Public Key Infrastructures (PKI) Cross-Certification Between Combined Communications-Electronics Board (CCEB) Nations

ACP 185

NOVEMBER 2011

FOREWORD

1. The Combined Communications-Electronics Board (CCEB) is comprised of the five member nations, Australia, Canada, New Zealand, United Kingdom and United States and is the sponsoring authority for all Allied Communications Publications (ACPs). ACPs are raised and issued under common agreement between the member nations.

2. ACP 185, PUBLIC KEY INSFRASTRUCTURES (PKI) CROSS-CERTIFICATION BETWEEN COMBINED COMMUNICATIONS-ELECTRONICS BOARD (CCEB) NATIONS is an UNCLASSIFIED CCEB publication.

3. This publication contains Allied military information for official purposes only.

4. It is permitted to copy or make extracts from this publication.

5. This ACP is to be maintained and amended in accordance with the provisions of the current version of ACP 198.

THE COMBINED COMMUNICATIONS-ELECTRONICS BOARD LETTER OF PROMULGATION

FOR ACP 185

1. The purpose of this Combined Communications-Electronics Board (CCEB) Letter of Promulgation is to implement ACP 185 within the Armed Forces of the CCEB Nations. ACP 185, PUBLIC KEY INSFRASTRUCTURES (PKI) CROSS-CERTIFICATION BETWEEN COMBINED COMMUNICATIONS-ELECTRONICS BOARD (CCEB) NATIONS, is an UNCLASSIFIED publication developed for Allied use under the direction of the CCEB Principals. It is promulgated for guidance, information and use by the Armed Forces and other users of military communications facilities.

2. ACP 185 is effective upon receipt for CCEB Nations. NATO Military Committee (NAMILCOM) will promulgate the effective status separately for NATO nations and Strategic Commands.

EFFECTIVE STATUS

Publication	Effective for	Date	Authority
ACP 185	CCEB	On Receipt	LOP

3. This ACP will be reviewed periodically as directed by the CCEB Permanent Secretary.

4. All proposed amendments to the publication are to be forwarded to the national coordinating authorities of the CCEB or NAMILCOM.

For the CCEB Principals

Paul Foster

PA FOSTER
Major, RCAF
CCEB Permanent Secretary

RECORD OF MESSAGE CORRECTIONS

Identification of Message Correction and Date Time Group (DTG)		Date Entered	Entered by (Signature, Name, Rank, Grade or Rate and Name of Command)
DTG	Correction		

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

PURPOSE

101. Allied Communications Publication (ACP) 185 - PKI Cross-Certification Between CCEB Nations establishes the framework for PKI interoperability to facilitate the cross-certification of CCEB National Defence/Defence Public Key (NDPKI). It defines the minimum set of standards which each PKI needs to meet and the processes and activities that each CCEB Nation needs to conduct prior to cross-certification, and, in order to maintain cross-certification.

102. This framework serves to describe a common approach to authentication within CCEB environments. Provided that each Nation meets the minimum standards listed in Annex A, each Nation can use their own processes to perform identity proofing and credentialing for their employees and affiliates, while relying on identity proofing and credentialing performed by other nations for their employees and affiliates. Although not mandated by this framework, the issuance of cross-certificates between NDPKIs is the preferred technical approach for implementing formal and reciprocal recognition of trust between the NDPKIs of two CCEB Member Nations.

SCOPE

103. This ACP applies to all CCEB NDPKIs that seek to or have established mechanisms to interoperate with another CCEB NDPKI at the Secret or below level environment under the Combined Joint Multilateral Master Military Information Exchange Memorandum of Understanding (CJM3IEM). It may be used by other non CCEB nations for information purposes. In no way does it imply that this will be employed as a basis for cross-certification outside of CCEB partners.

NATURE OF THE CROSS-CERTIFICATION ARRANGEMENT

104. This ACP provides a framework for bi-lateral PKI interoperability. Self-assertion to the requirements described in Annex A does not automatically result in interoperability across the CCEB. Each participating nation must establish a Cross-Certification Arrangement (CCA) with all other participating nations they wish to interoperate with as the arrangements are not transitive[1].

105. In addition, a CCA allows individuals with certificates from one NDPKI to authenticate to relying party information systems hosted by the other NDPKI. However, it is not an authorization arrangement and is not intended to supplement or replace any

[1] For example, if Nation A establishes a CCA with Nation B, and Nation B establishes a CCA with Nation C, there is no arrangement between Nation A and Nation C as a result.

existing policies for access to a Nation’s information. Access to specific information is at the discretion of the Nation. Information owners may also choose to impose additional requirements.

CHAPTER 2

CERTIFICATE POLICY MAPPING CRITERIA

OVERVIEW

201. Certificate Policies (CP) under which Certification Authorities (CA) are established and operate can vary as well the requirements for creating and managing certificates. Differences, if not known and managed, can introduce risks to entities exercising a CCA. Determining comparability and equivalence between CCEB National Defence certificate policies, is critical prior to moving forward with the cross-certification of PKIs.

BASELINE REQUIREMENTS

202. The CCEB Nations have agreed to a minimum set of standards that all NDPKIs must meet. This minimum set of standards is known as the CP Mapping Criteria (CPMC) and can be found in Annex A of this document. All PKI certificates issued by interoperable CCEB NDPKIs will be based on the Internet Engineering Task Force (IETF) Request for comments (RFC) 5280.

SELF-ASSERTION

203. Each CCEB nation will compare their CPs against the mapping criteria found in Annex A and confirm their compliance or equivalence to the requirements and any stated guidance listed therein. This process is called self-assertion.

RECORDING AND DISTRIBUTING RESULTS OF THE SELF-ASSERTION

204. The NDPKI Policy Management Authority (PMA) will notify the PMA's of each CCEB NDPKI when they have completed their self-assertion and will make available the formal self-assertion to the NDPKI PMA that they plan to/or are cross-certified with. Additionally where a criterion in relation to the CPMC cannot be met entirely the NDPKI PMAs involved shall reach an agreement on the resolution of non-conformance. Such agreement will be documented and be made available to the other Participant of the bi-lateral cross-certification.

FREQUENCY OF SELF-ASSERTION

205. A CCEB nation is required to complete a self-assertion prior to entering into any CCA with another CCEB nation or issuing a cross-certificate from their NDPKI to another CCEB NDPKI. After the initial self-assertion, each NDPKI PMA in a bi-lateral arrangement shall revalidate the self-assertion on an annual basis and shall share the results with the other NDPKI PMA in the bilateral arrangement. Additionally, NDPKI PMAs shall reassert compliance against the CPMC when an applicable NDPKI CP is amended and shall notify the other NDPKI PMA if any areas of non-compliance have

arisen as a result of modifications to their CP. Nations are also encouraged to notify the other NDPKI PMA of changes in status of previously non-compliant areas.

206. Each Participant will notify the other Participant immediately of any change it proposes to make to any part of its PKI that could have implications for interoperability between the Participants or affect the CCAs, including the intention to cross-certify with another CCEB nation, changes to algorithms or a decision to revoke the certificate of any applicable CA in the NDPKI. That Participant will notify the other Participant to enable it to assess the consequences and take any necessary action. The Participant shall also update the self-assertion based on these changes.

CHAPTER 3

TECHNICAL INTEROPERABILTY TESTING

OVERVIEW

301. Prior to cross-certification of two NDPKIs, interoperability testing shall be conducted to analyse and validate the PKIs of the two CCEB partners so that standards compliance is ensured and to assess that basic PKI services perform as expected across multiple international domains and repositories.

INTRODUCTION

302. Technical interoperability activities between CCEB nations are intended to test cross-certificate path building and validation in a test environment prior to bilateral cross-certification between the operational CAs of the two NDPKIs. Subsequent testing will focus on establishing stable configurations to support common applications.

PREREQUISITES

Test Infrastructure

303. Each CCEB Nation Participant shall have or establish a test infrastructure that is representative of their operational environment and is able to issue certificate requests, issue certificates, sign certificates, revoke certificates and provide the capability for partners to validate issued certificates.

Certificate Profiles

304. Certificate profiles shall be exchanged among the CCEB Nation Participants that address the population, or non-population, of the fields and extensions listed below to enable correct path discovery and validation:

- Policy Object Identifiers (OID)
- Policy OID mappings
- Cryptographic Algorithms
- Name constraints
- Policy constraints
- Basic constraints
- Key usage and extended key usage
- Authority Information Access (AIA)
- Subject Information Access (SIA)
- Subject name

- Subject alternative names
- Certificate Revocation List (CRL) Distribution Point (CRL DP)
    - Monolithic and partitioned CRLs
    - Local and remote On-Line Certificate Status Protocol (OCSP) service

PROCESS

Preliminary Technical Testing

305. It is recommended that prior to the commencement of any bilateral testing that nations perform some level of preliminary evaluation of their NDPKI's technical ability to support cross-certification.

306. The Test Infrastructure should be used to generate cross-certificates. It is recommended that each CCEB Nation checks that they are able to validate end entity certificates that are representative of certificates that would be issued by the other nation[2]. These tests can be conducted in an offline manner if required.

Technical Testing

307. It is mandatory that bilateral testing includes deeper level technical testing that expands on the preliminary technical testing that each nation should have performed earlier. These tests require connectivity between the two nations' Test Infrastructures. The testing should include:

- Ability to retrieve CRLs
- Ability to access revocation information through OCSP, if applicable
- Ability to retrieve a certificate chain using the AIA extension
- Ability to retrieve a certificate chain using the SIA extension, if applicable
- Assessment of any impact on certificate paths as a result of name constraints in cross-certificates and CA certificates
- Discovery and validation of all possible trust paths from the end entity certificates to the root, including testing for unintended trust.

Functional testing

308. It is recommended that the two nations perform functional testing that is representative of the expected use cases for cross-certification. These tests require connectivity between the two nations' Test Infrastructures. The two nations shall agree to the extent of the testing prior to commencing testing. The testing may include:

[2] It is recommended that the PKI Interoperability Test Tool (PITT) is used for deeper level validation of certificates. http://pkif.sourceforge.net/pitt.html

- Web server authentication
- Digitally signed email
- Encrypted email
- Smartcard login

Dry run of the Cross-certification signing ceremony

309. It is recommended that the two nations perform dry run testing of the cross-certification signing ceremony using the national Test Infrastructures. This may include:

- Generation of the cross-certificate requests
- Verification of the integrity of the cross-certificate requests upon receipt
- Generation of the Principal Cross-Certificate
- Understanding of roles and responsibilities related to the cross-certificate signing ceremony

Interoperability CA testing

310. Each CCEB Nation is expected to perform internal testing on the CA that will be used for CCEB Interoperability as part of the process of deploying the operational CA. These tests should align with the relevant self-assertions made in relation to the NDPKI CPs against the CPMC.

Operational testing

311. After the generation of a cross-certificate in the operational environment, one or more certificate chains that include the newly generated cross-certificate should be validated to ensure that cross-certification was successful.

