CCEB Publication 1010

PKI Cross-Certification Between CCEB Nations

Version 1.0

CCEB PUB 1010
(PKI Cross-Certification between CCEB Nations)

CCEB Pub1010 prescribes the processes and procedures, X.509 Certificate Policy (RFC 3647) criteria and guidelines, and technical interoperability activities to be carried out by CCEB nations to achieve cross-certification through self-certification and assertion. CCEB nations are not expected to list all of the procedural controls outlined in this publication in their own Certificate Policy and PKI document sets but only assert that they will comply with the controls articulated in this document. The document has the following Framework:

Section	Content
1	Architecture Overview
2	Processes and Procedures
3	x.509 Certificate Policy Mapping Criteria and Guidance for Cross-Certification
4	Technical Interoperability Activities
5	Governance and Change Control of Pub 1010
6	Compliance (on national certification) and audit
A	References
B	Acronyms
C	Glossary

DOCUMENT HISTORY SHEET

Issue Number	Description of Major Changes	Date

Table of Contents

Table of Figures

1 ARCHITECTURE OVERVIEW

1.1 Introduction

1.1.1 Purpose

This section provides the long-term Public Key Infrastructure (PKI) interoperability architecture for the CCEB Allies as agreed at the February 2005 Canberra Collocated Meeting. The architecture enables interoperability through direct cross-certification of each National Defence PKI (NDPKI) in a mesh configuration.[1]

1.1.2 Audience

The audience for this section is expected to be the PKI management and engineering/technical staff involved in Defense[2] PKI Program Management Offices (PMOs) or Project Teams. The audience includes Government and industry personnel involved in the definition, design, and development of the NDPKIs. Familiarity with PKI concepts is assumed.[3]

1.1.3 Background

CCEB Nations exchange Military information and data under the Combined Joint Multilateral Master Military Information Exchange Memorandum of Understanding (CJM3IEM). A Combined Joint Military Information Exchange Annex (CJMIEA) adds Authenticated Services which can use but are not limited to one, or a combination of, the following: Validation of Internet Protocol (IP) domain name; Presentation of user name; Presentation of user name and password; Presentation of cryptographic credentials using Public Key Technology; and Presentation of biometric credentials. CJMIEA Authentication Services involves policies, processes, and technologies to support the exchange and validation of authentication credentials. One basis for this exchange and validation is strong digital identities for both individuals and devices from interoperable NDPKIs that support strong identity management regimes, common policies and technical implementations. To achieve the CCEB Management Plan task of establishing interoperable NDPKIs[4], the CCEB Executive Group (EG) has endorsed the PKI Task Force (TF) recommendation for a two phase interoperability approach:[5]

a. Short-term which supports Allied access to US Department of Defense (DoD) owned websites on Unclassified but Sensitive Internet Protocol Network

---

1 This decision was based on workshops and national submissions of 5-Eyes Military PKI Interoperability Papers.

2 The spelling Defence or Defense is interchangeable and is used throughout the document but the meaning is the same.

3 The Cramer Report provides an overview of PKI concepts.

4 CCEB Management Plan Task 2.5.2.

5 Allied Communication Publication (ACP) 145 describes a near term PKI specific solution for Military Message Handling Systems (MMHS).

(NIPRNET). The solution, as agreed at the September 2004 Washington CCEB Collocated Meeting, creates policies and procedures, through the use of a Trusted Agent (TA) regime, for defense personnel in CCEB nations to obtain PKI Certificates from the US DoD PKI system.

b. The long-term approach supports interoperable, authenticated military information and data exchange within the SECRET high environment or within a lower classification system-high environment between CCEB nations over approved networks using PKI technology.

1.1.4 Scope

The PKI Forum has identified three major interoperability areas[6]

a. Component Level Interoperability – Interactions between the components of a Nation's PKI system. Some of the commonalities for interactions include:

(1) Algorithms to authenticate entities and protect data exchanges;

(2) Protocols and message formats for certification requests and response, PKI Certificate status check, repository access, etc.; and,

(3) PKI Certificate formats.

b. Application Level Interoperability – Interactions between Public Key Enabled (PKE) peer applications, examples include Secure Multipurpose Internet Mail Extensions (S/MIME), Secure Sockets Layer (SSL), and Internet Protocol Security (IPSec) applications. Some of the commonalities for interactions include:

(1) PKI Certificate and status information;

(2) Cryptographic algorithms: hash, digital signature, content encryption, key encryption, key transport, etc.;

(3) Data encoding formats; and,

(4) Communication protocols.

c. Inter-Domain Interoperability – Interactions between different NDPKIs. Some of the commonalities for interactions include:

(1) Trust relationships / cross certification,

(2) Adherence to and enforcement of agreed certificate policies.

1.1.5 Interoperability Architecture

This publication will indicate how Domain Level Interoperability is to be achieved between CCEB nations in the defence context. It will not dictate to each Nation how it is to implement their NDPKI system; however, to achieve application layer interoperability, trust relationships, adherence to and enforcement of certificate policies some level of agreement will need to be reached on key internal policies, processes, and

[6] http://www.oasis-pki.org/pdfs/PKIInteroperabilityFramework.pdf

technology. Nor will it provide common Peer PKE application data encoding formats or communication protocols. The interoperability architecture is capable of supporting:

a. People and devices that are NDPKI Subscribers, Groups, Roles, and Sets are also supported and there may be either devices (e.g., servers in a farm for www.mod.uk) or people (e.g., Watch Officers for USS Iwo Jima);

b. Information and data exchange on interconnected networks classified secret and below; and,

c. Environments that are bandwidth enabled, such as multi-Mb links between static locations, and bandwidth impaired, for example in the maritime environment where links could be in the lower Kbs capacity.

1.1.6 Security Protocols

The following security protocols are enabled by this architecture, the implementation of these protocols is beyond the scope of this document:[7]

a. SSL/Transport Layer Security (TLS) (Client-Server applications).

b. S/MIME (Mail applications).

c. IPSec (Network applications).

1.1.7 Commissioning a PKI

This publication does not provide requirements for commissioning a PKI; the programs that require NDPKI services provide those requirements. The publication does not provide pros and cons of available interoperability options; this has already been articulated in various 5-Eyes Military PKI Interoperability Papers and discussed at length in CCEB PKI forums. Finally this publication is not intended to be a PKI tutorial.

1.1.8 Assumptions

a. It is assumed that National defence domains are protected by Nationally-approved mechanisms.

b. Security domains are protected by Nationally-approved mechanisms.

c. Peer PKE applications agree on data encoding formats and communication protocols.

d. PKE and PKI agree on PKI Certificate formats and status information protocols required to support PKE.

e. PKI Certificate formats are based on the Internet Engineering Task Force (IETF) Request for Comments (RFC) 3280 – *The Internet Certificate and CRL Profile*.

f. Certificate Policies (CPs) and Certification Practice Statements (CPSs) are based on the IETF RFC 3647.

[7] Other security protocols will be enabled as required.

g. OCSP is based on the IETF RFC 2560.

h. Cryptographic algorithms to be used in this architecture are agreed by the CCEB INFOSEC Working Group.

i. Each nation will have a Policy Management Authority (PMA) with responsibility to oversee the implementation and maintenance of the NDPKI.

1.2 Architecture

a. Each nation has or intends to independently implement its own Defence PKI to issue PKI Certificates to national defence Subscribers/entities. Also, each NDPKI has Certificate Authorities (CAs), Registration Authorities (RAs), Lightweight Directory Access Protocol (LDAP) directories, Directory Service Agent's (DSAs), repositories, and PKI Certificate status responders based on national policy and doctrine.

b. Subscribers, which are people, devices, and sets/groups, use PKI Certificates to digitally sign or encrypt communications that traverse networks, which can be both bandwidth-enabled and bandwidth-impaired and at potentially different security classifications.

c. Each nation also needs its Subscribers to communicate with Subscribers of other CCEB Nations. National defence Subscribers will use PKI Certificates issued by their NDPKI to digitally sign and encrypt communications for communication with other member/coalition nations.[8] Before these communications can occur a number of policy decisions and technical measures must be taken; all are addressed in the following paragraphs:[9]

(1) Nations must compare their Certificate Policies (CPs) against Section 3 of this publication and determine their level of equivalence.

(2) Nations must sign using their Defence Root CA certificate the Defence Root CA PKI Certificate of each nation they consider to have equivalent CPs under this publication – referred to as a 'cross-certificate.

(3) Where a Defence CA is part of the national government PKI hierarchy it is expected that cross-certification will take place at the highest Defence CA level and that cross-certification will occur at one point only between the two NDPKIs.

(4) Nations must make the required NDPKI certificates available to member/coalition nations.

(5) Nations must make the required NDPKI certificate status information available to member/coalition nations.

[8] There may be special cases that require PKI Certificates to be issued to non-national subscribers, such as Liaison Officers working in a Framework Nation Headquarters.

[9] PKE application interoperability is required but is assumed to be addressed by the applications wishing to intercommunicate.

(6) Nations must interconnect their communications and information systems networks, and this requires that border protection devices are configured to permit PKE application exchange (i.e., signed encrypted email).

1.2.1 PKI Component Interactions

Not all NDPKI components need to communicate with their counterparts in another nation's PKI. The following paragraphs (1.2.2 – 1.2.6) cover the interactions required between PKI components.

1.2.2 Highest Level Defence CAs

a. Each Highest Level Defence CA will exchange a cross-certificate with the Highest Level Defence CA of those other CCEB nations with which it cross-certifies and will publish corresponding Certificate Revocation Lists (CRLs). It is likely that the Highest Level Defence CAs will be Defence Root CAs and, as such, will be off-line CAs separated from networks via an air gap; however this will be a national defence implementation decision. The processes and procedures to be followed during the exchange of cross-certificates are to be agreed in advance by the participating NDPKI PMAs.

b. For cross-certificate issuance, it is a national decision whether an off-line process (i.e., sneaker net) or on-line process (i.e., repository protocols) is used.

c. For cross-certificate publication, it is a national decision whether an off-line process or an on-line process is used.

