policy requirements. Review of a non-federal entity's certificate policy by the Federal PKI Policy Authority is not a substitute for due care and mapping of certificate policies by the non-federal entity.
	Match Comparable	
	QCP clause 7.5 d)	d) The CA has adequate arrangements to cover liabilities arising from its operations and/or activities.
	Match: Point of Note	Specific legal advise should be sought regarding liability under article 6 of the EU Directive 1 and US commercial and governmental liability.
	QCP clause 7.5 e)	e) The CA has the financial stability and resources required to operate in conformity with this policy.
	FBCA Cross Cert Criteria [6]	4. If the Applicant PKI is an organization not governed by the Federal Information Processing Standards (FIPS) (i.e., a non-Federal Applicant PKI), it may be asked to provide additional information, such as but not limited to the following: c. Evidence of the current legal status of the organization operating the PKI; d. Evidence of the financial capacity of the organization operating the PKI (such as bonds, letters of credit, insurance demonstrating the organization's ability to meet the financial responsibilities associated with operating a PKI)

Table No.	CP reference	Mapping Clause
	FBCA Cross Cert Criteria [6]	Part Two: Criteria for Cross Certification General Principles 1. Initiation Phase ….. External applicants, unless otherwise exempted, must provide evidence of the current legal status of the entity responsible for the PKI. A certificate from the authorities of the jurisdiction in which the organization was created, indicating that the organization is in good standing under the laws of that jurisdiction, may be requested for this purpose. Non-governmental applicants may be requested to provide evidence of financial capacity to manage risks associated with the operation of a PKI. Financial capacity can be demonstrated if the organization can provide a copy of a performance bond, a letter of credit from a financial institution, a letter indicating that insurance has been put in place, or a commitment letter from a bonding company, financial institution or insurance company. The purpose of this requirement is to demonstrate the organization's ability to meet any financial responsibility associated with operating a Certification Authority, including any liability to subscribers or others relying on certificates issued and digital signatures verifiable by reference to public keys in such certificates. The nature and sufficiency of the required financial capacity will be determined at the discretion of the Policy Authority on a case-by-case basis. Legal status and financial capacity constitute some of the evidentiary requirements needed to lay a foundation of trust between the US Government and applicants. Applicants exempted from these evidentiary requirements are: a. A US Federal entity; b. A state, local, or tribal government; c. A foreign state or government; or d. Any other entity exempted from this requirement by the FPKI Policy Authority. A Request will not be considered complete until the FPKI Policy Authority is satisfied that all relevant documentation, as set out in the requirements, has been submitted.
	FBCA section 1.3.1.2	The Federal PKI Policy Authority is a group of U.S. Federal Government Agencies
	Match comparable	Backed by US government.
	QCP clause 7.5 f)	f) The CA has policies and procedures for the resolution of complaints and disputes received from customers or other parties about the provisioning of electronic trust services or any other related matters.
	FBCA CP section 9.13	**Dispute Resolution Provisions** Any dispute arising with respect to this policy or certificates issued under this policy shall be resolved by the Parties. **Governing Law** Where an inter-governmental dispute occurs, resolution will be according to the terms of the MOA. For Entity CAs, the construction, validity, performance and effect of certificates issued under the Entity CP for all purposes shall be governed by law (statute, case law or regulation) under which the Entity operates.
	Match comparable	
	QCP clause 7.5 g)	g) The CA has a properly documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.
	FBCA section 1.3.1.2	…. The FPKIPA will execute a Memorandum of Agreement (MOA) with each cross-certified Entity setting forth the respective responsibilities and obligations of both parties and the mappings between the certificate levels of assurance contained in this CP and those in the Entity CP. (When the entity belongs to a sovereign nation, the United States Department of State may execute the MOA or delegate the authority to execute the MOA on its behalf.)

Table No.	CP reference	Mapping Clause
	Match Equivalent	
	QCP clause 7.5 h,i)	h) The parts of the CA concerned with certificate generation and revocation management shall be independent of other organizations for its decisions relating to the establishing, provisioning and maintaining and suspending of services; in particular its senior executive, senior staff and staff in trusted roles, must be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides. i) The parts of the CA concerned with certificate generation and revocation management shall have a documented structure which safeguards impartiality of operations.
	FBCA CP section 5.2.1	A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust for all uses of the FBCA or an Entity CA. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.
	Match: Comparable	Whilst no specific requirement of independence of operations requirements on separation of duties and trusted roles is considered to provide comparable protection.
Overall Match: COMPARABLE		See h) above

Annex A:
Memo from chair, U.S. Federal PKI Policy Authority

MEMORANDUM

Date: November 25, 2005

TO: Riccardo Genghini, Chair
ETSI TC ES1

From: Chair, U.S. Federal PKI Policy Authority

Subject: Algorithm Compromise

In the event that an algorithm or associated parameters in use by the U.S. Federal Public Key Infrastructure is compromised or becomes insufficient for its remaining intended usage, then the U.S. Federal PKI Policy Authority would immediately revise its Policy documents to remove the failed algorithm and require use of a new, secure algorithm and/or associated parameters.

The U.S. Federal PKI Policy Authority is able to make and enforce such policy decisions in real time. Should you have any questions concerning this subject, please feel free to contact me at: altermap@mail.nih.gov or by telephone at +01 301 252 8846.

Peter Alterman, Ph.D.

History

Document history		
V1.1.1	April 2006	Publication