REASONS FOR RE-TESTING

312. After a CCA is operational, changes to the configuration of a NDPKI may warrant re-testing. Re-testing should occur prior to the implementation of the configuration change, but may occur post implementation if prior testing is not possible. Re-testing may be initiated by the Nation making the change or may be requested by the other Participant in response to an update to the CCA or self-assertion. Types of changes that will likely require re-testing include:

- Establishment of a CA used for interoperability by the NDPKI
- Changes to algorithms used for hashing, encryption, or key agreement
- Changes to applicable CAs or end entity certificate profiles

CHAPTER 4

CROSS-CERTIFICATION ARRANGEMENT

OVERVIEW

401. Each bi-lateral cross-certification is supported by a CCA which is executed prior to establishing interoperability with CCEB NDPKIs. The CCA outlines the roles and responsibilities of each CCEB Nation in providing security services based upon PKI technology to enable and facilitate the exchange of authenticated Military Information and Data under the CJM3IEM.

SCOPE

402. The CCEB Nations that are participating in a bi-lateral cross-certification of one CCEB NDPKI with another must develop and execute a CCA before operational cross-certificates are issued. There is a one to one relationship between CCA's and bi-lateral cross-certifications. The cross-certification and reliance upon the cross-certificate are limited to the support of communications and information exchange between the Participants through their officials and employees, military personnel, and authorised eligible contractors for Military Information and Data exchange purposes in accordance with the CJM3IEM.

CCA CONTENT

403. The CCEB Nations that are parties to a CCA must state their agreement that they will use the policies, processes, and procedures described in this ACP to achieve and maintain PKI interoperability with one another. The CCA shall also cover the following key areas: limitation of communications; levels of assurance and object identifiers of NDPKI; detailed responsibilities of each CCEB nation that is a Participant to the CCA; effective period of the CCA; financial responsibilities imposed by the CCA; liability; security handling; and termination.

404. If one or both of the Participants to the CCA have procedural or technical considerations regarding PKI operations beyond those specified in Annex A, these considerations should also be included in the CCA, along with the ability of the other Participant to address the considerations.

405. Schedules shall be used in the CCA to document the following CCEB Nation specific items:

- Version details for the CP and Certificate Practice Statement
- List the policy identifiers (OIDs) that shall be mapped in the cross-certification and levels of assurance
- PKI architecture and operation details including CRL issuance frequency, latency, and publication
- Non-conformances for each NDPKI in relation to the CPMC
- Use of group and role based certificates
- If applicable, the parameters regarding the use of anonymous certificates
- Face to face authentication outside of bounds required

CCA TEMPLATE

406. A template for a CCA can be found in Annex B. If the language (outside of substituting the CCEB Nation called out) is not used verbatim from the template, CCEB nations need to ensure that the intention of all of the statements listed in the template are covered in their CCA's. It is recommended that each NDPKI legally review and confirm the prepared CCA prior to entering the CCA.

CCA SIGNATORY AUTHORITY

407. Each NDPKI PMA will determine the signatory authority required to execute the CCA and advise the other Participant of the relevant authority. The respective Participant shall validate the designated representative's authorization to act on behalf of the other NDPKI.

CHAPTER 5

ALGORITHM TRANSITION SYNCHRONIZATION

INTRODUCTION

501. National policies, mission needs, risks, application compatibility and funding are just some of the topics that can influence when a CCEB partner might transition to stronger key sizes or algorithms. Lack of algorithm synchronization amongst interoperable NDPKIs may present challenges and cause problems by limiting or eliminating access to some critical CCEB partner networks and systems that require PKI-based authentication, even if a partner previously had access.

502. Algorithm alignment must be continuously managed to ensure interoperability. Algorithms may be changed as a result of the following:

- The algorithm has been found to be subject to an unacceptable security vulnerability
- The National Security Agency for a Nation may declare an algorithm to be at the end of its useful life because of potential security vulnerabilities
- The algorithm has reached the end of its useful life based on support for the algorithm in off the shelf products
- In response to regular infrastructure upgrades

503. Because the selection of algorithms and the introduction of new algorithms can have a significant impact to interoperability, changes to algorithms used by an NDPKI must be coordinated with the other participating Nations.

BACKGROUND

504. PKIs use cryptographic algorithms for authentication to systems, signing information and data confidentiality. The choice of algorithms by the PKI may impact whether a specific user application can make effective use of certificates and keys. The choice of algorithm and key size also impacts the level of assurance that can be provided in a certificate of the PKI. Weaker algorithms/smaller key sizes are less secure against attacks. However, while a PKI can unilaterally change algorithms, user applications have to support the algorithms or the certificates issued by the PKI with those stronger algorithms will not work in the user environment. If the PKI issues certificates or other artefacts (e.g., CRLs) using algorithms not supported by the applications of a Participant nation, applications that rely on the cross-certified NDPKIs will fail. Conversely, if NDPKIs do not transition to stronger algorithms and key sizes, they provide less assurance over time and systems may block them from access.

505. There are three classes of algorithms typically used in PKI - hashing, encryption, and key agreement. Hashing and encryption are used for authentication and digital signature. Either an encryption or key agreement algorithm is used for data encryption. Additionally, encryption and key agreement algorithms may use different key sizes.

ALGORITHM COORDINATION

506. As algorithms deprecate, Participant nations are to review the level of assurance asserted in the CCA and notify the other Participant of any change it proposes to make in relation to OID mappings.

507. In addition, Nations are required to declare in advance their intent with regards to algorithm migrations to provide the opportunity for all Nations to prepare for the potential change. This declaration should include a timeline for the transition, including the period of time where multiple algorithms (old and new) will be used and accepted by the Nation's PKI and relying parties. If possible, the declaration should also include known or anticipated interoperability impacts.

CHAPTER 6

PROCESS FOR CROSS-CERTIFICATION

INTRODUCTION

601. Cross-certification is the preferred mechanism for formal and reciprocal recognition of trust between the NDPKIs of two CCEB Member Nations. Once the two NDPKIs have completed interoperability testing and signed a CCA, the generation, exchange and signing of principal cross-certificates is achieved through a formally managed process known as a Cross-certification signing ceremony.

602. The process for generating, exchanging and signing principal cross-certificates is outlined below. A cross-certification signing ceremony template can be found at Annex C. CCEB nations may modify the template to suit their individual cross-certification requirements.

603. The goal is for the cross-certified community to be able to trust that the procedures involved were executed correctly, and that the private key materials are stored securely. Security of the private key is important because it ensures that any signature made by that key is known to originate from a legitimate key ceremony, and not by an untrusted third party.

604. For the initial generation and signing of principal cross-certificates, at least one authorised representative from both CCEB Member Nations is required to act as a witness[3] at the Cross-Certification Signing Ceremony. The generation and signing of subsequent principal cross-certificates between two NDPKIs will be at the discretion of each nation through an agreed secure mechanism. Participants will determine if authorised representatives from both nations are required to witness subsequent Cross-Certification Signing Ceremonies.

PROCESS

605. Nations will mutually agree to the process for generation and delivery of the cross-certificate request (CSR) and signing and publication of Principal Cross-Certificate.

606. The following outlines an indicative process for the generation, exchange and signing of principal cross-certificates.

[3] The role of the witness is to confirm that the certificate details conform to the authorised certificate policy. Witnesses must sign statements to attest that the cross certification signing ceremony proceedings have been carried out correctly.

607. Generation and transport of the certificate signing request

- The NDPKI operating the CA to be cross-certified will arrange for the generation of the principal cross-certificate request at a mutually agreed date and time. At least two persons will act as witnesses of the generation of the certificate request. The Nation that will sign the cross-certificate request may have a representative at the generation
- The principal cross-certificate request will be generated in an agreed file format
- Authorised witnesses will record the requesting CA's thumbprint, e.g. a hash of its public key
- The request is saved to a media or application suitable for transportation (e.g. on a CD)
- The request is safe handed[4] to authorised national representatives of the other CCEB Member Nation
- The request is delivered to the cross-certifying NDPKI environment

608. Signing and publishing the principal cross-certificate

- Prior to signing the request, the cross-certifying NDPKI CA checks that the request has not been tampered with, by verifying the CAs thumbprint on the request file
- After checking that the request has not been tampered with, the principal cross-certificate is signed by the applicable cross-certifying CCEB Member Nation CA
- The principal cross-certificate is returned to the originating CCEB Member Nation by a mutually agreed secure mechanism (e.g. safe hand)
- The principal cross-certificate will be published to a location where it is accessible by Relying Parties (i.e. Subscribers) of the cross-certified NDPKI

Note: The indicative process described above is a one way process, i.e. the trust is one way. The process will need to be repeated with roles reversed for mutual trust.

[4] Alternatively by any mutually agreed secure method.

CHAPTER 7

GOVERNANCE and CHANGE CONTROL

DOCUMENT MAINTENANCE

701. This document shall be subject to the normal CCEB staffing process for ACPs, but as a minimum the ACP is to be reviewed every two years or when required to ensure that it remains consistent with CCEB national policies and evolving technologies. Suggestions for amendments should be forwarded through normal channels to the CCEB Washington Staff (WS).

702. This document will be subject to the ACP amendment process which provides for major and minor amendments. The major amendment process will be used to change the content or intent of this document and may result in the incorporation of a number of minor amendments resulting in the creation of a new edition to this ACP. Any nation or group can request a major amendment. The minor amendment process will be used to make smaller editorial wording changes, which are not meant to significantly change the intent of this ACP.

X.509 CERTIFICATE POLICY MAPPING CRITERIA (CPMC) INTRODUCTION

The CPMC follows the format of the Internet Engineering Task Force Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Certificate Policy and Certification Practices Framework. The CERTIFICATE POLICY MAPPING CRITERIA (CPMC) was developed based on RFC 3647 and the collective Certificate Policies from each of the representative Combined Communications Electronics Board (CCEB) member nations.

The CPMC states the criteria against which National Defence Public Key Infrastructure (NDPKI) Policy Management Authorities (PMAs) assess their NDPKIs. Each NDPKI PMA shall formally assess their NDPKI CPs against the CPMC and assert compliance. This process is known as self-assertion. The CPMC sets the minimum standards that shall be met. Where a criterion cannot be met entirely, NDPKI PMAs involved shall reach an agreement on the resolution of non-conformance.

1.1 Overview

1.1.1 Certificate Policy (CP)

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

1.2 Document Name and Identification

NDPKI CPs shall be identified using an OID registered in each Nation’s Object ID Registry.

There are three general policies for certificates: Device, Hardware, and Software.

A Device OID shall only be used in cross-certificates which map to a member policy OID that is only for devices.

The Hardware and Software OIDs may be used for certificates issued to people, roles or devices.

The Hardware OID shall only be asserted in a cross-certificate if the member policy OID for the subscriber certificates requires that:

- Keys shall be generated in a hardware cryptographic module. If generated off token, no copies, other than authorized escrowed copies of the private keys associated with Encryption certificates, continue to exist after the generation and insertion process has completed.