1.2.3 CAs

a. It is expected that each NDPKI will issue PKI Certificates to its NDPKI Subscribers. Under special circumstances a NDPKI may issue a PKI Certificate to Subscribers who belong to the defence organisation of another CCEB nation; this is often the case for liaison/exchange officers and where special arrangements are put in place such as the issue of US DoD PKI certificates to the members of CCEB nations.

b. Where a PMA has entered into a cross-relationship with the PMA of another CCEB nation as part of the cross-certification process, it shall notify to the PMA of that other CCEB nation any other such cross-relationships that it has.

c. Each national defence CA that has Subscribers that communicate with Subscribers of a PKI belonging to another CCEB nation must publish all the appropriate PKI certificate information necessary for checking and validation in a repository that is available to the other CCEB nation. It is a national decision whether to pre-generate CRLs that indicate the status of cross-certificate and CA PKI Certificates with Subscribers who communicate with the Subscribers of the other CCEB nations. It is also a NDPKI decision whether the CA status CRL that is published within the organisation is mirrored to the users in the other CCEB

nations or whether that CRL is partitioned in some way prior to publication to only include CAs that have Subscribers that communicate with CCEB users.

d. CRL publication is an off-line process or an on-line process.

e. The CA publishes directly to the border repository or the CA publishes the PKI Certificate locally/nationally and the repository system handles publication to the border repository.

1.2.4 Repository Servers

a. Repository servers hold national defence CA PKI Certificates, Subscribers PKI Certificates as applicable, and CRLs. For any Subscriber of a defence PKI that communicates externally to Subscribers in another CCEB nation, Certificate and CRL information necessary for validation of the subscriber certificate and all certificates chaining to the cross-certificate must be made available to the users of the other CCEB nations. It is a NDPKI decision:

(1) Which protocols are used to publish to national and border repositories.

(2) Whether border repositories should act as CRL Distribution Points (CDPs).

b. Border repositories must support access from relying parties using the Lightweight Directory Access Protocol (LDAP). By bi-lateral agreement, access to repository information may also be provided using Hypertext Transfer Protocol (HTTP). Revocation information may be made available via Online Certificate Status Protocol (OCSP).

1.2.5 Certificate Status Authority

The NDPKI may implement a Certificate Status Authority to operate one or more certificate status servers that provide PKI Certificate status information generally on NDPKI own Subscribers. For any subscriber of a defence PKI that communicates with the subscriber of another CCEB nation, the revocation status server information must be made available to that subscriber. It is an NDPKI decision whether direct or indirect access is provided to revocation status information. It is also a NDPKI decision whether Authority Information Access (AIA) pointers are provided through the border repository. Since a Certificate Status Authority provides an alternate means of publishing revocation information, it must be installed, operated and maintained at the same level of security as the CAs for which it provides revocation status.

1.2.6 Subscribers and Relying Parties

National defense Subscribers are served by their NDPKI. They will only need to interact with border repositories and revocation status responders.

1.3 CCEB Trust Model

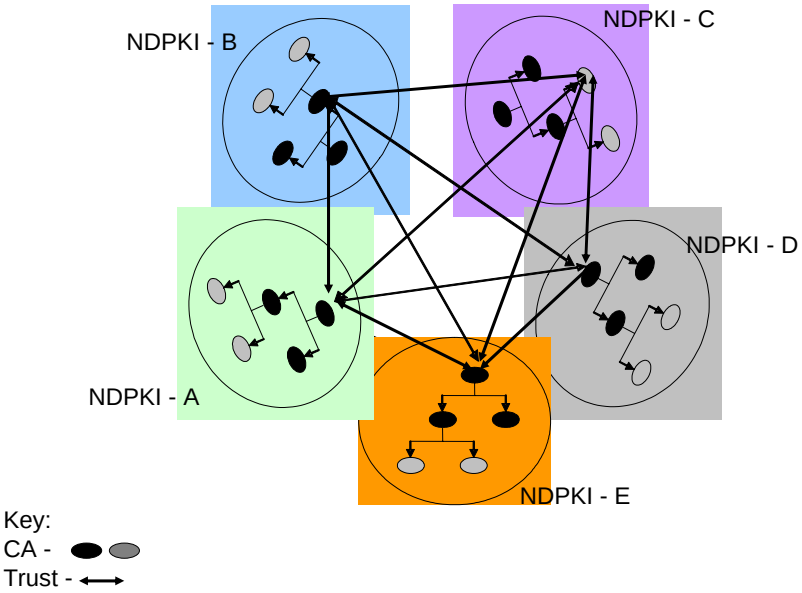

Figure 1. CCEB Trust Model.

The CCEB Trust Model shown at Figure 1 is based on NDPKIs cross-certifying at the Root and Subordinate CA level. Some nations may wish to authorize cross-certification at the subordinate CA level and this is permitted within the model.

2 PROCESS AND PROCEDURES

It will be the Defence PMA of each CCEB nations that will lead on the processes and procedures in each nation. The aim of this section is to articulate the high level processes and procedures needed to achieve and maintain cross certification within the CCEB construct.

2.1 ESTABLISH THE RELATIONSHIP

a. CCEB Nations are to agree then register their intent to establish a bi-lateral cross certification with the other members of the CCEB PKI Task Force.

b. National and CCEB stakeholders and dependencies are to be identified.

c. Each of the participating nations in the bi-lateral cross certification process is to formally self-assert (confirm their Compliance) against Section 3 of Pub 1010 (X.509 Certificate Policy Mapping Criteria and Guidance (CPMCG)). All members of the CCEB PKI Task Force are to be notified when self-assertion has been completed successfully.

d. PKI interoperability testing is to be carried out in accordance with Section 4 of Pub 1010 (Technical Interoperability Activities).

e. Each bi-lateral cross-certification is to be supported by a Cross-Certification Agreement. This agreement as minimum should document the results of the self-assertion by each nation against the Section 3 criteria; the bi-lateral resolution of non-conformance where a nation self-asserts with some caveats; identification of national POCs; agreements regarding incident response, maintenance and termination. The contents of the Cross-Certification Agreement will only become clear once nations start to engage in drawing up the Agreement.

f. Nations are to execute the bi-lateral cross-certification in accordance with their national procedures and notify other members of the CCEB PKI Task Force when completed successfully.

2.2 MAINTAIN THE RELATIONSHIP

a. Each nation in a bi-lateral agreement is to conduct self-assertion against Section 3 of Pub 1010 on an annual basis. Thereafter confirming with the other member nations of the CCEB PKI Task Force that the cross certification is still in place.

b. The frequency at which cross-certificates are to be renewed/replaced should be documented in the Cross-Certification Agreement and agreed on a bi-lateral basis.

c. CCEB nations that have bi-lateral cross-certification in place are to notify other nations of any changes to their PKI which impacts on the Cross-

Certification Agreement, such as cross-certification with the CA of another organisation or revocation of a subordinate CA.

d. CCEB nations involved in bi-lateral cross certification are to monitor and give notification of incidents that may impact on the ability to maintain the cross certification, such as the compromise of a CA.

e. At the time of carrying out the cross-certification process the nations involved are to designate and notify to the opposite nation a high level POC for incident response notification and handling.

f. At the time of carrying out the cross-certification process the nations involved are to designate and notify to the opposite nation a high level POC for operational problem resolution.

2.3 TERMINATION

a. Nations participating in a bi-lateral cross-certification are to give notification of termination of an agreement to CCEB nations and key stakeholders through their CCEB Principal.

b. Closure of the cross-certification and withdrawal of capability is to be conducted in a manner agreed by the participating nations and documented in the Cross-Certification Agreement (CCA).

3 X.509 CERTIFICATE POLICY MAPPING CRITERIA AND GUIDANCE FOR CROSS-CERTIFICATION

3.1 INTRODUCTION

a. This section of publication 1010 the CCEB CPMCG for cross-certification is consistent with the Internet Engineering Task Force Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Certificate Policy and Certification Practices Framework.

b. The purpose of the CPMCG is to identify appropriate criteria against which to assess NDPKI CPs, leading ultimately to an assertion of compliance with the criteria. The criteria are expressed in terms of minimum standards that should be met or exceeded by the policies of a NDPKI. Where it is clear that a criterion cannot be met for some reason, the two PMAs involved should reach an agreement on the treatment of the non-conforming policy areas and both the non-conforming policy areas and the agreement on treatment recorded within the CCA.

3.1.1 Overview

3.1.1.1 Certificate Policy (CP)

Certificates must contain at least one registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The OID corresponds to a specific level of assurance and (optionally) functionality specified in the CCA. The bi-lateral mapping of policy identifiers between two NDPKIs should be documented and be available to Relying Parties. Each certificate will assert the appropriate level of assurance using the X.509 *certificatePolicies* extension.

3.1.1.2 Relationship between the CPMCG and a NDPKI Certificate Practice Statement (CPS).

This CCEB CPMCG document indicates what assurance can be placed in a certificate issued by a CCEB nation that has issued a statement of self-assertion against the CPMCG. Defence PMAs are not expected to undertake a correlation with the CPMCG when drawing up CPSs.

3.1.1.3 Scope

This document is bound to the NDPKIs of the CCEB nations and exists to facilitate trusted electronic business transactions between CCEB National Defence organisations. As used in CPMCG, Entity PKI or Entity CA may refer to a National Defence organisation's PKI, a PKI provided by a commercial service for defence, or a bridge CA serving a defence community of interest.

3.1.1.4 Interaction with PKIs External to a CCEB Nations Defense PKI

A CCEB National Defence organisation may extend interoperability with other entities when it is beneficial to that organisation's PKI and if the nation concerned ensures that there is no effect on its relationship with the other CCEB NDPKIs. The entity PKI shall notify those NDPKI authorities with which it has cross certified that it intends to extend interoperability to other PKI systems.

3.1.2 Document Name and Identification

a. This CPMCG does not identify a specific CCEB X.509 CP. Instead, this CPMCG provides a framework of the agreed criteria that national candidate PKIs will use when asserting their National Defence CPs.

b. Each nation has identified one or more CPs that is considered capable of assertion against the CPMCG. CPs will be identified using an OID registered in each Nation's Object ID Registry Arc. The members of the PKI TF have agreed a broad equivalence between the CPs; however the detailed mapping between policy identifiers is a bi-lateral matter to be documented in the CCA.

3.1.3 PKI Participants

The following are the roles that are expected to be present for the administration and operation of a NDPKI. NDPKIs self-asserting against this CPMCG should indicate within the CCA if a particular role is not used in its PKI.