- The private key shall never leave the subscriber hardware token once the key is generated/inserted into the subscriber token.
- For encryption certificates – escrowed private keys shall be protected at a level commensurate with the CA private signing key while in escrow.

1.3 PKI Participants

The following are the roles that are expected to be present for the administration and operation of a NDPKI. NDPKI PMAs self-asserting against this CPMC shall document in the Cross-Certification Arrangement (CCA) roles not used within its NDPKI.

1.3.1 Policy Management Authority

Each NDPKI shall have an identifiable body or management structure that is responsible for the NDPKI. This includes responsibility for:

- Establishing, maintaining, and updating the Certificate Policies under which the NDPKI operates
- Monitoring the governance and performance of the NDPKI
- Reviewing and approving the NDPKI CPS(s) of their Certificate Management Authorities (CMA)[5]
- Ensuring independent audits are performed and reviewed in accordance with National guidelines
- Approving the terms for interoperation with other PKIs
- Approving the appropriate mechanisms and controls for the management of the NDPKI
- Authorising the establishment of Certificate Authorities (CA)
- Authorising the establishment of Cross-certification relationships

1.3.2 Certification Authority

A NDPKI CA is an entity authorised by the NDPKI 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 the NDPKI PMA.

A CA may be a single hardware/software component or its functions may be distributed among several components. If distributed, all CA security requirements apply to all of these

Uncontrolled copy when printed

[5] CMAs are CAs and RAs of the NDPKI. If the NDPKI implements a Certificate Status Authority, it also is a CMA

components. In addition, the distribution of CA responsibilities between the CA itself and Registration Authorities (RA) may vary in the implementation of the PKI.

If the NDPKI operates Certificate Status Authorities (CSA) or Key Escrow Servers (KES), all requirements that apply to a CA apply equally to these entities unless specifically excluded.

Collectively the hardware, software, and operating personnel that create, sign, and issue public key certificates to Subscribers is a Certificate Authority System (CAS).

1.3.3 Registration Authority

An RA is an entity authorized by the CAS to collect, verify, and submit information provided by potential Subscribers which is to be entered into public key certificates. The term RA refers to hardware, software, and individuals that collectively perform this function. Unless expressly stated otherwise, RA requirements are imposed on all RA components of the NDPKI. RA operations shall be performed in accordance with a CPS approved by the NDPKI PMA. RA functions may be included in a single CPS, which also governs CAS operations, or may be defined in a separate CPS. The RA is responsible for the following:

- Control over the registration process
- Identification and authentication process

1.3.4 Subscribers

A Subscriber is the entity whose name appears in the Subject field of a certificate, and who asserts that the use of its public key and certificate is in accordance with the NDPKI CP. The Subscriber is sometimes also called an “applicant” after applying to a CAS for a certificate, but before the certificate issuance procedure is completed. Subscribers include entities that have been approved in the NDPKI CP, such as but not limited to:

- Personnel
- Devices (e.g. Workstations, Firewalls, Routers, Trusted Servers, applications, systems and other infrastructure components)
- Organisational roles associated with individuals, groups of individuals or organisational entities

A Subscriber with a certificate issued under a NDPKI does not automatically receive access, authority or privilege to the Defence assets or systems of the cross-certified NDPKI.

1.3.5 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber’s name to a public key. A Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A Relying Party may use information in the certificate (such as CP OID identifiers) to determine the suitability of the certificate for a particular use.

A Relying Party uses a Subscriber's certificate to verify or establish one or more of the following:

- The identity and status of an individual, role, or device
- The integrity of a digitally signed message
- The identity of the creator of a message
- Confidential communications with the Subscriber

Relying Parties may base the reliance they choose to place on a certificate on the factors such as the amount and type of inherent risk of an activity, the consequence of failure, and the use of risk mitigation controls.

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.

1.4 Certificate Usage

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

- Authenticate its identity.
- Digitally sign electronic documents, transactions and communications.
- Encrypt data.

Cross-certificates shall be issued to enable NDPKI Subscribers to release and exchange Military Information and Data under the Combined Joint Multilateral Master Military Information Exchange Memorandum of Understanding (CJM3IEM.)

1.4.1 Appropriate NDPKI Certificate Uses:

Appropriate use of NDPKI certificates shall be as defined in the NDPKI CPs.

1.4.2 Prohibited Certificate Uses

Prohibited use of certificates shall be as defined in the NDPKI CPs.

1.5 Policy Administration

1.5.1 Organisation administering a NDPKI CP

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

1.5.2 Contact Person

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

1.5.3 Person Determining CPS Suitability for the Policy

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

1.5.4 CPS Approval Procedures

All NDPKI CPS(s) shall be approved by their NDPKI PMA.

1.6 Definitions and acronyms

See the GLOSSARY OF TERMS AND ACRONYMS

PUBLICATION & REPOSITORY RESPONSIBILITIES

1.7 Repositories

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

1.8 Publication of certification information

Each NDPKI PMA shall ensure that relevant CA certificates, CRLs and appropriate Subscriber certificates are published to a repository available to Subscribers and Relying Parties. The NDPKI may additionally choose to provide access to an authoritative Certificate Status Authority. Each NDPKI PMA shall ensure Subscribers and Relying Parties are provided with the URL of a public website where their NDPKI CP is publicly available.

Where the CPS contains additional responsibilities and requirements for Subscribers and Relying Parties, the NDPKI PMA shall provide the relevant parties, under such terms and conditions as it shall deem appropriate, all or part of the CPS.

1.9 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 is at 4.9.7 CRL Issuance Frequency.

Details of repository publication timescales and frequency shall be disclosed between parties within the CCA.

1.10 Access controls on repositories

Repository information shall be protected from unauthorized modification or disclosure.

IDENTIFICATION & AUTHENTICATION

1.11 Naming

1.11.1 Types of Names

The NDPKI PMA shall ensure that each entity:

- Shall have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate Subject and Issuer field.
- May be assigned additional names via the subject AltName field.
- The DN shall not be blank.
- Any attribute or name that is encoded as directory string shall be encoded as printable string.
- A Relative Distinguished Name (RDN) is a single component within a distinguished name. Each RDN shall carry a single attribute.
- The appropriate 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.

1.11.2 Need for Names to Be Meaningful

The NDPKI PMA shall ensure that names used to identify NDPKI Subscribers are:

- Meaningful.
- Relate directly to the identity of the Subscriber.
- Meaningfully related to the identity information used to verify the Subscriber as specified in Section 3.2.3.

Each NDPKI root CA shall only sign certificates with subject names from within a name-space approved by the NDPKI PMA. In the case where one CA certifies another, the certifying CA shall impose restrictions on the name space authorized in a subordinate CA, which are at least as restrictive as its own name constraints.

1.11.3 Anonymity or Pseudonymity of Subscribers

A CA shall not issue anonymous Subscriber certificates without the express consent of the NDPKI PMA. If anonymous Subscriber certificates are authorized, the parameters for issuance shall be specified in the CCA. 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. Where pseudonyms are used, a Relying Party shall be able to determine this from the content of the certificate.

1.11.4 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.

1.11.5 Uniqueness of Names

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

1.11.6 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.

1.12 Initial Identity Validation

1.12.1 Method to Prove Possession of Private Key

In all cases, the CA shall establish that the private key corresponding to the public key contained in any request is in the possession, or control of, the entity submitting the certificate request. This may be done by use of any appropriate Proof of Possession algorithm or technique approved for use by the NDPKI PMA.

Each NDPKI PMA shall ensure that policies are established appropriate to the key generation and distribution technologies that it uses.

1.12.2 Authentication of Organisation Identity

Where a NDPKI makes use of group/role identities, or issues certificates to devices, procedures shall be in place to:

- Establish the authenticity of any organisational identity claimed or implied in the identity asserted by a certificate.
- Authenticate the identity of the requestor as specified in Section 3.2.3 or by use of a valid certificate as issued by the NDPKI. The requestor is the PKI Sponsor.
- Validate the authority of the PKI Sponsor to act on the behalf of the organization and make the request for the certificate.

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

1.12.3 Authentication of Individual Identity

The CA shall ensure that a Subscriber's identity is established as required by national policy for the OID specified in the certificate. For first-time registration of human subscribers, the elements of this process shall include, at a minimum:

- A face-to-face identification process.
- A Government issued Photo ID.
- Validation of vetting of the identity.
- For certificates used at a classified level, verification that the named subscriber has an account on a classified network and the appropriate clearance.

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

1.12.4 Non-verified Subscriber Information

All information offered by, or on behalf of, the Subscriber shall be verified. Non-verified Subscriber information shall not be included in certificates.

1.12.5 Validation of Authority

Certificates that contain explicit or implicit organisation affiliation shall be issued only after ascertaining that the Subscriber has the authorisation to act on behalf of the organisation in the implied capacity.

1.12.6 Criteria for Interoperation

Interoperation between NDPKIs is a bi-lateral decision that is formalised in the signing of a Cross-Certification Arrangement (CCA) and the issuance of a signed cross-certificate. The basis for this decision shall be:

- A self-assertion by each nation of compliance with this CPMC;
- Completion of interoperability testing and;
- Completion of negotiations regarding the CCA.

For cross-certification each NDPKI PMA shall validate the designated representative's authorization to act on behalf of the other NDPKI.

1.13 Identification and authentication for re-key requests

1.13.1 Identification and Authentication for Routine Re-key

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 shall periodically obtain keys in accordance with the NDPKI CP.

A request for re-key shall only be made by a Subscriber (or PKI sponsor acting on the Subscriber’s behalf) in whose name the keys have been issued.

For certificates issued in hardware, the entity shall use the valid signature certificate and associated private key stored on the hardware token to authenticate to the CA. The process shall 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 PKI sponsor shall provide proof of possession of its current private key.

Re-key requests for certificates shall be identified and authenticated on the basis of current valid Subscriber certificates. The validity period of the new certificate shall not extend beyond the periodic in-person authentication requirements listed in the table below.

Certificate Type	**In Person Authentication Requirement**
Software	9 Years
Hard Token	6 Years
Device	9 Years

For CA Key Changeover see 5.6 Key Changeover.

1.13.2 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 identity validation. Any change in the information contained in the certificate shall be verified before the certificate is issued.

1.14 Identification and authentication for revocation request

Revocation requests shall be authenticated.

1.15 Identification and Authentication for Key Recovery Request

The identity of the requestor shall be authenticated either in a face to face authentication as specified in Section 3.2.3 or using a digital signature based on a valid certificate with cryptographic strength at least that of the certificate of the key to be recovered.

CERTIFICATE LIFE-CYCLE

1.16 Certificate Application

The applicant and the CMA shall perform the following steps when an applicant applies for a certificate:

- Establish and record the identity of the Subscriber (per Section 3.2);

- Obtain a public/private key pair for each certificate required;
- Establish that the public key forms a functioning key pair with the private key held by the Subscriber (per Section 3.2.1); and,
- Provide a point of contact for verification of any roles or authorizations requested.