3.1.3.1 Policy Management Authority

Each NDPKI should have an identifiable body or management structure that is responsible for functional management of the NDPKI. Functional management in this context is defined as management responsibility for:

a. The national Defence organisation's overarching policy under which the nation's Defence PKI operates.

b. Overseeing the creation and update of certification policies.

c. Reviewing and approving the CPS of their organisation's Certificate Management Authority (CMA). CMAs are CAs and RAs of the NDPKI. If the NDPKI implements a Certificate Status Authority, it also is a CMA.

d. Presiding over audit programmes.

e. Defining the rules for interoperation with other PKIs.

f. Approving the appropriate mechanisms and controls for the management of the PKI.

g. Approving the operational standards and guidelines to be followed.

h. Addressing strategic PKI issues of the Defence organisation, with national and international significance.

i. Monitoring the governance and performance of the national organisation's defence PKI program.

j. Authorising the establishment of Certification Authorities.

3.1.3.2 Certification Authorities

A National Defence Certification Authority (CA) is an entity authorised by its PMA to create, sign, issue and revoke public key certificates. The CA has control over, and is responsible for all aspects of the issuance and management of certificates and describes its practices in a CPS that has been approved by its PMA.

3.1.3.3 Registration Authority

A Registration Authority (RA) will collect and verify each Subscriber's identity and other information for inclusion in the Subscriber's public key certificates. A CA may designate its own RAs. The RA must perform its functions in accordance with a CPS that has been approved by the PMA.

3.1.3.4 Subscribers

a. A subscriber is the entity whose name appears as the subject in a certificate, and who asserts that the use of its public key and certificate is in accordance with the national Defence CP. Subscribers include entities that have been approved in the national Defence CP, such as but not limited to:

(1) Personnel.

(2) Devices (e.g. Workstations, Firewalls, Routers, Trusted Servers and other infrastructure components).

(3) Organisational roles associated with individuals, groups of individuals or organisational entities.

(4) A Subscriber which is issued with a certificate under a national CP that is self-certified to this framework does not automatically receive access, authority or privilege to the Defence assets or systems of the cross-certified NDPKI.

3.1.3.5 Relying Parties

a. A Relying Party is responsible for deciding whether or how to check the validity of a certificate by establishing and validating a path to an appropriate trust anchor; the path validation process should include a check of the revocation status of all certificates in the path.

b. A Relying Party relies on the binding of the Subscriber's name to a public key; information in the certificate (such as certificate policy identifiers and key usage) may be used to determine the suitability of the certificate for a particular use.

3.1.3.6 Other Participants

The NDPKI may require the services of other security, community, and application authorities, such as directories, smartcard management systems and compliance auditors. The CCA shall identify the parties, services, and mechanisms used to support these services.

3.1.4 Certificate Usage

a. Certificates issued under NDPKI CPs that are self-asserted to CPMCG are assumed, in conjunction with their associated private keys, to allow a Subscriber to:

(1) Authenticate its identity.

(2) Digitally sign electronic documents, transactions and communications.

(3) Confidentially communicate with another party.

b. Cross-certificates will be issued between NDPKI Root CAs or the designated Highest Level Defence CA to enable national Defence Subscribers to release and exchange Military Information and Data under the CJM3IEM. All CCEB nations require that this Military Information and Data be accurate, available when needed, and available only to those authorized to receive it. Further it is necessary for the source of the information to be identifiable and capable of authentication as an official source.

c. Appropriate Certificate Uses NDPKI certificates as a minimum are expected to be used:

(1) To authenticate the identity of a Subscriber for any lawful business conducted between that Subscriber and the cross-certified CCEB nation, where the level of assurance has been assessed as sufficient by the PMA and the Relying Party.

(2) To provide accountability, and non-repudiation, of NDPKI Subscribers transactions or communications.

(3) To verify the integrity of a communication between a Subscriber and a Relying Party.

(4) To provide data confidentiality of NDPKI transactions or communications.

3.1.4.1 Prohibited Certificate Uses

The CPMCG explicitly prohibits the following uses for certificates:

a. To infer, or assume, from the certificate any attribute, authority, access, privilege or delegations that may be afforded the Subscriber unless it is specifically included in the certificate.

b. To infer, or assume, from the presentation of a certificate, digital signature or authentication process that the transactions or communications have or are occurring over appropriate infrastructure for that transaction or communication.

c. For a Subscriber to conduct any transaction, or communication, which is any or all of the following:

(1) Illegal.

(2) Unauthorised.

(3) Unethical.

(4) Unrelated to national business.

d. The acceptance of any certificate which is being used for a prohibited purpose shall be at the Relying Party's risk.

3.1.5 Policy Administration

3.1.5.1 Organisation administering a Defense CP

Each NDPKI PMA is responsible for all aspects of its CP.

3.1.5.2 Contact Person

Each NDPKI PMA must provide a contact point for questions regarding its CP.

3.1.5.3 Person Determining Certification Practices Statement Suitability for the Policy

Each NDPKI PMA is responsible for ensuring that its CPS(s) conform to the NDPKI CP.

3.1.5.4 CPS Approval Procedures

All nations self-asserting against the CPMCG must have their CPS(s) approved by their PMA.

3.1.6 Definitions and acronyms

See Annex B.

3.2 Publication & Repository responsibilities

3.2.1 Repositories

Nations shall operate repositories in support of their NDPKI and its operations and make available the information needed to determine the validity of a certificate. This may be achieved by providing access to the repository, or to such parts of the repository that may be needed to support certificate validation.

3.2.2 Publication of certification information

a. Each nation shall publish relevant CA certificates, CRLs and Subscriber certificates to their repository.

b. Each nation shall provide Subscribers and Relying Parties with the URL of a public website where it's CP is publicly available and shall provide, the relevant parties, under such terms and conditions as it shall deem appropriate, all or part of the CPS.

3.2.3 Time or Frequency of Publication

All information to be published in the repository shall be published promptly after such information becomes available. Detail on CRL issuance frequency can be found at Section 3.4.9.7. Details of repository publication timescales and frequency should be disclosed between parties within the CCA.

3.2.4 Access controls on repositories

Repository information shall be protected from unauthorized modification or disclosure.

3.3 Identification & Authentication

3.3.1 Naming

3.3.1.1 Types of Names

Each entity:

a. Must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate *Subject* and *Issuer* field.

b. May be assigned additional names via the *subjectAlternativeName* field.

c. The DN must be in the form of a X.501 printable string and must not be blank.

d. The CMA shall investigate and correct if necessary any name collisions brought to its attention. If appropriate, the CMA shall coordinate with and defer to the appropriate naming authority.

3.3.1.2 Need for Names to Be Meaningful

a. Names used to identify the Subscriber's must:

(1) Be meaningful.

(2) Relate directly to the identity of the Subscriber.

(3) Should be meaningfully related to the Evidence of Identity (EoI) information used to verify the Subscriber identity.

b. Where a NDPKI wishes to make use of group/role based certificates that are not related to the evidence presented by a Subscriber, this is stated in the CCA. Other nations are not bound to accept group/role based certificates for access control decisions and it is recommended that certificates that contain such names should be distinguishable from those that do not.

3.3.1.3 Anonymity or Pseudonymity of Subscribers

A CA shall not issue anonymous Subscriber certificates without the express consent of the NDPKI PMA. However pseudonymous Subscriber certificates may be issued by a CA. A certificate issued in the name of a role or group associated with a Subscriber is an example of a pseudonymous Subscriber certificate. A Relying Party should be able to determine, where pseudonyms are used, this from the content of the certificate.

3.3.1.4 Rules for Interpreting Various Name Forms

The rules for interpreting name forms shall comply with national defence standards and be shared with other nations when undergoing interoperability testing.

3.3.1.5 Uniqueness of Names

Name uniqueness must be enforced within the NDPKI. Wherever practical the national PMA should enforce name uniqueness policy within the X.500 namespace that it has been authorized to use.

3.3.1.6 Recognition, Authentication, & Role of Trademarks

A CMA shall not knowingly use trademarks in names unless the subject has rights to use that name, or issue a certificate knowing that it includes a trademark owned by another individual or entity or that a court of competent jurisdiction has determined infringes the trademark of another.

3.3.2 Initial Identity Validation

3.3.2.1 Method to Prove Possession of Private Key

a. In all cases, the CA must establish that the private key corresponding to the public key contained in any request is in the possession, or control of, the requestor. This may be done by use of any appropriate Proof of

Possession algorithm or technique approved for use within the NDPKI by the PMA.

b. Each NDPKI should establish policies that are appropriate to the key generation and distribution technologies that it uses.

3.3.2.2 Authentication of Organisation Identity

Where a NDPKI makes use of group/role identities, or issues certificates to devices, procedures must be in place to establish the authenticity of any organisational identity claimed or implied in the identity asserted by a certificate.

3.3.2.3 Authentication of Individual Identity

The CA must ensure that a Subscriber's identity is established to a level of assurance that is determined by national policy. For first-time registration, the elements of this process **must** include:

a. A face-to-face identification process.

b. A Government recognised Photo ID.

c. Validation of vetting or security clearance.

d. An auditable recording mechanism should be in place that captures information relevant to the identification process.

3.3.2.4 Non-verified Subscriber Information

All information offered by, or on behalf of, the Subscriber should be verified. Non-verified Subscriber information must not be included in certificates. It is recognised that e-mail addresses are a common exception to this requirement, and should be noted within the CCA if this is applicable.

3.3.2.5 Validation of Authority

Certificates that contain explicit or implicit organisation affiliation (e.g. group/role certificates) shall be issued only after that ascertaining the Subscriber has the authorisation to act on behalf of the organisation in the implied capacity.

3.3.2.6 Criteria for Interoperation

For cross certification the PMA shall validate the designated representative's authorization to act on behalf of the organisation.

3.3.3 Identification and authentication for re-key requests

3.3.3.1 Identification and Authentication for Routine Re-key

a. To maintain assurance provided to a Relying Party that a unique binding between the public and private key and it's named Subscriber is valid, a Subscriber must periodically obtain keys in accordance with the NDPKI CP.

b. A request for re-key may only be made by an entity (or sponsor acting on its behalf) in whose name the keys have been issued.

c. The entity must authenticate the hardware token to a CMA, if applicable, to authenticate itself to the RA. The process must ensure that the signature keys are generated within the hardware token or, in the case of externally generated keys, are inserted in the appropriate token, and the entity or entity sponsor must provide proof of possession of its current private key.

d. Re-key requests for certificates may be authenticated on the basis of current valid Subscriber certificates as long as the validity period of the new certificate does not extend beyond the periodic in-person authentication requirements listed in the table below. Individual NDPKI organisations may require shorter or longer periods for in-person authentication to deliver positive reinforcement of identification, in which case this should be covered during the drawing up of the CCA.

e. For CA Key Changeover see Section 3.5.6.

Assurance Level (a)	In Person Authentication Requirement (b)
Medium Assurance Software	9 Years
Medium Assurance Hard Token	3 Years
High Assurance	3 Years

3.3.3.2 Identification and Authentication for Re-key after Revocation

Where the information in a certificate has changed or where the certificate is revoked the CA shall authenticate a re-key in the same manner as in initial registration. Any change in the information contained in the certificate shall be verified before the certificate is issued.

3.3.4 Identification and authentication for revocation request

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.

3.4 Certificate Life-Cycle

3.4.1 Certificate Application

3.4.1.1 Who Can Submit a Certificate Application

The NDPKI PMA shall specify who may submit a certificate application and the associated process.

3.4.1.2 Enrollment Process and Responsibilities

The NDPKI PMA shall approve the enrolment process used by subjects to submit certificate applications and responsibilities in connection with this process.

3.4.2 Certificate Application Processing

Information in certificate applications must be verified as accurate in accordance with national policies and procedures before certificates are issued.

3.4.2.1 Performing Identification and Authentication Functions

The CA must ensure that each application is accompanied by confirmation of the end entity's identity and proof or confirmation of authorization for any requested certificate.

3.4.2.2 Approval or Rejection of Certificate Applications

The approval or rejection of certificate applications shall be dealt with in accordance with NDPKI Certificate Policy.

3.4.2.3 Time to Process Certificate Applications

The time for processing certificate applications shall be dealt with in accordance with NDPKI CPS.

3.4.3 Certificate Issuance

3.4.3.1 CA Actions during Certificate Issuance

a. The CA shall:

(1) Authenticate a certificate request.

(2) Verify whether a certificate request is correctly formed.

(3) Perform any additional process as specified in the CA CPS.

(4) Compose and sign the certificate.

(5) Provide the certificate to the Subscriber.

(6) Publish the certificate, as applicable.

b. An auditable record of this process shall be kept containing at a minimum:

(1) Details of the certificate request.

(2) The success, or rejection (with reason), of the certificate request.

(3) The identity of the Registration Authority (RA).

c. The CA is not bound to issue keys and certificates to any person despite receipt of an application.

d. The CA shall authenticate a certificate request, ensure that the public key is bound to the correct Subscriber, obtain a proof of possession of the private key, then generate a certificate, and provide the certificate to the Subscriber.

3.4.3.2 Notification to Subscriber of Certificate Issuance

Notification to a subscriber of certificate issuance must occur.

3.4.4 Certificate Acceptance

3.4.4.1 Conduct constituting certificate acceptance

A process shall be in place that shall notify the Subscriber that a certificate has been issued and their responsibilities upon acceptance. Certificate acceptance should include proof of possession of the private key and an ability to exercise it.

3.4.4.2 Publication of the Certificate by the CA

CA certificates and Subscriber encryption certificates shall be published to appropriate repositories, including those needed to support cross-certification with the NDPKI of another CCEB nation. A NDPKI may also elect to publish other certificates (e.g. for authentication or non-repudiation) to its repository.

3.4.4.3 Notification of Certificate Issuance by the CA to other entities

No stipulation

3.4.5 Key Pair and Certificate Usage

3.4.5.1 Subscriber Private Key and Certificate Usage

a. Subscribers shall protect their private keys from access by other parties.

b. Where *keyUsage* or *extendedKeyUsage* extensions are placed into a certificate then Subscribers should not use certificates for purposes that are implicitly or explicitly excluded by the extensions. Subscribers should use keys and certificates in accordance with the NDPKI policies.

c. The subscriber shall not use the signature private key after the associated certificate has been revoked or has expired. The Subscriber may continue to use the decryption private key solely to decrypt previously encrypted information after the associated certificate has been revoked or has expired.

3.4.5.2 Relying Party Public key and Certificate Usage

a. Relying Parties shall ensure that the public key in a certificate is used only for the purposes indicated by the *keyUsage* and *extendedKeyUsage* extensions, if these extensions are present in the certificate.

b. Relying Parties should use keys and certificates in accordance with the NDPKI policies.

3.4.6 Certificate Renewal

3.4.6.1 Circumstance for certificate renewal

a. The NDPKI PMA shall define the criteria to be met for certificate renewal.

b. These criteria should include as a minimum that:

(1) The current certificate is still within its validity period.

(2) The Subscriber has an approved affiliation.

(3) The new validity period will not extend beyond the usable life of the private keys.

(4) Certificate renewal shall not permit a Subscriber to avoid re-key or the associated identification and authentication process.

3.4.6.2 Who may request renewal

Any Subscriber or a CMA on behalf of the Subscriber who satisfies the NDPKI PMA defined criteria may request a certificate renewal.

3.4.6.3 Processing certificate renewal requests

The NDPKI PMA shall approve any certificate renewal processes, which shall be documented in the relevant CPS.

3.4.6.4 Notification of new certificate issuance to Subscriber

No stipulation.

3.4.6.5 Conduct constituting acceptance of a renewal certificate

Subscribers shall be informed of the process for certificate acceptance.

3.4.6.6 Publication of the renewal certificate by the CA

CA Certificates and Subscriber encryptions certificates shall be published to appropriate repositories, including those needed to support cross-certification with the NDPKI of another CCEB nation.

3.4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

3.4.7 Certificate Re-Key

3.4.7.1 Circumstance for certificate re-key

a. Circumstances for certificate re-key, shall be defined by the NDPKI PMA, and include but not be limited to:

(1) Useable life of current key material has been reached.

(2) Change in algorithm, or key length, required.

b. The NDPKI PMA shall define which circumstances initiating re-key require revocation of the current certificate.

3.4.7.2 Who may request certification of a new public key

Certificate re-key may be requested by the:

a. NDPKI PMA.

b. Subscriber or a CMA on behalf of the Subscriber.

3.4.7.3 Processing certificate re-keying requests

No stipulation.

3.4.7.4 Notification of new certificate issuance to Subscriber

No stipulation.

3.4.7.5 Conduct constituting acceptance of a re-keyed certificate

Subscribers shall be informed of the process for certificate acceptance.

3.4.7.6 Publication of the re-keyed certificate by the CA

Re-keyed CA Certificates and Subscriber encryption certificates shall be published to appropriate repositories, including those needed to support cross-certification with the NDPKI of another CCEB nation.

3.4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

3.4.8 Certificate Modification

3.4.8.1 Circumstance for certificate modification

a. Circumstances for certificate modification shall be defined by the NDPKI PMA, and include as a minimum:

(1) Details in the certificate relevant to the Subscriber have changed or been found to be incorrect.

(2) Interoperation with approved "Third Party" PKI, or national assets and systems, require certificate attributes or contents to be added, modified or deleted.

b. Subject name changes shall be processed as an initial issue.

3.4.8.2 Who may request certificate modification

Certificate modification may be requested by the:

(1) NDPKI PMA.

(2) Subscriber or a CMA on behalf of the Subscriber.

3.4.8.3 Processing certificate modification requests

No stipulation.

3.4.8.4 Notification of new certificate issuance to Subscriber

No stipulation.

3.4.8.5 Conduct constituting acceptance of modified certificate

Subscribers should be informed of the process for certificate acceptance.

3.4.8.6 Publication of the modified certificate by the CA

Modified CA Certificates and Subscriber encryptions certificates shall be published to appropriate repositories, including those needed to support cross-certification with the NDPKI of another CCEB nation.

3.4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation

3.4.9 Certificate Revocation & Suspension

3.4.9.1 Circumstances for Revocation

a. A certificate issued to a Subscriber shall be revoked:

(1) Upon suspected or known compromise of the private key.

(2) Upon suspected or known loss or compromise of the media holding the private key.

(3) When a Subscriber or CA server fails to comply with obligations set out in the CP, the relevant CPS, or any other agreement or applicable law.

(4) When the identity or other attributes asserted in the certificate becomes invalid (e.g. following termination of affiliation or employment).

b. In addition, if it is determined subsequent to issuance of new certificates that a private key used to sign requests for one or more additional certificates may have been compromised at the time the requests for additional certificates were made, al certificates authorised by directly or indirectly chaining back to that compromised key shall be revoked.

3.4.9.2 Who Can Request Revocation

The NDPKI PMA shall detail who can request revocation.

3.4.9.3 Procedure for Revocation Request

All certificate revocation requests shall be processed and authorised in accordance with NDPKI Certificate Policy.

3.4.9.4 Revocation Request Grace Period

Subscribers and authorized PKI entities shall request the revocation of a certificate as soon as the need for revocation comes to their attention.

3.4.9.5 Time within which CA must Process the Revocation Request

The time within which the CA must process the revocation request shall be defined by the NDPKI PMA.

3.4.9.6 Revocation Checking Requirements for Relying Parties

It is the Relying Party's responsibility to determine its requirements for revocation checking.

3.4.9.7 CRL Issuance Frequency

a. Subordinated CAs will issue, and publish, an up to date CRL at intervals not exceeding 24 hours.

b. CAs may publish CRLs following certificate revocation, prior to the routine publishing of a CRL.

c. The time period for a self-signed CA (Root) is to be specified in the CCA.

3.4.9.8 Maximum Latency for CRLs

The CRLs shall be published on generation.

3.4.9.9 On-line Revocation/Status Checking Availability

Nations may provide an on-line certificate status service. If provided, the service shall function in a manner that ensures that:

a. Accurate and up-to-date information from the authorized CA is used to provide the revocation status.

b. Revocation status responses provide authentication and integrity services commensurate with the assurance level of the certificate being checked.

3.4.9.10 On-line Revocation Checking Requirements

Nations may implement a Certificate Status Authority to operate one or more Certificate Status Servers.

3.4.9.11 Other Forms of Revocation Advertisements Available

CRLs will always be provided. No further stipulation.

3.4.9.12 Special Requirements Re Key Compromise

No stipulation.

3.4.9.13 Circumstances for Suspension

Circumstances for Suspension are not stipulated in this publication. If Suspension is to be used by a NDPKI the circumstances are to be covered in the CCA.

3.4.9.14 Who can Request Suspension

If Suspension is to be used by a NDPKI who can Request Suspension is to be articulated in the CCA.

3.4.9.15 Procedure for Suspension Request

If Suspension is to be used by a NDPKI the procedure for Suspension Request is to be articulated in the CCA.

3.4.9.16 Limits on Suspension Period

If Suspension is to be used by a NDPKI the limits on the Suspension Period are to be articulated in the CCA.

3.4.10 Certificate Status Services

3.4.10.1 Operational Characteristics

If the NDPKI implements an on-line certificate status service, it shall comply with RFC 2560.