These steps may be performed in any order that is convenient for the CMA and Subscribers that does not defeat security; but all must be completed prior to certificate issuance.

1.16.1 Who Can Submit a Certificate Application

The Certificate application shall be submitted to the CA by the Applicant, or the PKI Sponsor or an RA on behalf of the Applicant.

1.16.2 Enrolment Process and Responsibilities

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

1.17 Certificate Application Processing

1.17.1 Performing Identification and Authentication Functions

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

1.17.2 Approval or Rejection of Certificate Applications

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

1.17.3 Time to Process Certificate Applications

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

1.18 Certificate Issuance

1.18.1 CA Actions during Certificate Issuance

The CA shall:

- Authenticate a certificate request.
- Verify whether a certificate request is correctly formed.
- Perform any additional process as specified in the CA CPS.
- Ensure that the public key is bound to the correct Subscriber.
- Obtain a proof of possession of the private key.

- Compose and sign the certificate.
- Provide the certificate to the Subscriber.
- Publish the certificate, as applicable.

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

- Details of the certificate request.
- The success, or rejection (with reason), of the certificate request.
- The identity of the Registration Authority (RA).

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

1.18.2 Notification to Subscriber of Certificate Issuance

A process shall be in place that shall notify the Subscriber that a certificate has been issued and their responsibilities upon acceptance.

1.19 Certificate Acceptance

1.19.1 Conduct constituting certificate acceptance

Use of the certificate constitutes acceptance.

1.19.2 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.

1.19.3 Notification of Certificate Issuance by the CA to other entities

NDPKI shall notify other affected NDPKIs when issuing a cross-certificate.

1.20 Key Pair and Certificate Usage

1.20.1 Subscriber Private Key and Certificate Usage

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

Subscribers shall use keys and certificates in accordance with the NDPKI policies.

The Subscriber shall not use the signature private key after the associated certificate has been suspended, 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.

An NDPKI that supports Role Subscribers shall develop internal policies and procedures for the use of Role Certificates and protection of the associated private keys for its specific operational environment. PKI Sponsors shall maintain a record of individuals with access to the private key of Role certificates at any given date/time.

1.20.2 Relying Party Public key and Certificate Usage

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.

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

1.21 Certificate Renewal

1.21.1 Circumstance for certificate renewal

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

These criteria shall include as a minimum that:

- The current certificate is still valid.
- The new validity period will not extend beyond the usable life of the private keys.

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

1.21.2 Who may request renewal

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

1.21.3 Processing certificate renewal requests

The certificate renewal processes shall be dealt with in accordance with NDPKI CP.

1.21.4 Notification of new certificate issuance to Subscriber

If the Subscriber does not directly participate in the process, the PKI shall notify the Subscriber of the issuance of a new certificate. Where the Subscriber directly participates in the issue of the renewed certificate there is no stipulation.

1.21.5 Conduct constituting acceptance of a renewal certificate

The Subscriber's failure to object to the issuance of the renewed certificate or use of the certificate shall constitute acceptance.

1.21.6 Publication of the renewal certificate by the CA

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

1.21.7 Notification of certificate issuance by the CA to other entities

NDPKI shall notify other NDPKIs when renewing a cross-certificate.

1.22 Certificate Re-Key

1.22.1 Circumstance for certificate re-key

Circumstances for certificate re-key, shall be defined by the NDPKI PMA.

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

1.22.2 Who may request certification of a new public key

Certificate re-key may be requested by the:

- NDPKI PMA.
- Subscriber or the PKI Sponsor
- CMA on behalf of the Subscriber.

1.22.3 Processing certificate re-keying requests

The certificate rekey processes shall be dealt with in accordance with NDPKI CP .

1.22.4 Notification of new certificate issuance to Subscriber

If the Subscriber does not directly participate in the process, the PKI shall notify the Subscriber of the issuance of a new certificate. Where the Subscriber directly participates in the issue of the renewed certificate there is no stipulation.

1.22.5 Conduct constituting acceptance of a re-keyed certificate

The Subscriber's failure to object to the issuance of the rekeyed certificate shall constitute acceptance. Use of the certificate constitutes acceptance.

1.22.6 Publication of the re-keyed certificate by the CA

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

1.22.7 Notification of certificate issuance by the CA to other entities

NDPKI shall notify other NDPKIs when rekeying a cross-certificate.

1.23 Certificate Modification

1.23.1 Circumstance for certificate modification

Circumstances for certificate modification shall be defined by the NDPKI PMA.

If the Subscriber CN or other information that could be used for authorization has changed, that information shall be validated before the certificate is processed.

1.23.2 Who may request certificate modification

Certificate modification may be requested by the:

- NDPKI PMA.
- Subscriber or PKI Sponsor.
- CMA on behalf of the Subscriber.

1.23.3 Processing certificate modification requests

The certificate modification processes shall be dealt with in accordance with NDPKI CP

1.23.4 Notification of new certificate issuance to Subscriber

If the Subscriber does not directly participate in the process, the PKI shall notify the Subscriber of the issuance of a new certificate. Where the Subscriber directly participates in the issue of the modified certificate there is no stipulation.

1.23.5 Conduct constituting acceptance of modified certificate

The Subscriber's failure to object to the issuance of the modified certificate or use of the certificate shall constitute acceptance.

1.23.6 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.

1.23.7 Notification of certificate issuance by the CA to other entities

NDPKI shall notify other NDPKIs when modifying a cross-certificate.

1.24 Revocation & Suspension

1.24.1 Circumstances for Revocation

A certificate issued to a Subscriber shall be revoked:

- Upon suspected or known compromise of the private key.
- Upon suspected or known loss or compromise of the media holding the private key.
- When a Subscriber or CA server fails to comply with obligations set out in the NDPKI CP, the relevant CPS, or any other agreement or applicable law.
- When the identity or other attributes asserted in the certificate becomes invalid (e.g. following termination of affiliation or employment).

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, all certificates authorised by directly, or indirectly, chaining back to that compromised key shall be revoked.

1.24.2 Who Can Request Revocation

Who can submit certificate revocation requests shall in accordance with the NDPKI CP.

1.24.3 Procedure for Revocation Request

All certificate revocation requests shall be processed and authorised in accordance with the NDPKI CP.

1.24.4 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.

In exceptional circumstances, the CMA may delay revoking the certificate.

1.24.5 Time within which CA must Process the Revocation Request

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

1.24.6 Revocation Checking Requirements for Relying Parties

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

1.24.7 CRL Issuance Frequency

Subordinated CAs shall issue, and publish, an up to date CRL at intervals not exceeding 24 hours. Interoperability CAs shall issue, and publish, an updated CRL at intervals not exceeding 31 days.

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

If a CA signing or cross-certificate is revoked, the revoking CA shall issue a new CRL immediately.

1.24.8 Maximum Latency for CRLs

In order to ensure that Relying Parties may obtain a current, valid CRL, the time indicated in the nextUpdate field of the CRL shall be past the time indicated in the thisUpdate field by a minimum of the latency indicated; and not past the time indicated in the thisUpdate by more than the maximum of the latency indicated in the following table:

Subordinate CAs

- Minimum: issuance frequency + 4 hours
- Maximum: issuance frequency + 6 days

Interoperability CAs

- Minimum: issuance frequency + 1 day
- Maximum: issuance frequency + 7 days

1.24.9 On-line Revocation/Status Checking Availability

A NDPKI may implement a Certificate Status Authority that provides on-line certificate status. If provided, the service shall function in a manner that ensures that:

- Accurate and up-to-date information from the authorized CA is used to provide the revocation status.
- Revocation status responses provide authentication and integrity services commensurate with the assurance level of the certificate being checked.

1.24.10 On-line Revocation Checking Requirements

See Section 4.10.

1.24.11 Other Forms of Revocation Advertisements Available

Other forms of revocation advertisement may be used. If used, the form shall provide commensurate levels of authentication, integrity and timeliness as CRLs.

1.24.12 Special Requirements Related to Key Compromise

No stipulation.

1.24.13 Circumstances for Suspension and Restoration

CAs may support certificate suspension and restoration.

1.24.13.1 Circumstances for Suspension

For CAs that support suspension, a certificate shall be suspended when there is reason to believe that the binding between the subject and the subject's public key defined within a certificate is not currently valid; or there is reason to question the security of the private key, but additional research is necessary to fully determine the status.

Examples of circumstances that may lead to certificate suspension are:

- The Subscriber for the certificate has misplaced the token containing the private key associated with the certificate, but believes that the token is in a protected location;
- The PKI Sponsor is known or believed to have the token containing the private key associated with the certificate, and fails to appear at an expected duty location.

1.24.13.2 Circumstances for Restoration

For CAs that support suspension, a suspended certificate may be restored when the binding between the subject and the subject's public key defined within a certificate is determined to still be valid or the question of the security of the private key is resolved and there was no compromise of the private key.

Examples of circumstances that may result in certificate restoration are:

- The Subscriber who previously reported a certificate token misplaced returns and verifies current possession of the token, that the token was where the Sponsor expected it to be and there is no evidence of tampering;
- The Subscriber returns to duty in possession of the token and verifies it was always under appropriate control.

1.24.14 Who can Request Suspension and Restoration

1.24.14.1 Who Can Request Suspension

Subscribers and PKI Sponsors shall be authorized to request suspension of their own certificates. Any member of the Subscriber's or PKI Sponsor's chain of command is authorized to request suspension of certificates.

1.24.14.2 Who Can Request Restoration

Subscribers and PKI Sponsors may request restoration of their own certificates.

The party that requested suspension of the certificate is authorized to request restoration by providing a reason for the restoration to an RA through an authenticated mechanism.

Other parties may request restoration of certificates by providing a reason for the restoration to an RA through an authenticated mechanism. The RA shall validate the authority of the requestor to make the restoration request before restoring the certificate.

1.24.15 Procedure for Suspension and Restoration Requests

1.24.15.1 __Procedure for Suspension Request__

Any format that is used to request a suspension shall identify the certificate to be suspended, explain the reason for suspension, include an estimated time for the resolution of the suspension, and allow the request to be authenticated (e.g., digitally or manually signed). Digital authentication shall use a certificate at the same or higher assurance level as the certificate to be suspended.

Prior to approving a certificate suspension, the RA shall verify the suspension request, which includes authenticating the identity of the requestor and verifying the requestor’s authority to request revocation and the validity of the reason for the suspension request. Once approved by the RA, the CA shall mark the certificate as suspended. The issuing CA shall place the certificate’s serial number on a CRL, or any other revocation or suspension mechanisms used.

1.24.15.2 __Procedure for Restoration Request__

Only a certificate which is suspended can be restored; a certificate which has been revoked shall remain on the CRL until the certificate expires.

Any request for a restoration shall identify the certificate to be restored, explain the reason for restoration, and allow the request to be authenticated (e.g., digitally or manually signed). The RA shall validate all restoration requests to ensure that they have appropriate justification, are requested by an authorized entity, and are authentic. Suspended certificates shall not be used as the basis for restoration.