3.4.10.2 Service Availability

No stipulation.

3.4.10.3 Optional Features

No stipulation.

3.4.11 End of Subscription

a. A subscription for a certificate ends when a certificate is revoked or allowed to expire.

b. A subscription for a certificate ends when all tokens containing the certificate's matching private key have been surrendered and destroyed or zeroised in an approved manner.

3.4.12 Key Escrow & Recovery

3.4.12.1 Key Escrow and Recovery Policy and Practices

Under no circumstances is a private key that is issued for a signing service to be placed into a key recovery system.

3.4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation

3.5 Facility Management & Operations Controls

3.5.1 Physical Controls

The Physical security requirements for a NDPKI technical infrastructure must be operated in accordance with the national security regulations. The minimum standard is IAW ACP122. If the NDPKI implements a Certificate Status Authority, it shall comply with the physical controls specified for the NDPKI CA's for which it provides revocation status.

3.5.1.1 Site Location and Construction

Site location and construction shall be determined in accordance with NDPKI policies.

3.5.1.2 Physical Access

Physical access shall be determined in accordance with NDPKI policies.

3.5.1.3 Power and air conditioning

Power and air conditioning shall be determined in accordance with NDPKI policies.

3.5.1.4 Water exposures

In accordance with NDPKI policies.

3.5.1.5 Fire prevention and protection

Fire prevention shall be determined in accordance with NDPKI policies.

3.5.1.6 Media storage

Media storage shall be determined in accordance with NDPKI policies.

3.5.1.7 Waste disposal

Waste disposal shall be determined in accordance with NDPKI policies.

3.5.1.8 Off-Site backup

To safeguard business continuity, it is essential that full system backups are performed. The NDPKI PMA must define procedures for full system backups sufficient to recover from system failure.

3.5.2 Procedural Controls

If the NDPKI implements a Certificate Status Authority, it shall comply with the procedural controls specified for the NDPKI CA's for which it provides revocation status.

3.5.3 Trusted Roles

The NDPKI CP is to specify the trusted roles to be utilised within the PKI.

3.5.3.1 Number of Persons Required per Task

The number of persons per task shall be specified in the NDPKI CP.

3.5.3.2 Identification and Authentication for Each Role

A person occupying a trusted role shall have his/her identity and authorisation verified, before being permitted to perform any action for that role or identity. A person occupying a trusted role shall authenticate to a remote infrastructure component of the NDPKI using a valid NDPKI X.509 certificate.

3.5.3.3 Roles Requiring Separation of Duties

Any person acting in a trusted role should not also undertake an audit role on the system for which the trusted role is associated. Under no circumstances shall the incumbent of a CMA role perform its own compliance or security auditor function. The person performing the compliance auditor function shall not perform any other role on the CMA. The person performing the security audit function shall not perform any other role on the CMA. An RA shall not perform any role on the CA, including the security or compliance audit functions. An RA shall not perform system administrator duties on any system where they exercise CMA authority.

3.5.4 Personnel Controls

If the NDPKI implements a Certificate Status Authority, it shall comply with the personnel controls specified for the NDPKI CA's for which it provides revocation status.

3.5.4.1 Qualifications, Experience, & Clearance Requirements

Personnel engaged in the NDPKI must be suitably qualified and experienced. Personnel requesting certificates shall hold a national security clearance equal to or above the clearance being asserted. All personnel engaged in the operation of the NDPKI will hold the appropriate national clearance in accordance with the nation's defence security regulations.

3.5.4.2 Background Check Procedures

All personnel engaged in the operation of the NDPKI must undergo background security checks in accordance with the nation's Defence security regulations.

3.5.4.3 Training Requirements

The NDPKI PMA should be able to demonstrate that a suitable training regime exists and is executed for personnel engaged in the management and operation of the NDPKI.

3.5.4.4 Retraining Frequency & Requirements

The NDPKI CP must demonstrate the intent for the appropriate re-training of personnel engaged in the management and operation of the NDPKI.

3.5.4.5 Job Rotation Frequency & Sequence

Job rotation frequency and sequence shall be specified in the appropriate CPS.

3.5.4.6 Sanctions for Unauthorized Actions

Each nation must be able to demonstrate that procedures and processes are in place to ensure that appropriate action is taken following an unauthorized action that brings into question the security of the system.

3.5.4.7 Independent Contractor Requirements

Each national Defence CP shall have policies that apply equally to all personnel who manage or operate the PKI.

3.5.4.8 Documentation Supplied To Personnel

Documentation sufficient to define duties and procedures for each role shall be provided by nations to the personnel filling each such role.

3.5.5 Audit Logging Procedures

If the NDPKI implements a Certificate Status Authority, it shall comply with the audit logging procedures specified for the NDPKI CA's for which it provides revocation status except as specified below.

3.5.5.1 Types of Events Recorded

a. All NDPKIs shall have an audit system that records certificate lifecycle operations, attempts to access NDPKI assets such as CAs, PKI directories, and RAs and requests made to the system. For each event the minimum information shall be recorded:

(1) Type of event.

(2) Date and time of event.

(3) Identity of entity causing event and that of those handling it.

(4) The success or failure (along with reason for failure) of the event.

b. Certification Status Authorities are not required to log requests for revocation status or the responses to those requests.

3.5.5.2 Frequency of Processing Log

Audit logs shall be reviewed periodically at least six times a year for anomalous and unauthorised events, with at least 25% of the security data generated since the last review being examined.

3.5.5.3 Retention Period for Audit Log

Security audit shall be available onsite for at least 2 months or until review, then offsite as archive records in accordance with each nation's Defence regulations. Audit data can only be deleted from a system after it has been archived.

3.5.5.4 Protection of Audit Log

Audit data should not be open for reading or modification by any person or automated system process, other than those performing an audit function. NDPKI system and configuration procedures must be in place to protect the electronic audit log system and audit information captured electronically or manually from unauthorized viewing, modification, deletion or destruction.

3.5.5.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be backed up. A copy of the audit log shall be sent off-site.

3.5.5.6 Audit Collection System (Internal vs. External)

The security audit process shall be in accordance with each nation's Defence security regulations. Should it become apparent that an automated security audit system has failed; the CMA shall cease all operation except for revocation processing until the security audit capability can be restored. Under these circumstances, the CMA shall employ mechanisms to preclude unauthorized CMA functions.

3.5.5.7 Notification to Event-Causing Subject

No stipulation.

3.5.5.8 Vulnerability Assessments

NDPKIs shall have vulnerability assessments in place that are in accordance with each nation's Defence security regulations. At a minimum security auditors shall check for continuity of the security audit data.

3.5.6 Records Archive

If the NDPKI implements a Certificate Status Authority, it shall comply with the records archives requirements specified for the NDPKI CA's for which it provides revocation status.

3.5.6.1 Types of Events Archived

Archive records shall be sufficiently detailed to establish the validity of a signature and the proper operation of the PKI.

3.5.6.2 Retention Period for Archive

a. The retention period for archives shall be in accordance with national Defence security regulations.

b. Applications necessary to read these archives must be maintained for at least the applicable retention period above.

3.5.6.3 Protection of Archive

The protection of archives shall be in accordance with national Defence security regulations.

3.5.6.4 Archive Backup Procedures

Archive backup procedures shall be in accordance with national Defence security regulations.

3.5.6.5 Requirements for Time-Stamping of Records

Time stamping shall take place in accordance with national policy and procedures.

3.5.6.6 Archive Collection System (Internal or External)

Archive collection shall take place in accordance with national policy and procedures.

3.5.6.7 Procedures to Obtain & Verify Archive Information

Nations shall ensure that a process to affirm the integrity and authenticity of archival records is in place.

3.5.7 Key Changeover

Nations shall ensure that processes for key change-over and other transitional mechanisms relating to CA keys, which maintain the integrity of the systems, are in place.

3.5.8 Compromise & Disaster Recovery

3.5.8.1 Incident and Compromise Handling Procedures

Each NDPKI PMA shall be notified of all incidents, and where the continued integrity of service is impacted, a formal notice to cross-certified entities, and accrediting bodies shall be issued indicating the corrective action being taken and the estimated schedule for implementation

3.5.8.2 Computing Resources, Software, and/Or Data Are Corrupted

The CA shall maintain backup copies of system, databases, and private keys in order to rebuild the CA capability in case of software and/or data corruption.

3.5.8.3 Entity Private Key Compromise Procedures

See Para 3.5.8.1

3.5.8.4 Business Continuity Capabilities after a Disaster

Each CA shall prepare and maintain a business continuity plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster.

3.5.9 CA & RA Termination

In the event that a NDPKI CA ceases operation, the CA shall notify all NDPKI CAs which with it has cross-certified. Such notice shall be given prior to or immediately upon termination of operations.

3.6 Technical Security Controls

3.6.1 Key Pair Generation & Installation

a. Key pair generation shall be undertaken via combination of products and processes approved by each nation's appropriate Defence Security Authority/Organisation, to provide keys suitable for:

(1) Use in PKI based authentication, non-repudiation and integrity services for systems and data up to and within a SECRET high environment; and

(2) Use in PKI based confidential communications capable of protecting symmetric (Secret Key encryption) keys used to protect data up to and including the RESTRICTED classification over publicly accessible data networks (e.g. the Internet)[10].

(3) Use in PKI based confidential communications within a SECRET high environment to protect "need to know" using processes which are approved by the appropriate National Security Authority(NSA)/Defence Security Organisation (DSO).

b. Where key-pairs are generated within a hardware token that is intended for use by a human Subscriber copies of private signature keys shall not be kept, or capable of recovery.

c. Key pair generation for encryption keys may occur within the hardware token intended for use by the Subscriber; or within an approved Hardware Security Module (HSM) using processes which are approved by the NSA/DSO; or, where appropriate, transferred from an original Subscriber token to a new Subscriber token as long as there are assurances that no copies other than authorized key escrow copies of the keys continue to exist after the generation and insertion processes have completed.

[10] Canada and the United States do not use the classification RESTRICTED in their national systems. Canada and the United States handle and protect UK/AU/NZ RESTRICTED information in a manner no less stringent than the standards and procedures they apply on the security protection of NATO RESTRICTED information.

d. Where key-pairs for signature and encryption purposes are stored or managed within a software token, such key generation should employ a cryptographic module meeting or exceeding the NDPKI specified standard for Subscriber software cryptographic modules.

e. The NDPKI CPS shall detail the products, process and procedures that have been approved and the approved combinations they may be used in.

f. If the NDPKI implements a Certificate Status Authority, it shall comply with the records archives requirements specified for the NDPKI CA's for which it provides revocation status.