The CA shall restore the certificate by removing its serial number from the next CRL. The CA shall also restore the certificate to an un-revoked state in any other revocation or suspension mechanisms used.

1.24.16 Limits on Suspension Period

Suspended certificates shall be periodically reviewed to determine if the reason for suspension remains valid. The RA that approved a suspension request shall review suspended certificates monthly or at the time specified in the suspension request, whichever is shorter. The RA shall revoke any certificate that has not been restored or for which the time limit has expired and the requestor has not submitted a valid extension request.

1.25 Certificate Status Services

Certificate Status Services are provided by CSAs. CSAs are not a required component of the NDPKI. If supported as part of the NDPKI, the CSA is considered an integral part of the CAS and, except where expressly noted, all requirements imposed on CAS apply.

1.25.1 Operational Characteristics

A CSA shall meet the following requirements:

- The CSA shall be operated in compliance with this CP and any applicable Internet standards.
- Information exchanged between the CA and the CSA shall be authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the certificates being issued.
- Accurate and up-to-date information from the associated CA shall be used to provide the revocation status.
- Revocation status responses shall provide authentication and integrity services commensurate with the requirements of the data to be protected by the certificates being issued, to include the status of the certificate and the time the status indication was generated.
- Latency of certificate status information shall meet or exceed the requirements for CRL issuance stated in Section 4.9.7.

1.25.2 Service Availability

No stipulation.

1.25.3 Optional Features

No stipulation.

1.26 End of Subscription

As defined in the NDPKI CP.

1.27 Key Escrow & Recovery

The NDPKI may support key escrow and recovery for private keys associated with encryption certificates.

1.27.1 Key Escrow

1.27.1.1 Circumstances for Key Escrow

Private keys associated with encryption certificates may be escrowed prior to certificate issuance. Private keys associated with certificates that assert digitalSignature shall never be escrowed.

1.27.1.2 Escrowing Keys

Escrowed keys shall be stored in a KES. All requirements (e.g., Section 6.1.2, Section 6.2.6) for storage and transfer of private keys shall apply to the process of escrowing private keys.

1.27.1.3 Notification of Key Escrow to Subscriber

Where applicable, as part of the enrolment process, all subscribers shall be notified that the private keys associated with their encryption certificates will be escrowed.

1.27.1.4 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

1.27.2 Key Recovery

At all times, escrowed keys shall be protected against disclosure to any party except the requestor and the trusted roles responsible for the recovery.

1.27.2.1 Circumstances for Key Recovery

Escrowed keys may be recovered to support the recovery of encrypted data for business, law enforcement or other requirements. In general, escrowed keys are recovered for the following purposes:

- The original copy of the escrowed key has been lost or damaged and the Subscriber cannot access data encrypted with the corresponding public key.
- The certificate is to be re-keyed and the earlier issued private keys are recovered to be included on the token containing the re-keyed certificate.
- An authorized third party (i.e., a person other than the Subscriber or PKI Sponsor) requires access to data encrypted with the corresponding public key.

1.27.2.2 Who May Request Key Recovery

The Subscriber or PKI Sponsors may request recovery of their own escrowed keys. An RA may request initiation of the recovery of escrowed keys as part of a re-key process. Key recovery may also be requested by the following National third parties:

- Subscriber or PKI Sponsor’s manager, Information System Security Officer, supervisor, or superior officers.
- Law enforcement or counterintelligence agents.
- Agents of a Court system with jurisdiction over the NDPKI.
- Any person or organization authorized by the NDPKI PMA via an authenticated communication.

1.27.2.3 Processing Key Recovery Requests

The KES may act on a key recovery request from the Subscriber or the PKI Sponsor acting on behalf of the Subscriber or from a single RA as part of a RA authenticated process to rekey a Subscriber hardware token. In all other cases, the KES shall require authentication by two individuals holding trusted roles prior to releasing the private key.

The RA shall authenticate to the KES using a mechanism commensurate with the cryptographic strength of the strongest key stored in the KES.

All copies of recovered keys shall be continuously protected using mechanisms at least commensurate with the level of the data the key provides access to or protects.

1.27.2.4 Notification of Key Recovery to the Subscriber

When executing a key recovery based solely on a request authenticated by the Subscriber or the PKI Sponsor acting on behalf for the Subscriber, the KES shall send an email to the requestor at an address in authorized repository. If there is no address, the request is rejected.

There is no requirement to notify the Subscriber of key recovery operations executed directly by an RA.

1.27.2.5 Notification of Key Recovery by the CA to Other Entities

No Stipulation.

FACILITY MANAGEMENT & OPERATIONS CONTROLS

1.28 Physical Controls

Physical security controls shall be implemented that protect the CMA hardware and software from unauthorized use and shall be operated in accordance with the National Defence security regulations and procedures. CMA cryptographic modules shall be protected against theft, loss, and unauthorized use.

1.28.1 Site Location and Construction

The location and construction of the facility that will house CMA equipment and operations shall be in accordance with National Defence security regulations and procedures and local policy for protecting information of the same value or classification as the material that will be protected by the public key certificates issued or managed there.

1.28.2 Physical Access

Physical access to NDPKI CAs shall be allowed only when at least two trusted role personnel are present. The CA facility shall be manually or electronically monitored for unauthorized intrusion at all times.

Removable cryptographic modules, activation information used to access or enable cryptographic modules, and other sensitive CA equipment shall be placed in secure containers when not in use. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

A security check of the facility housing the CA equipment or remote workstations used to administer the CAs shall occur if the facility is to be left unattended. At a minimum, the check shall verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "open", and secured when "closed";
- Any security containers are properly secured;
- Physical security systems (e.g., door locks, vent covers) are functioning properly; and
- The area is secured against unauthorized access.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

1.28.3 Power and air conditioning

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

The CA equipment shall have or be provided with sufficient back-up power to execute a standard shutdown (including locking out input, finishing any pending actions, and recording the state of the equipment) before lack of primary power or air conditioning causes the CA equipment to cease functioning.

1.28.4 Water exposures

Water exposure shall be determined in accordance with NDPKI policies.

1.28.5 Fire prevention and protection

Fire prevention and protection shall be determined in accordance with NDPKI policies.

1.28.6 Media storage

Media storage shall be determined in accordance with NDPKI policies for the classification of the media.

1.28.7 Waste disposal

Waste disposal shall be determined in accordance with NDPKI policies for the classification of the waste.

1.28.8 Off-Site backup

The NDPKI PMA shall define procedures for backups sufficient to recover from system failure.

1.29 Procedural Controls

1.29.1 Trusted Roles

The primary trusted roles defined by this policy are the CA, and the RA. The NDPKI CP specifies the other trusted roles to be utilised within the PKI. The names of all persons able to control the operation of PKI equipment or provide access to CA private key authentication components shall be recorded and made available for audit purposes.

1.29.2 Number of Persons Required per Task

See Section 6.2.2.

1.29.3 Identification and Authentication for Each Role

A person occupying a trusted role shall have their 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. For classified networks, the token used by the RA is protected from the class of threats associated with general use within the environment (e.g., a separate token for RA functions.)

1.29.4 Roles Requiring Separation of Duties

Any person acting in another trusted role shall 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.

CA, RA and System Administration duties shall be separate roles.

1.30 Personnel Controls

1.30.1 Qualifications, Experience, & Clearance Requirements

Personnel engaged in the NDPKI shall be suitably qualified and experienced.

All personnel engaged in the operation of the NDPKI shall hold an appropriate national clearance at or above the level of information protected by the PKI as specified in the National Defence security regulations.

1.30.2 Background Check Procedures

All personnel engaged in the operation of the NDPKI shall undergo background checks in accordance with the National Defence security regulations.

1.30.3 Training Requirements

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

1.30.4 Retraining Frequency & Requirements

The NDPKI PMA shall ensure that appropriate re-training of personnel engaged in the management and operation of the NDPKI is executed.

1.30.5 Job Rotation Frequency & Sequence

Job rotation frequency and sequence shall be in accordance with the NDPKI policies.

1.30.6 Sanctions for Unauthorized Actions

The NDPKI PMA shall 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.

1.30.7 Independent Contractor Requirements

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

1.30.8 Documentation Supplied To Personnel

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

1.31 Audit Logging Procedures

1.31.1 Types of Events Recorded

All NDPKIs shall audit the system to ensure that the trust and integrity of the PKI is maintained. This may include but not limited to certificate lifecycle operations, physical and logical access (successful and failed) of NDPKI assets such as CAs, authorised repositories, and RA workstations, changes to the configuration of these systems, functions performed on the audit log, security relevant changes to the platform and PKI applications, and requests made to the system and responses to those requests.

For each event the following minimum information shall be recorded:

- Type of event.
- Date and time of event.
- Identity of entity causing event and that of those handling it.
- The success or failure (along with reason for failure) of the event.

CSAs are not required to log requests for revocation status or the responses to those requests.

1.31.2 Frequency of Processing Log

Audit logs shall be reviewed periodically at least six times a year for anomalous and unauthorised events in accordance with the NDPKI policies.

1.31.3 Retention Period for Audit Log

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

1.31.4 Protection of Audit Log

Audit data shall not be open for modification by any person or automated system process, other than those performing the security audit function.

NDPKI system and configuration procedures shall be in place to protect the electronic audit log system and audit information captured electronically or manually from unauthorized viewing, modification, deletion or destruction.

1.31.5 Audit Log Backup Procedures

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

1.31.6 Audit Collection System (Internal vs. External)

The audit collection system shall be in accordance with National Defence regulations.

Should it become apparent that the audit collection system has failed; the CMA shall cease all operation except for revocation processing until the security audit capability can be restored.

1.31.7 Notification to Event-Causing Subject

No stipulation.

1.31.8 Vulnerability Assessments

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

1.32 Records Archive

1.32.1 Types of Events Archived

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

1.32.2 Retention Period for Archive

The retention period for archives shall be in accordance with National Defence regulations. At a minimum, archives related to any certificate shall be maintained beyond the life of the certificate.

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

1.32.3 Protection of Archive

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

1.32.4 Archive Backup Procedures

Archive backup procedures shall be in accordance with National Defence regulations.

1.32.5 Requirements for Time-Stamping of Records

Time stamping shall take place in accordance with National Defence regulations.

1.32.6 Archive Collection System (Internal or External)

Archive collection shall take place in accordance with National Defence regulations.

1.32.7 Procedures to Obtain & Verify Archive Information

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

1.33 Key Changeover

NDPKI PMA 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.

1.34 Compromise & Disaster Recovery

1.34.1 Incident and Compromise Handling Procedures

The 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.

1.34.2 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. Prior to resuming operations, the integrity of the CA shall be verified.

1.34.3 Entity Private Key Compromise Procedures

In case of a CA key compromise, a superior CA shall revoke that CA's certificate, and the revocation information shall be published immediately in the most expedient manner. If the CA is a Root CA, NDPKI PMA must advise Relying Parties, including the NDPKI PMAs which with it has cross-certified.