3.6.1.1 Private Key Delivery to Subscriber

a. Where private keys are generated by the Subscriber on the Subscriber's token, no additional delivery process is required.

b. Where private keys are generated in another cryptographic module the process for delivery of the private key securely onto the Subscriber's token is to be approved by the nation's NSA/DSO. While outside of the cryptographic module and the Subscriber's token, private keys are always to be encrypted using an algorithm and process approved by the NSA/DSO.

c. The appropriate CPS shall detail the products, process and procedures that have been approved and the approved combinations they may be used in.

3.6.1.2 Public Key Delivery to Certificate Issuer

Public keys shall be delivered to the certificate issuer in a way that binds the applicant's verified identification to the public key being certified. This binding shall be accomplished using means that are as secure as the security offered by the keys being certified. The binding shall be accomplished using cryptographic, physical, procedural, and other appropriate methods. The methods used for public key delivery shall be stipulated in the appropriate CPS.

3.6.1.3 CA Public Key Delivery to Relying Parties

Trusted CA certificates for the NDPKIs and any directly trusted intermediate CAs must be delivered to Relying Parties via a secure mechanism.

3.6.1.4 Key Sizes

Intentional omission from Pub 1010 Version 1.

3.6.1.5 Public Key Parameters Generation and Quality Checking

Public key parameters shall always be generated and checked in accordance with the NSA/DSO that defines the crypto algorithm in which the parameters are to be used.

3.6.1.6 Key Usage Purposes (as per X.509 v3 key usage field)

Public keys that are bound into certificates shall be certified for use in signing or encrypting, but not both, with the exception of device certificates intended to support TLS/SSL servers. The use of a specific key is determined by the key usage extension in the X.509 certificate.

3.6.2 Private Key Protection & Cryptographic Module Engineering Controls

3.6.2.1 Cryptographic Module Standards & Controls

All cryptographic modules, HSM's and hardware tokens are to be approved for the intended use by the appropriate NSA/DSO.

3.6.2.2 Private Key Multi-Person Control

a. There must be multi person control for CA key generation operations; for CAs and OCSP Responders, a single person shall not be permitted to generate or invoke the complete CA or OCSP signature or access any cryptographic module containing the complete CA or OCSP private signing key. Access to CA or OCSP Responder signing keys backed up for disaster recovery shall be under at least two-person control.

b. The NDPKI is to define the trusted roles in the CP indicating those roles that require multi-person control.

c. The names of all persons able to control the operation of the equipment or provide access to private key authentication components must be recorded and available for audit purposes

3.6.2.3 Private Key Escrow

a. Under no circumstances shall signature keys used to support non-repudiation services be held in trust by any party other than the Subscriber.

b. Where Encryption Private Key recovery capabilities are offered by a NDPKI, methods and procedures shall be documented in a Key Recovery policy.

3.6.2.4 Private Key Backup

a. All copies of private keys, including those that might be embedded in component backups, shall be adequately protected from compromise.

b. Backed up keys must be stored in encrypted form and protected at a level no lower than stipulated for the primary version of the key if outside an approved crypto-module.

3.6.2.5 Private Key Archival

Refer to 3.6.2.3 and 3.6.2.4

3.6.2.6 Private Key Transfer into or from a Cryptographic Module

To be carried out in accordance with the nation's NSA/DSO regulations.

3.6.2.7 Private Key Storage on Cryptographic Module

The method of storing private keys on cryptographic modules must be done in accordance with approved procedures identified by each national security policy.

3.6.2.8 Method of Activating Private Keys

Activation of the private key within a cryptographic module must always be protected by an approved NSA/DSO authentication mechanism.

3.6.2.9 Methods of Deactivating Private Keys

Cryptographic modules, which have been activated, must not be left unattended or otherwise open to unauthorized access. After use, they must be deactivated. Hardware cryptographic modules shall be removed and stored when not in use.

3.6.2.10 Method of Destroying Subscriber Private Signature Keys

Private keys are to be destroyed in accordance with each national security policy.

3.6.2.11 Cryptographic Module Rating

See 3.6.2.1

3.6.3 Other Aspects of Key Management

3.6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

3.6.3.2 Certificate Operational Periods/Key Usage Periods.

Maximum periods of:

Entity	Key Life	Certificate Life
Root CAs	25 years	25 Years
CA & RA servers	10	10
Validation Server	3	3

Subscriber	3	3
Trusted Role	3	3

3.6.4 Activation Data

3.6.4.1 Activation Data Generation & Installation

a. Activation data may be Subscriber selected. A pass-phrase, PIN, biometric data, or other mechanisms of equivalent authentication robustness shall be used to protect access to use of a private key. PINS, when used, shall be a minimum of 6 digits in length. Passwords when used shall be a minimum of 6 characters.

b. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

c. The type of activation data used and the processes carried out with regard to activation data is to be included in the CCA.

3.6.4.2 Activation Data Protection

a. Activation data in conjunction with other access control must have an appropriate level of strength for the keys or data to be protected,

b. Activation data for cryptographic modules should be memorised, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module.

c. Activation data for private keys associated with certificates asserting individual identities shall never be shared.

d. Activation data for private keys associated with certificates asserting organisational identities shall be restricted to those in the organisation authorized to use the private keys.

3.6.4.3 Other Aspects of Activation Data

In accordance with NDPKI CPS.

3.6.5 Computer Security Controls

3.6.5.1 Specific Computer Security Technical Requirements

Computers shall be approved for use by the NSA/DSO.

3.6.5.2 Computer Security Rating

No stipulation.

3.6.6 Life-Cycle Security Controls

3.6.6.1 System development controls

System development controls shall be undertaken in accordance with the relevant NDPKI CPS.

3.6.6.2 Security management controls

Security management controls shall be undertaken in accordance with the relevant NDPKI CPS.

3.6.6.3 Life cycle security controls

Life cycle security controls shall be undertaken in accordance with the relevant NDPKI CPS

3.6.7 Network Security Controls

a. Network security controls shall be undertaken in accordance with national security policy.

b. NDPKI equipment shall be located in National Defence networks in a manner that affords sufficient protection given the risk assessment conducted during the accreditation process.

3.6.8 Time Stamping

No stipulation.

3.7 Certificate, CARL/CRL, And OCSP profiles Format

The profiles contained within this section are considered to be tentative and separate profiles for different user certificates will be fully defined and subsequently published following CCEB PKI interoperability testing.

3.7.1 Certificate Profile

3.7.1.1 Version Numbers

PKI Certificates issued shall be X.509 v3 certificates (populate version field with integer “2”).

3.7.1.2 Certificate Extensions

a. CA Certificates issued by NDPKIs shall not include private critical extensions. The following extensions are included in cross-certificates:

Extension	CA	Cross-Certificate
Authority Key Identifier	Non-critical 20-byte SHA1 hash	Non-critical 20-byte SHA1 hash
Subject Key Identifier	Non-critical 20-byte SHA1 hash	Non-critical 20-byte SHA1 hash
Basic Constraints	critical cA True	critical cA True
Name Constraints	See Note 1	See Note 1
Policy Constraints	See Note 1	See Note 1
Key Usage	critical keyCertSign mandatory; cRLSign optional	critical keyCertSign mandatory; cRLSign optional
Certificate Policies	Non-critical Includes national policy OID(s)	Non-critical Includes national policy OID(s)
Policy Mappings	not populated	Non-critical Approved mappings
Subject Alternative Name	not populated	not populated
Issuer Alternative Name	not populated	not populated
Authority Information Access	non-critical LDAP mandatory; HTTP optional; OCSP optional	non-critical LDAP mandatory; HTTP optional; OCSP optional
Subject Information Access	not populated	See Note 1
CRL Distribution Points	non-critical LDAP mandatory; HTTP optional	non-critical LDAP mandatory; HTTP optional
Freshest CRL	not populated	not populated
Extended Key Usages	non-critical	non-critical
Inhibit Any Policy	See Note 1	See Note 1

b. The following are included in Subscriber certificates:

Extension	People SW	People HW	Server
Authority Key Identifier	Non-critical 20-byte SHA1 hash	Non-critical 20-byte SHA1 hash	Non-critical 20-byte SHA1 hash
Subject Key Identifier	Non-critical 20-byte SHA1 hash	Non-critical 20-byte SHA1 hash	Non-critical 20-byte SHA1 hash
Basic Constraints	optional	optional	optional

Name Constraints	not populated	not populated	not populated
Policy Constraints	not populated	not populated	not populated
Key Usage	Critical	Critical	Critical
Certificate Policies	Non-critical Includes national policy OID	Non-critical Includes national policy OID	Non-critical Includes national policy OID
Subject Alternative Name	Non-critical RFC822Address mandatory; X.400 address optional	Non-critical RFC822Address mandatory; X.400 address optional	Non-critical RFC822Address mandatory; X.400 address optional
Issuer Alternative Name	not populated	not populated	not populated
Authority Information Access	non-critical LDAP mandatory; HTTP optional; OCSP optional	non-critical LDAP mandatory; HTTP optional; OCSP optional	non-critical LDAP mandatory; HTTP optional; OCSP optional
Subject Information Access	not populated	not populated	not populated
CRL Distribution Points	non-critical LDAP mandatory; HTTP optional	non-critical LDAP mandatory; HTTP optional	non-critical LDAP mandatory; HTTP optional
Freshest CRL	not populated	not populated	not populated
Extended Key Usages	non-critical	non-critical	non-critical

c. Where a known NDPKI transition plan to a new PKI crypto algorithm exists this is to be made known at the time of planning and preparing for the bilateral cross-certification in order for PMAs to determine the impact on Relying Parties.

3.7.1.3 Algorithm Object Identifiers

a. Certificates issued by NDPKIs shall identify the signature algorithm using the following OID:

sha-1WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) PKI certificates(1) PKI certificates-1(1) 5 }

b. Certificates issued by National PKIs shall identify the cryptographic algorithm associated with the subject public key using the following OID:

RsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) PKI certificates(1) PKI certificates-1(1) 1 }

c. Certificates under this policy will use the following OIDs for signatures:

sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) PKI certificates(1) PKI certificates-1(1) 5}

d. Certificates under this policy will use the following OIDs for identifying the algorithm for which the subject key was generated:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) PKI certificates(1) PKI certificates-1(1) 1}
dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}

e. The NDPKI shall only certify public keys associated with the cryptographic algorithms identified above, and shall only use the signature algorithms identified above to sign certificates, CRLs and any other DPKI product.