1.34.4 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 disaster.

1.35 CA & RA Termination

In the event of a CA termination, the CA certificate shall be revoked. CA termination shall follow notification procedures equivalent to key compromise (Section 5.7.3).

RA termination is in accordance with the NDPKI policies.

TECHNICAL SECURITY CONTROLS

1.36 Key Pair Generation & Installation

1.36.1 Key Pair Generation

Cryptographic modules for a UNCLASSIFIED PKI are either approved as specified below or be approved by the nation's appropriate Defence Security Authority/ Defence Security Organisation (DSA/DSO),   Cryptographic modules for a CLASSIFIED PKI need to be approved by DSA/DSO.

Software	Subscriber	RA	CA
FIPS 140 Level	1	2	2

Hardware	Subscriber	RA	CA
FIPS 140 Level	2	2	3

Device	Subscriber	RA	CA
FIPS 140 Level	1	2	2

Key pair generation shall be undertaken via combination of products and processes approved by each nation's appropriate DSA/DSO, to provide keys suitable for:

- Use in PKI based authentication, non-repudiation and integrity services for systems and data up to and within a SECRET high environment;
- 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)[6]; and
- Use in PKI based confidential communications within a SECRET high environment to protect "need to know" using processes which are approved by the appropriate DSA/DSO.

For hardware certificates:

- Signature key pairs shall be generated within a hardware cryptographic module.
- Encryption key pairs generation may occur within the hardware token intended for use by the Subscriber; or within an approved Hardware Security Module (HSM)

For software certificates:

- Key pairs for signature and encryption may be generated, stored and managed in software.
- Key generation shall employ a method that meets or exceeds the NDPKI specified standard for Subscriber software cryptographic modules.

[6] 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.

1.36.2 Private Key Delivery to Subscriber

Where private keys are generated or recovered by the Subscriber on/into the Subscriber's cryptographic module, no additional delivery process is required. Where private keys are generated on the Subscriber's cryptographic module under the control of another person, the process for delivery of the Subscriber's cryptographic module to the Subscriber shall ensure:

- The correct token and activation data are provided to the correct Subscriber
- No unauthorized parties can access or use the token during the delivery process

Where private keys are generated in another cryptographic module or recovered by an RA, the process to delivery of the private key securely onto the Subscriber's token or to the requestor shall be approved by the nation's DSA / DSO. While outside of the cryptographic module or the Subscriber's token, private keys shall be encrypted using an algorithm and process approved by the DSA / DSO.

1.36.3 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.

1.36.4 CA Public Key Delivery to Relying Parties

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

1.36.5 Key Sizes

The strength of key size and hash algorithms shall be as specified in National Institute of Standards and Technology Special Publication 800-57 Part 1 – "Recommendation for Key Management – Part 1: General. [SP 800-57P1]"

1.36.6 Public Key Parameters Generation and Quality Checking

Public key parameters shall always be generated and checked in accordance with the standard that defines the crypto-algorithm in which the parameters are to be used. For example, public key parameters for use with algorithms defined in the Federal Information Processing Standard 186-3, Digital Signature Standard [FIPS 186] shall be generated and tested in accordance with [FIPS 186]. Whenever a crypto-algorithm is described in [FIPS 186], the parameter generation and checking requirements and recommendations of [FIPS 186] shall be required of all entities generating key pairs whose public components are to be certified by the CA.

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

The use of a specific key is determined by the key usage extension in the X.509 certificate.

Certificates used by individuals (e.g., human Subscriber) shall not assert both the digitalSignature and encryption (i.e., keyEncipherment or keyAgreement). Nations may choose to require separate signature and authentication certificates.

Certificates used by devices may be used for both digital signature and key management and may assert both the digitalSignature and encryption (e.g., keyEncipherment or keyAgreement) as necessary.

1.37 Private Key Protection & Cryptographic Module Engineering Controls

1.37.1 Cryptographic Module Standards & Controls

All cryptographic modules, HSM's and hardware tokens shall be as specified for key generation in Section 6.1.1.

1.37.2 Private Key Multi-Person Control

There shall 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.

The NDPKI PMA shall define the trusted roles in the CP indicating those roles that require multi-person control.

1.37.3 Private Key Escrow

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

1.37.4 Private Key Backup

Private keys associated with individual's hardware certificate shall not be backed up.

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

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

1.37.5 Private Key Archival

If the CA private signing keys and private keys associated with certificates are archived, the NDPKI PMA shall ensure the security of the private keys in the archive. .

1.37.6 Private Key Transfer into or from a Cryptographic Module

To be carried out in accordance with the process approved by each DSA / DSO regulations.

1.37.7 Private Key Storage on Cryptographic Module

The method of storing private keys on cryptographic modules shall be done in accordance with policy approved by each nation's DSA / DSO.

1.37.8 Method of Activating Private Keys

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

1.37.9 Methods of Deactivating Private Keys

Deactivation of the private key within a cryptographic module shall be in accordance a method approved by each nation's DSA / DSO.

1.37.10 Method of Destroying Subscriber Private Signature Keys

Private keys shall be destroyed when no longer needed in accordance with a method approved by each nation's DSA / DSO.

1.37.11 Cryptographic Module Rating

See 6.2.1 Cryptographic Module Standards & Controls

1.38 Other Aspects of Key Management

1.38.1 Public Key Archival

The public key shall be archived as part of the certificate archival.

1.38.2 Certificate Operational Periods / Key Usage Periods.

Key lifetimes are set as a matter of policy by each nation's DSA / DSO. This will depend on a number of factors, which includes the size of the key.

Maximum operational periods / key usage periods for the following entities are detailed below:

Entity	Maximum Key Usage Periods	Maximum Certificate Operational Periods
Root CAs	25 years	25 years
CA & RA servers	10 years	10 years
Certificate Status Authority	3 years	3 years

Cross-Certificate	3 years	3 years
Subscriber	3 years	3 years
Code/Content Signing	8 years	8 years
Trusted Role	3 years	3 years

1.39 Activation Data

1.39.1 Activation Data Generation & Installation

Activation data may be Subscriber selected. A pass-phrase, personal identification number (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.

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

If activation data is selected by the RA, the Subscriber or PKI Sponsor shall change activation data upon initial receipt.

1.39.2 Activation Data Protection

Activation data in conjunction with other access control shall have an appropriate level of strength for the keys or data to be protected when transmitted or at rest.

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

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

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.

1.39.3 Other Aspects of Activation Data

No stipulation.

1.40 Computer Security Controls

1.40.1 Specific Computer Security Technical Requirements

CA equipment used for NDPKI shall use operating systems that:

- Require authenticated logins;
- Provide discretionary access control;
- Provide a security audit capability.
- Provide process isolation; and
- Support recovery from key or system failure.

For CA components, either remote management and login shall be disabled, or remote maintenance shall be conducted via an end-to-end (administrator machine to component) virtual private network using cryptography commensurate with the strength of the NSS PKI keys being issued.

Network protocols not required for CAS or RA operation or remote administration shall be disabled. TELNET and File Transfer Protocol (FTP) shall never be enabled.

For classified networks, the workstation used by the RA is protected from the class of threats associated with general use within the environment (e.g., Separate workstation, use of a non-persistent environment on a general purpose workstation.)

1.40.2 Computer Security Rating

No stipulation.

1.41 Life-Cycle Security Controls

1.41.1 System development controls

No stipulation.

1.41.2 Security management controls

Security management controls shall be undertaken in accordance the policies approved by each nation's DSA / DSO.

Hardware and software on CA systems shall be dedicated to performing CA functions. This does not preclude running multiple CA instances on a single hardware platform in virtual environments.

1.41.3 Life cycle security controls

Life cycle security controls shall be undertaken in accordance with the policies approved by each nation's DSA / DSO.

1.42 Network Security Controls

Network security controls shall be undertaken in accordance with the policies approved by each nation's DSA / DSO.

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.

1.43 Time Stamping

No stipulation.

CERTIFICATE, CRL, AND OCSP PROFILES FORMAT

This chapter establishes the settings required for a core set of extensions required by a PKI solution. Particular attention was given to those which are necessary to ensure successful interoperation between nations.

This chapter also addresses the profile settings required to ensure that the CRL and OCSP requests and responses can be correctly interpreted by all parties in the cross-certification.

Each Nation shall implement these parameters to ensure compliance to the cross-certification model supported by this policy.

1.44 Certificate Profile

1.44.1 Version Numbers

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

1.44.2 Certificate Extensions

The tables below constrain the use of certificate extensions in order to ensure interoperability. The tables do not address all certificate extensions. Other use of extensions should conform to RFC 5280. For extensions which do not conform to RFC 5280, they shall be marked non-critical. In the tables, the following terms are used:

- Required Critical – the extension shall be present and is always marked critical;
- Required – the extension shall be present and may be marked non-critical;
- Optional – the extension may be included at the Nations discretion; and
- Not Used – the extension shall never be used

The following extensions are included in cross-certificates:

Field/ Extension	Cross-Certificate
Version	**Required**
	V3 (2)
Serial Number	**Required**
	Must Be unique by Issuer
Issuer Signature Algorithm	**Required**
	• **sha-1WithRSAEncryption {1 2 840 113549 1 1 5}** Or one of the following signature algorithms: • sha256WithRSAEncryption {1 2 840 113549 1 1 11} • sha384WithRSAEncryption {1 2 840 113549 1 1 12} • sha512WithRSAEncryption {1 2 840 113549 1 1 13} • ecdsa-with-SHA1 {1 2 840 10045 4 1} • ecdsa-with-SHA256 {1 2 840 10045 4 3 2} • ecdsa-with-SHA384 {1 2 840 10045 4 3 3} • ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	**Required**
	Each RDN is a printableString and contains a single attribute type and attribute value tuple
Validity Period	**Required**
	Maximum 3 years from date of issue in UTCT format. Note: the notBefore component will be the certificate's issue date. The notAfter component is the day ending the validity period.
Subject Distinguished Name	**Required**
	Each RDN is a printableString and contains a single attribute type and attribute value tuple
Subject Public Key Information	**Required**
	Key size should provide security at 112 bit crypto security or greater now and 128 bit if the key lasts beyond 2030. The following encryption algorithms are acceptable: • RsaEncryption {1 2 840 113549 1 1 1 } • Id-ecPublicKey {1 2 840 10045 2 1}
Issuer Unique Identifier	**Not used**