3.7.1.4 Name Forms

The subject and issuer fields of the base certificate shall be populated with an X.500 Distinguished Name. Distinguished names shall be composed of standard attribute types, as identified in X.501 and ACP133.

3.7.1.5 Name Constraints

CA certificates issued by NDPKIs shall include name constraints to limit the name space of the CAs, as determined by the Nation.

3.7.1.6 Certificate Policy Object Identifier

All certificates issued by NDPKIs should include a certificate policies extension asserting the appropriate OID(s).

3.7.1.7 Usage of Policy Constraints Extension

All certificates issued by NDPKIs may include a policy constraints extension asserting the appropriate OID(s).

3.7.1.8 Policy Qualifiers Syntax & Semantics

Not to be used.

3.7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics in accordance with RFC 3280.

3.7.2 CRL Profile

3.7.2.1 Version Numbers

Where possible CRLs issued shall be v2 CRLs (populate version field with integer "1") however legacy V1 CRLs may be used.

3.7.2.2 CRL and CRL Entry Extensions

a. The following CRL Entry Extensions may be included: Reason Code and Invalidity Date. Both are non-critical.

b. If using partition CRLs, the issuing distribution point is critical.

c. The following CRL Extensions may be included: Authority Key Identifier, CRL Number, and Issuing Distribution Point. Issuing Distribution point is critical the others are not. The Authority Key Identifier shall use the keyIdentifier choice.

3.7.3 OCSP Profile

3.7.3.1 Version Numbers

OCSP version 1 as defined in RFC2560.

3.7.3.2 OCSP Extensions

Appropriate extensions from RFC 2560 may be used in OCSP requests and responses

3.8 Compliance Audit & Other Assessments

Each NDPKI is expected to conduct audit activities against its CP. The cross-certification agreement between the respective PMAs is to include an indication of the processes and procedures to be used for the exchange of audit compliance information.

3.8.1 Frequency of Audit or Assessments

All CAs shall be audited in accordance with the requirements of the NDPKI CP.

3.8.2 Identity & Qualifications of Assessor

The auditor must demonstrate competence in the field of PKI compliance audits.

3.8.3 Assessor's Relationship to Assessed Entity

The compliance auditor and audited party shall be sufficiently organisationally separated to provide an unbiased, independent evaluation.

3.8.4 Topics Covered By Assessment

The purpose of a compliance audit shall be to verify that the audited party has in place, a system to assure the quality of the services that it provides, and that it complies with all of the requirements of the CP and CPSs.

3.8.5 Actions Taken As A Result Of Deficiency

When the compliance auditor finds a discrepancy between a CMA's operation and the stipulations of its CPS, the procedures defined in national policy are to be followed.

3.8.6 Communication of Results

The PMA shall provide the compliance audit results to the PMA of cross certified PKIs if required by cross certification agreements.

3.9 Other Business & Legal Matters

Where CJM3IEM can be applied it shall have precedence over any other clauses in this Section. With regard to the specific legal position the provisions of the nations' respective Certificate Policies will apply. Any detailed provisions will need to be included in the relevant Cross-Certification Agreement.

3.9.1 Fees

Each of the nations shall bear its own costs in connection with cross-certification. The nations shall not impose fees on the Relying Parties of other CCEB nations in accordance with the principles of Section IV of the CJM3IEM.

3.9.2 Financial Responsibility

Each of the nations shall bear its own costs in connection with cross-certification in accordance with the principles of Section IV of the CJM3IEM.

3.9.3 Confidentiality of Business Information

The information which may be exchanged between nations following cross-certification and how it may be used is specified in Section V, VI and VIII of the CJM3IEM. For the purposes of this Publication 1010, all such information is Business Information. Any such information which is confidential shall be kept confidential. Any such information which is protectively marked shall be treated in accordance with the appropriate provisions of the CJM3IEM[11].

[11] The CJM3IEM provides different rules for different categories of protectively marked information.

3.9.4 Privacy of Personal Information

a. Subscriber information gathered during the registration process is confidential personal information and shall not be disclosed by the authority which gathers it.

b. Personal information shall be treated in accordance with the national laws of the CCEB member which gathers it.

c. Personal information contained within certificates may only be transferred to other CCEB nations through the PKI process with the written consent of the subject of that information.

3.9.5 Intellectual Property Rights

Subject to any existing rights of thirds parties, all IPR in any information exchanged between CCEB nations shall remain the property of the originator.

3.9.6 Representations & Warranties

Any representations and warranties shall be set out in the respective cross-certification agreement.

3.9.7 Disclaimers of Warranties

The disclaimer of warranties shall be as provided for in the respective cross-certification agreement.

3.9.8 Limitations of Liability

Subject to Section XI of CJM3IEM, the liability of the nations shall be limited respectively as provided in the respective cross-certification agreement.

3.9.9 Indemnities

Subject to Section XI of CJM3IEM, the provision of indemnities shall be as provided in the respective cross-certification agreement.

3.9.10 Term & Termination

This publication 1010 shall remain effective unless and until terminated or replaced with the unanimous written agreement of the CCEB nations, or on the earlier expiration of the CJM3IEM.

3.9.11 Individual Notices & Communications With participants

Extant processes and procedures between nations for the notification of incidents shall apply.

3.9.12 Amendments

3.9.12.1 Procedure for Amendment

a. The CCEB PKI Task Force and representing Nations shall review this publication when tasked to do so by the CCEB Executive Group (EG).

b. NDPKIs shall reassert their compliance with CCEB Pub 1010 when performing Amendments to their national Defence CPs.

c. Amendments to this Publication 1010 shall only be made with the unanimous written consent of the CCEB nations through the CCEB EG.

3.9.12.2 Notification Mechanism and Period

CJM3IEM and Section 5 of Pub 1010 apply.

3.9.12.3 Circumstances under which OID must be changed

Although it is not expected, if an OID change is required by a national authority the CCEB PKI Task Force and representing Nations shall review this publication for policy mappings.

3.9.13 Dispute Resolution Provisions

Any dispute in relation to this Publication 1010 shall be resolved initially by consultation amongst the CCEB nations at the PKI TF level with further consultation if necessary at the CCEB EG level.

3.9.14 Governing Law

Not applicable[12].

3.9.15 Compliance with Applicable Law

CJM3IEM applies

3.9.16 Miscellaneous Provisions

Not applicable.

3.9.17 Other Provisions

Not applicable.

[12] This is document is an international publication, therefore a governing law provision is not appropriate.

3.10 ACKNOWLEDGEMENTS

The CCEB PKI Task Force developed this section of Pub 1010 based on RFC 3647 and the collective Certificate Policies (and drafts) from each of the representative CCEB member nations.

4 TECHNICAL INTEROPERABILITY ACTIVITIES

4.1 INTRODUCTION

a. This section gives an overview of the technical interoperability activities that will be carried out between CCEB NDPKIs.

b. Technical interoperability activities will take place to support PKI interoperability between the CCEB nations. The intention is to link up the test/development labs of each nation and undertake interoperability testing leading to bilateral cross-certification between the test roots; subsequent testing will take place to focus on establishing stable configurations to support common applications.

4.2 Test Architecture

PKI interoperability testing will be conducted over the Coalition Unclassified Environment on CFBLNet. Labs will connect on a bi-lateral basis for testing purposes.

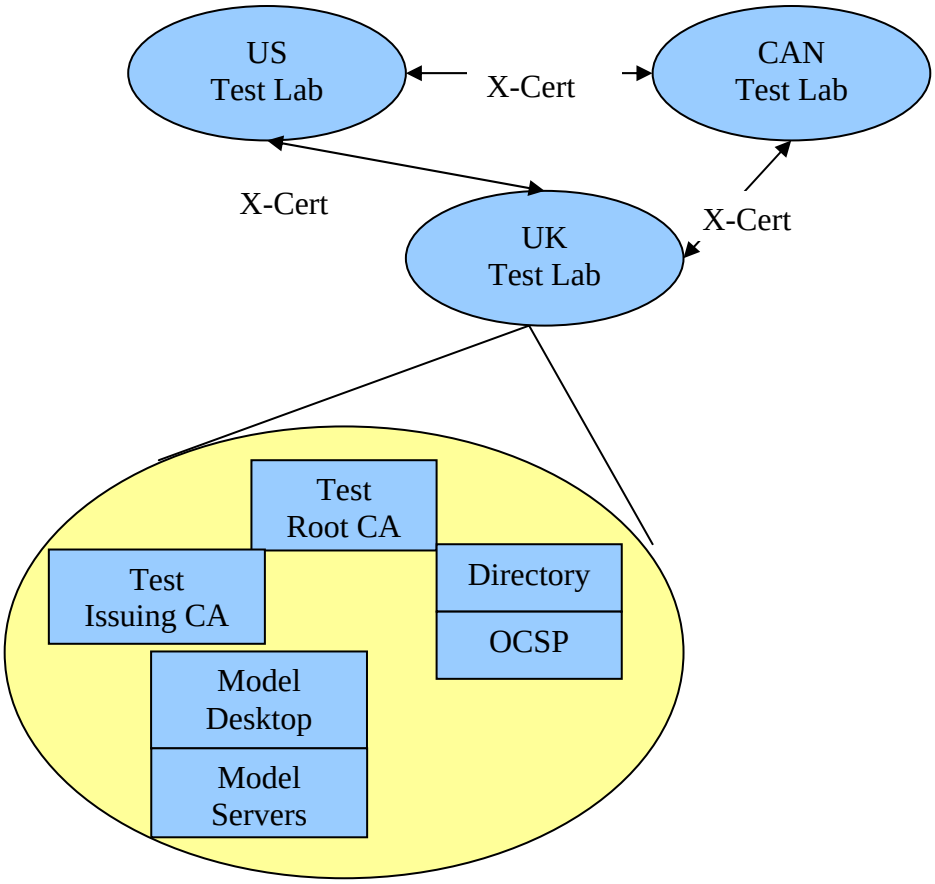

Figure 2. Test Architecture.

4.3 Scope

a. The scope is deliberately limited to supporting the objectives of PUB 1010:

(1) Supporting cross-certification between CCEB nations.

(2) Supporting present and future CCEB operational requirements.

b. Existing CCEB standards will be used as the baseline for defining application requirements and usage.

4.4 Objectives

a. To establish bilateral procedures for generating and exchanging cross-certification data, including:

(1) A Cross-certificate profile for each bilateral relationship.