Field/ Extension	Cross-Certificate
Subject Unique Identifier	**Not used**
Issuer’s Signature	**Required**
	ASN.1 DER encoded certificate signature value corresponding to Issuer signature algorithm
Authority Key Identifier	**Required**
	keyID, Octet String Recommended that that the octet string contain the 20 byte SHA-1 hash of the binary DER encoding of the subject CA’s public key information
	Not Used
	Issuer DN, Serial Number tuple
Subject Key Identifier	**Required**
	Recommended that the octet string contain the 20 byte SHA-1 hash of the binary DER encoding of the subject CA’s public key information
Key Usage	**Required** **Critical**
	keyCertSign, CRLSign
Basic Constraints	**Required** **Critical**
	cA True; path length constraint absent or value per PKI hierarchy
Extended Key Usage	**Not used**
Private Key Usage Period	**Not used**
Certificate Policies	**Required**
	Sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optionally id-qt-cps | id-qt-unotice qualifiers
Policy Mappings	**Required**
	Sequence of one or more pairs of OIDs; each pair includes an issuerDomainPolicy and a subjectDomainPolicy
Subject Alternative Name	**Not Used**
Issuer Alternative Name	**Not Used**

Field/ Extension	Cross-Certificate
Subject Directory Attributes	**Not Used**
Name Constraints	**Optional**
	If included, it shall contain permittedSubtrees or excludedSubtrees field. Recommend that if asserted it be marked critical.
Policy Constraints	**Required** **Critical**
	inhibitPolicyMapping with skipcerts=0
Authority Information Access	**Required**
	id-ad-caIssuers Primary HTTP URI mandatory Secondary Lightweight Directory Access protocol (LDAP) URI optional
	id-ad-ocsp Optional
CRL Distribution Points	**Required**
	Primary HTTP URI mandatory Secondary LDAP URI optional
Subject Information Access	**Optional**
	Id-ad-carepository Primary HTTP URI mandatory if extension is present Secondary LDAP URI optional
Freshest CRL	**Not Used**
Inhibit Any Policy	**Required** **non-critical**[7]
	skipcerts=0

The following extensions are included in signing CA certificates:

Field/ Extension	Intermediate or Signing CA

[7] **This is not conformant to the RFC due to application compatibility issues.**

Field/ Extension	Intermediate or Signing CA
Version	**Required**
	V3 (2)
Serial Number	**Required**
	Must Be unique by Issuer
Issuer Signature Algorithm	**Required**
	• **sha-1WithRSAEncryption {1 2 840 113549 1 1 5}** Or one of the following signature algorithms: • sha256WithRSAEncryption {1 2 840 113549 1 1 11} • sha384WithRSAEncryption {1 2 840 113549 1 1 12} • sha512WithRSAEncryption {1 2 840 113549 1 1 13} • ecdsa-with-SHA1 {1 2 840 10045 4 1} • ecdsa-with-SHA256 {1 2 840 10045 4 3 2} • ecdsa-with-SHA384 {1 2 840 10045 4 3 3} • ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	**Required**
	Each RDN is a printableString and contains a single attribute type and attribute value tuple
Validity Period	**Required**
	Maximum 10 years from date of issue in UTCT format. Note: the notBefore component will be the certificate's issue date. The notAfter component is the day ending the validity period.
Subject Distinguished Name	**Required**
	Each RDN is a printableString and contains a single attribute type and attribute value tuple
Subject Public Key Information	**Required**
	Key size should provide security at 112 bit crypto security or greater now and 128 bit if the key lasts beyond 2030. The following encryption algorithms are acceptable: • RSAEncryption {1 2 840 113549 1 1 1 } • id-ecPublicKey {1 2 840 10045 2 1}
Issuer Unique Identifier	**Not used**
Subject Unique Identifier	**Not used**

Uncontrolled copy when printed

Field/ Extension	Intermediate or Signing CA
Issuer’s Signature	**Required**
	ASN.1 DER encoded certificate signature value corresponding to Issuer signature algorithm
Authority Key Identifier	**Required**
	keyID, Octet String Recommended that that the octet string contain the 20 byte SHA-1 hash of the binary DER encoding of the subject CA’s public key information
	Not Used
	Issuer DN, Serial Number tuple
Subject Key Identifier	**Required**
	Recommended that that the octet string contain the 20 byte SHA-1 hash of the binary DER encoding of the subject CA’s public key information
Key Usage	**Required** **Critical**
	keyCertSign, CRLSign and, optionally, others to include digitalSignature and nonRepudiation
Basic Constraints	**Required** **Critical**
	cA True; path length constraint per PKI hierarchy
Extended Key Usage	**Not used**
Private Key Usage Period	**Not used**
Certificate Policies	**Required**
	Sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optionally ID-QT-CPS and ID-QT-UNotice. Qualifiers
Subject Alternative Name	**Not Used**
Issuer Alternative Name	**Not Used**
Subject Directory Attributes	**Not Used**
Authority Information Access	**Optional**
	id-ad-caIssuers

Field/ Extension	Intermediate or Signing CA
	Primary HTTP URI mandatory Secondary LDAP URI optional
	id-ad-ocsp Optional
CRL Distribution Points	**Required**
	Primary HTTP URI mandatory Secondary LDAP URI optional
Subject Information Access	**Optional**
	Id-ad-carepository Primary HTTP URI mandatory if extension is present Secondary LDAP URI optional
Freshest CRL	**Not Used**

The following are included in people and role Subscriber certificates:

Field/ Extension	People and Role Subscriber
Version	**Required**
	V3 (2)
Serial Number	**Required**
	Must Be unique by Issuer
Issuer Signature Algorithm	**Required**
	• **sha-1WithRSAEncryption {1 2 840 113549 1 1 5}** Or one of the following signature algorithms: • sha256WithRSAEncryption {1 2 840 113549 1 1 11} • sha384WithRSAEncryption {1 2 840 113549 1 1 12} • sha512WithRSAEncryption {1 2 840 113549 1 1 13} • ecdsa-with-SHA1 {1 2 840 10045 4 1} • ecdsa-with-SHA256 {1 2 840 10045 4 3 2} • ecdsa-with-SHA384 {1 2 840 10045 4 3 3} • ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	**Required**
	Each RDN is a printableString and contains a single attribute type

Field/ Extension	**People and Role Subscriber**
	and attribute value tuple
Validity Period	**Required**
	Maximum 3 years from date of issue in UTCT format. Note: the notBefore component will be the certificate's issue date. The notAfter component is the day ending the validity period.
Subject Distinguished Name	**Required**
	Each RDN is a printableString and contains a single attribute type and attribute value tuple
Subject Public Key Information	**Required**
	Key size should provide security at 112 bit crypto security or greater now and 128 bit if the key lasts beyond 2030. The following encryption algorithms are acceptable: • RSAEncryption {1 2 840 113549 1 1 1 } • id-ecPublicKey {1 2 840 10045 2 1} • id-ecDH {1 3 132 1 12} • dhpublicnumber {1 2 840 10046 2 1}
Issuer Unique Identifier	**Not used**
Subject Unique Identifier	**Not used**
Issuer's Signature	**Required**
	ASN.1 DER encoded certificate signature value corresponding to Issuer signature algorithm
Authority Key Identifier	**Required**
	keyID, Octet String Recommended that that the octet string contain the 20 byte SHA-1 hash of the binary DER encoding of the subject CA's public key information
	Not Used
	Issuer DN, Serial Number tuple
Subject Key Identifier	**Required**
	Recommended that that the octet string contain the 20 byte SHA-1 hash of the binary DER encoding of the subject CA's public key information
Key Usage	**Required**

Field/ Extension	People and Role Subscriber
	Critical
	One or more of: digital signature, non repudiation, key encipherment, key agreement
Basic Constraints	**Not used**
Extended Key Usage	**Optional**
Private Key Usage Period	**Not used**
Certificate Policies	**Required**
	Sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers
Policy Mappings	**Not Used, Not Applicable**
Subject Alternative Name	**Optional; Recommended RFC 822 Name and UPN**
Issuer Alternative Name	**Not Used**
Subject Directory Attributes	**Optional**
Name Constraints	**Not Used, Not Applicable**
Policy Constraints	**Not Used, Not Applicable**
Authority Information Access	**Required**
	id-ad-caIssuers Primary HTTP URI mandatory Secondary LDAP URI optional
	id-ad-ocsp Optional
CRL Distribution Points	**Required**
	Primary HTTP URI mandatory Secondary LDAP URI optional
Subject Information Access	**Not Used, Not Applicable**
Freshest CRL	**Not Used**
Inhibit Any Policy	**Not Used, Not Applicable**

The following are included in Device Subscriber certificates:

Field/ Extension	Device
Version	**Required**
	V3 (2)
Serial Number	**Required**
	Must Be unique by Issuer
Issuer Signature Algorithm 1 2	**Required**
	• Or one of the following signature algorithms: • sha256WithRSAEncryption {1 2 840 113549 1 1 11} • sha384WithRSAEncryption {1 2 840 113549 1 1 12} • sha512WithRSAEncryption {1 2 840 113549 1 1 13} • ecdsa-with-SHA1 {1 2 840 10045 4 1} • ecdsa-with-SHA256 {1 2 840 10045 4 3 2} • ecdsa-with-SHA384 {1 2 840 10045 4 3 3} • ecdsa-with-SHA512 {1 2 840 10045 4 3 4}
Issuer Distinguished Name	**Required**
	Each RDN is a printableString and contains a single attribute type and attribute value tuple
Validity Period	**Required**
	Maximum 3 years from date of issue in UTCT format. Note: the notBefore component will be the certificate's issue date. The notAfter component is the day ending the validity period.
Subject Distinguished Name	**Required**
	Each RDN contains a single attribute type and attribute value tuple. directoryString is encoded as printableString cn={ Host URL | Host Internet protocol (IP) Address | Host Name }
Subject Public Key Information1 2	**Required**

	Key size should provide security at 112 bit crypto security or greater now and 128 bit if the key lasts beyond 2030.
	The following encryption algorithms are acceptable:
	rsaEncryption {1 2 840 113549 1 1 1 }
	id-ecPublicKey {1 2 840 10045 2 1}

Issuer Unique Identifier	**Not used**

Field/ Extension	Device
Subject Unique Identifier	**Not used**
Issuer's Signature	**Required**
	ASN.1 DER encoded certificate signature value corresponding to Issuer signature algorithm
Authority Key Identifier	**Required**
	keyID, Octet String Recommended (20 byte SHA-1 hash of the binary DER encoding of the issuing CA's public key information)
	Not Used
	Issuer DN, Serial Number tuple
Subject Key Identifier	**Required**
	Recommended Octet String (20 byte SHA-1 hash of the binary DER encoding of the subject's public key information)
Key Usage	**Required** **Critical**
	digital signature, and key encipherment (when SPKI has rsaEncryption OID) or key agreement (when SPKI has id-ecPublicKey OID)
Basic Constraints	**Not used**
Extended Key Usage	**Optional**[3]
Private Key Usage Period	**Not used**
Certificate Policies	**Required**
	Sequence of one or more policy information terms, each of which consists of an object identifier (OID) and optional qualifiers
Policy Mappings	**Not Used, Not Applicable**
Subject Alternative Name	**Required;** Host URL | IP Address | Host Name
Issuer Alternative Name	**Not Used**
Subject Directory Attributes	**Optional**
Name Constraints	**Not Used, Not Applicable**
Policy Constraints	**Not Used, Not Applicable**
Authority Information	**Required**