(2) Authentication data to support the cross-certification process.

b. To establish bilateral procedures for accessing revocation information, including but not limited to:

(1) CRL exchange.

(2) Directory data redirection.

(3) OCSP.

c. Using representative applications, to determine working profiles that enable correct path discovery and validation using combinations of:

(1) Policy OID mappings.

(2) Name constraints.

(3) Path length constraints.

(4) Key and extended key usage.

(5) Subject and subject alternative names.

(6) Monolithic and partitioned CRLs.

(7) Local and remote OCSP (i.e. this nation vs. that nation).

d. Other activities:

(1) Exercise possible incident response scenarios.

(2) Investigate future technology initiatives of relevance to CCEB.

4.5 Expected Outputs

Recommended technical guidelines, with procedures, for:

a. Bi-lateral cross-certification

b. Certificate profiles for CCEB use

c. Supporting present and future CCEB operational requirements

d. S/MIMEv3 +/- ESS configurations

e. Outlook/Exchange

f. Other mail systems

g. For signatures and encryption

h. TLS 1.0 and SSL 3.0 configurations and options

i. Focus on HTTPS

j. IPSec VPN (tunnel and transport)

5 GOVERNANCE & CHANGE CONTROL OF CCEB PUB 1010

5.1 INTRODUCTION

a. This section gives a high level description of the procedures and processes for the governance and change control of CCEB Pub 1010.

b. The Master Copy of CCEB Pub 1010 is retained by the CCEB Washington Staff who will also be responsible for version control of the document.

c. Management of change to the document is the through CCEB PKI TF chair. Out of committee ad hoc meetings/teleconferences can be carried between member nations to discuss and agree changes prior to submission to the CCEB EG as amendments.

d. Proposed amendments to Pub 1010 are to be distributed by the proposing nation to other member nations of the PKI TF for discussion and agreement. Amendments to Pub 1010 shall only be made with the unanimous written consent of the CCEB nations through the CCEB EG.

e. The CCEB PKI Task Force and representing Nations shall review this publication when tasked to do so by the CCEB Executive Group (EG).

f. NDPKIs shall reassert their compliance with this CCEB Pub 1010 when performing Amendments to their national Defence CPs.

g. Changes to Pub 1010 once agreed by the PKI TF member nations will be notified to the CCEB Washington Staff by the PKI TF Chair. The CCEB Washington Staff will promulgate the change to the EG using extant CCEB process.

h. After an amendment has been ratified by the EG the PKI TF Chair will incorporate the amendment into Pub 1010 and return the amended version to the CCEB Washington Staff to be held as the Master Copy.

6 COMPLIANCE (ON NATIONAL CERTIFICATION) & AUDIT

6.1 ACCREDITATION

a. To ensure the mutual recognition and compliance of national accreditation standards for PKI within the CCEB community, the Multinational Security Accreditation Board (MSAB) is the endorsement authority in accordance with ACP122E.

b. The MSAB exists to facilitate and endorse the accreditation of all interconnected CIS and (in the case of Griffin each service/capability) established between two or more of the CCEB nations and NATO.

c. Each national MSAB representative will coordinate the inputs from each of the national accreditation agencies and produce a National Accreditation Endorsement Certificate (NAEC) for the MSAB chair confirming that national accreditation standards have been met for PKI.

d. As NAECs are received the MSAB Chair will issue a Coalition Accreditation Endorsement Certificate for each bi-lateral agreement established between the CCEB NDPKIs.

6.2 AUDITING

All security related events, as defined by national policy, shall be recorded in audit records.

A REFERENCES

a. Interoperability Options v0.3 – 5-Eyes Military PKI Interoperability

b. Cramer Report – Access to DoD Online Resources

c. ACP 145 – Gateway-to-Gateway Implementation Guide for ACP123/STANAG 4406 Messaging Services

d. Memorandum of Understanding - Combined Joint Multilateral Master Military Information Exchange

e. CJM3IEM Information Exchange Annex – *Authentication Services*

f. PKI Forum's White Paper – PKI Interoperability Framework

g. ITU-T X.509 Recommendation – The Directory: Authentication Framework

h. IETF RFC 2560 – Online Certificate Status Protocol

i. IETF RFC 3280 – The Internet Public Key Certificate and CRL Profile

j. IETF RFC 3647 – Certificate Policy and Certificate Practices Framework

B ACRONYMNS

ACP	Allied Communication Publication
ADF	Australian Defence Force
AIA	Authority Information Access
CA	Certification Authority
CCA	Cross Certificate Agreement
CCEB	Combined Communications Electronics Board
CFBLNet	Combined Federated Battle Lab Network
CJM3IE	Combined Joint Multilateral Master Military Information Exchange Memorandum of Understanding
CJMIEA	Combined Joint Military Information Exchange Annex
CMA	Certificate Management Authority
CRL	Certificate Revocation List
CRLDP	CRL Distribution Point
CP	Certificate Policy
CPMCG	CP Mapping Criteria and Guidance
CPS	Certificate Practice Statement
DN	Distinguished Name
DoD	Department of Defense
DND	Department of National Defence
DSA	Directory Service Agent
EG	Executive Group
EoI	Evidence of Identity
ESS	Enhanced Security Services
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSec	Internet Protocol Security
ITU-T	International Télécommunications Union – T Sector
LDAP	Lightweight Directory Access Protocol
MMHS	Military Message Handling System
MoD	Ministry Of Defence
MSAB	Multinational Security Accreditation Board
NAEC	National Accreditation Endorsement Certificate
NSA	National Security Authority
NDPKI	National Defence PKI
NIPRNET	Unclassified but Sensitive Internet Protocol Network
NZDF	New Zealand Defence Force
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509)
PKE	Public Key Enabled

PMA	Policy Management Authority
PMO	Program Management Office
POC	Point of Contact
RFC	Request for Comments
RO	Registration Officer
RSA	Rivest, Shamir, Adleman (encryption algorithm)
SHA	Secure Hash Algorithm
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Socket Layer
SW	Software
TA	Trusted Agent
TF	Task Force
TLS	Transport Layer Security
VPN	Virtual Private Network

C GLOSSARY

Access	Ability to make use of any information system (IS) resource.
Access control	Process of granting access to information system resources only to authorised users, programs, processes, or other systems.
Accreditation	Formal declaration by an authority that a system is approved to operate in a particular security Mode using a prescribed set of safeguards at an acceptable level of risk.
Applicant	The Subscriber is sometimes also called an “applicant” after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.
Approved	The approval authority for a NDPKI-is the PMA:
Archive	Long-term, physically separate storage.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Audit data Audit log	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes during an event.
Authentication	Verification of the identity claimed by an entity.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.
Biometric	A physical characteristic of a person.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate’s trustworthiness, and may also provide additional attribute information for the subject certificate.
Certification Authority (CA)	An authority trusted by one or more users to create and assign certificates.
CA facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.

Certificate Management Authority (CMA)	A Certification Authority (CA) or Registration Authority (RA). If the NDPKI implements a Certificate Status Authority, it also is a CMA.
CA server	The equipment used in the process of issuing and revoking certificates. Part of the CA facility.
Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it.
Certificate-related information	Information, such as a Subscriber's postal address, that is not included in a certificate, but that may be used by a CA in certificate management.
Client (application)	A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server.
Compromise	Disclosure of information to unauthorised persons, or a violation of the security policy of a system in which unauthorised intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
Confidentiality	Assurance that information is not disclosed to unauthorised entities or processes –not to be confused with concept of classification "CONFIDENTIAL".
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
Crypto period	Time span during which each key setting remains in effect.
Dual use certificate	A certificate that is intended for use with both digital signature and data encryption services.
Encryption certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. The process of storing, protecting and escrowing the private component of the key pair associated with the encryption certificate is sometimes referred to as key management.

Firewall	Gateway that limits access between networks in accordance with local security policy.
Integrity	Protection against unauthorised modification or destruction of information.
Intellectual property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
Intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
Key escrow	The retention of the private component of the key pair associated with a Subscriber's encryption certificate to support key recovery.
Key exchange	The process of exchanging public keys (and other information) in order to establish secure communication.
Key generation material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Level 1 CA	A CA directly subordinate to the Root CA
Local Registration Authority (LRA)	A type of Registration Authority with responsibility for a local community.
Naming authority	An organisational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
NDPKI	National Defence/Defense Public Key Infrastructure
Non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data.
OCSP Responder	A trusted entity that provides on-line revocation status of certificates to Relying Parties. The OCSP Responder is either explicitly trusted by the Relying Party or through a CA that Relying Party trusts, or through the CA that issued the certificate whose revocation status is being sought.
Outside threat	An unauthorised entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.

Physically isolated network	A network that has no electronic connection to individuals outside a physically controlled space.
PKI Sponsor	Fills the role of a Subscriber for non-human system components or organisations that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this document.
Policy Management Authority (PMA)	Policy Management Authority. Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.
Privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	Entity responsible for identification and authentication of certificate subjects and subsequently issuing an authorised certificate request.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
Relying Party	A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates.
Risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
Risk tolerance	The level of risk an entity is willing to assume in order to achieve a

	potential desired result.
Server	A system entity that provides a service in response to requests from clients.
Signature certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
SSL	Secure Sockets Layer. Proprietary secure communications protocol widely used in COTS products. Version 3 of the protocol is a subset of TLS version 1.0.
Subordinate CA	In a hierarchical PKI, a CA whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA. (see superior CA)
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate.
Superior CA	In a hierarchical PKI, a CA who has certified the certificate signing key of another CA, and who constrains the activities of that CA. (see subordinate CA)
System equipment configuration	A comprehensive accounting of all system hardware and software types and settings.
System high	The highest security level supported by an information system.
Technical non-repudiation	The contribution public key mechanisms make to the provision of technical evidence supporting a non-repudiation security service.
Threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service.
TLS	Transport Layer Security. Standard secure communications protocol supporting application-to-application security.
Trust list	Collection of Trusted Certificates used by relying parties to authenticate other certificates.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in Trusted Certificates are used to start certification paths. Also known as a “trust anchor”.

Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
Two person control	Continuous surveillance and control of positive control material at all times by a minimum of two authorised individuals, each capable of detecting incorrect and/or unauthorised procedures with respect to the task being performed and each familiar with established security and safety requirements.
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorisations granted to the subject, are changed by issuing a new certificate.
Validation Authority	That part of the CMA responsible for confirming the status of a certificate (via OCSP) or providing access to CRLs.
Zeroise	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.