Field/ Extension	Device
Access	id-ad-caIssuers Primary HTTP URI mandatory Secondary LDAP URI optional
	id-ad-ocsp Optional
CRL Distribution Points	**Required**
	Primary HTTP URI mandatory Secondary LDAP URI optional
Subject Information Access	**Not Used, Not Applicable**
Freshest CRL	**Not Used**
Inhibit Any Policy	**Not Used, Not Applicable**

For specific certificates:

Certificate Type	SPKI	KU	EKU
Authentication	rsaEncryption	digital signature	{client authentication, smart card log on}
	id-ecPublicKey	digital signature	{client authentication, smart card log on}
Signature	rsaEncryption	digital signature, non-repudiation	Extension Omitted or {secure email, document signing}
	id-ecPublicKey	digital signature, non-repudiation	Extension Omitted or {secure email, document signing}
Authentication & Signature	rsaEncryption	digital signature, non-repudiation	Extension Omitted or {client authentication, secure email, document signing, smart card log on and anyEKU}

	id-ecPublicKey	digital signature, non-repudiation	Extension Omitted
Encryption	rsaEncryption	key encipherment	Extension Omitted
	id-ecPublicKey	key agreement	Extension Omitted
	id-ecDH	key agreement	Extension Omitted
	dhpublicnumber	key agreement	Extension Omitted

1.44.3 Algorithm Object Identifiers

The NDPKI shall only certify public keys associated with the cryptographic algorithms identified below (7.1.3.2 Cryptographic Algorithm Subject Public Key OID), and shall only use the signature algorithms identified below (7.1.3.1 Signature Algorithm OID) to sign certificates, CRLs and any other NDPKI product. NDPKI planning to transition to a new PKI crypto algorithm shall make planning information available to other nations as early as possible in order for other NDPKI PMAs to determine the impact on Relying Parties[8].

1.44.3.1 Signature Algorithm OID

Certificates issued by NDPKIs shall identify the signature algorithm using the following OIDs:

sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) PKI certificates(1) PKI certificates-1(1) 5 }
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
ecdsa-with-SHA1	{iso(1) member-body(2) us(840) ansi-x9-62 (10045) signatures (4) 1}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}

[8] Although there are several acceptable signature and encryption algorithms, use of anything besides sha-1WithRSAEncryption {1 2 840 113549 1 1 5} and RsaEncryption {1 2 840 113549 1 1 1 } may cause interoperability problems.

ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}
ecdsa-with-SHA512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4}

1.44.3.2 Cryptographic Algorithm Subject Public Key OID

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

RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) PKI certificates(1) PKI certificates-1(1) 1 }
Id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public key-type (2) 1}
id-ecDH	{iso(1) identified-organization(3) certicom(132) schemes(1) ecdh(12)}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}

1.44.3.3 Elliptic Curve Public Key Curve OID

Where certificates contain an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
ansip384r1	{iso(1) identified-organization(3) certicom(132) curve(0) 34}
ansip521r1	{iso(1) identified-organization(3) certicom(132) curve(0) 35}

1.44.4 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. Each RDN shall be encoded as printable string where possible or UTF-8 where it is not possible to use printable strings.

1.44.5 Name Constraints

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

Cross-Certificates issued by a NDPKI to a remote PKI should contain a nameConstraints extension. A Subscriber Certificate shall not contain a nameConstraints extension.

1.44.6 Certificate Policy Object Identifier

Except for self-signed certificates, all certificates issued by NDPKIs shall include a certificate policies extension asserting the appropriate OID(s). Except for Root CAs, CAs shall only issue certificates from within the set of OIDs in the CA's signing certificate.

Cross-Certificates issued by a ND PKI to a remote PKI shall contain at least one policyMappings.

1.44.7 Usage of Policy Constraints Extension

A Principal Cross-Certificate issued to a bridge PKI shall contain the policyConstraints extension with inhibitPolicyMapping field omitted, and with requiredExplicitPolicy field with a skipCerts value of zero. It shall contain the inhibitAnyPolicy extension with a skipCerts value of zero.

A Principal Cross-Certificate issued to a non-Bridge (e.g., Enterprise) PKI shall contain the policyConstraints extension with inhibitPolicyMapping field with a skipCerts value of zero, and with requiredExplicitPolicy with a skipCerts value of zero. It shall contain the inhibitAnyPolicy extension with a skipCerts value of zero.

A CA certificate issued within an Enterprise may contain the policyConstraints extension with inhibitPolicyMapping field, if so inhibitPolicyMapping field shall contain skipCerts value of zero. The certificate may contain the policyConstraints extension with requiredExplicitPolicy field, if so the requiredExplicitPolicy field shall contain skipCerts value of zero. It may contain the inhibitAnyPolicy extension with a skipCerts value of zero.

A Subscriber Certificate shall not contain a policyConstraints or inhibitAnyPolicy extension.

A Subscriber Certificate shall not contain a policyConstraints extension.

1.44.8 Policy Qualifiers Syntax & Semantics

The only policy qualifiers that are permitted are the CPS Pointer qualifier and the User notice qualifier.

The CPS Pointer, if used, shall contain a HTTP URI link to the Certification Practice Statement (CPS) published by the CA, or to a webpage from which the CPS can then be downloaded.

The User notice, if used, shall only contain the explicitText field using an IA5String.

1.44.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics shall be done in accordance with RFC 5280

1.45 CRL Profile

1.45.1 Version Numbers

CRLs issued shall be v2 CRLs (populate version field with integer “1”).

1.45.2 CRL and CRL Entry Extensions

The following CRL Entry Extensions may be included:

- Reason Code (non-critical)
- Invalidity Date (non-critical).

The following CRL Extensions must be included:

- Authority Key Identifier (non-critical). The Authority Key Identifier shall use the keyIdentifier choice.
- CRL Number (non-critical)
- The following CRL Extensions may be included: Issuing Distribution Point (critical).

1.46 OCSP Profile

1.46.1 Version Numbers

OCSP version 1 as defined in RFC 2560.

1.46.2 OCSP Extensions

Appropriate extensions from RFC 2560 may be used in OCSP requests and responses. If the extensions are used, they shall not be marked critical.

Uncontrolled copy when printed

COMPLIANCE AUDIT & OTHER ASSESSMENTS

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

1.47 Frequency of Audit or Assessments

All CAs shall be audited at least every 3 years. RAs shall be audited in accordance with the requirements of the NDPKI CP.

1.48 Identity & Qualifications of Assessor

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

1.49 Assessor's Relationship to Assessed Entity

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

1.50 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 this CPMC and the NDPKIs CP and CPSs.

1.51 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 shall be followed.

Where the audit finds a discrepancy between the CMA's operation and ACP 185 that is not covered in the self assertion or CCA, the NDPKI PMA shall advise the other Participant immediately and shall seek to reach an agreement on the resolution of the non-conformance with the other Participant.

1.52 Communication of Results

The PMA shall promptly provide a summary of the results of each such audit to the other Participant.

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 shall be included in the CCA.

1.53 Fees

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

1.54 Financial Responsibility

Each of the nations shall bear its own costs in connection with cross-certification.

1.55 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. Any such information which is protectively marked shall be treated in accordance with the appropriate provisions of the CJM3IEM[9].

1.56 Privacy of Personal Information

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

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

1.57 Intellectual Property Rights

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

1.58 Representations & Warranties

No stipulation.

1.59 Disclaimers of Warranties

No stipulation.

1.60 Limitations of Liability

The liability of the nations shall be limited respectively as provided in the respective cross-certification agreement.

1.61 Indemnities

No stipulation.

1.62 Term & Termination

This publication 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.

1.63 Individual Notices & Communications With Participants

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

1.64 Amendments

1.64.1 Procedure for Amendment

See ACP 198(M).

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

1.64.2 Notification Mechanism and Period

See ACP 198(M).

1.64.3 Circumstances under which OID must be changed

Although it is not expected, if a Nation changes an OID, the ND PKI PMA shall notify partner nations to make appropriate updates to cross-certificates.

1.65 Dispute Resolution Provisions

Dispute resolution procedures shall be specified in the CCA.

1.66 Governing Law

Not applicable[10].

1.67 Compliance with Applicable Law

CJM3IEM applies.

1.68 Miscellaneous Provisions

Not applicable.

1.69 Other Provisions

Not applicable.

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

CROSS-CERTIFICATION ARRANGEMENT TEMPLATE

COMBINED JOINT MULTILATERAL MASTER MILITARY INFORMATION EXCHANGE

MEMORANDUM OF UNDERSTANDING

INFORMATION EXCHANGE ANNEX

COMPRISING CROSS-CERTIFICATION ARRANGEMENTS

(To Facilitate Information Exchanges Under the Combined Joint Multilateral Master Military Information Exchange Memorandum of Understanding)

BETWEEN

{NATION A}

AND

{NATION B}

({NATION A} – {NATION B} Cross-Certification Arrangements)

In accordance with the Memorandum of Understanding Among the Department of Defence of Australia and the Department of National Defence of Canada and the New Zealand Defence Force and the Ministry of Defence of the United Kingdom of Great Britain and Northern Ireland and the Department of Defense of the United States of America Concerning Combined Joint Multilateral Master Military Information Exchange (CJM3IEM), which entered into effect on June 29, 2004,

The {Nation A} and {Nation B} (collectively, the "Participants") hereby establish this Combined Joint Military Information Exchange Annex (CJMIEA) comprising Cross-Certification Arrangements for their respective Public Key Infrastructures.

1. Purpose

1.1. To establish Public Key Infrastructure (PKI) Cross-Certification Arrangements between the Participants, in order to enable and facilitate the secure electronic exchange of Military Information and Data between them under the CJM3IEM.

2. Description

2.1. The Participants enter into this CJMIEA comprising Cross-Certification Arrangements to support security services based upon PKI technology in furtherance of the implementation of policies, processes, and technologies in support of the exchange and validation of authentication credentials to facilitate the exchange of Military Information and Data under the CJM3IEM.

2.2. The Participants will work towards creating interoperability between their approved PKI systems, incorporating strong identity management regimes and common policies, to support the exchange of authenticated Military Information and Data under the CJM3IEM.

2.3. In order to enable, on a bilateral basis, PKI interoperability between the Participants, the Participants with each other in accordance with this CJMIEA.

2.4. The Participants the policies, processes, and procedures described in the Allied Communications Publication 185 (ACP 185)[11], as amended from time to time, to achieve PKI interoperability in order to facilitate the secure electronic exchange of Military Information and Data between them under the CJM3IEM.

3. Definitions and Acronyms

3.1. The following words, terms, and acronyms will, unless the context otherwise requires, have the meanings set forth below:

[11] The current version ACP 185 is available from the CCEB Secretariat.

ACP 185	Allied Communications Publication 185, as amended from time to time
CA	Certification Authority, an Authority trusted by the participants to create and assign certificates
CCEB	Combined Communications-Electronics Board
CCEB Nations	Australia, Canada, New Zealand, the United Kingdom of Great Britain and Northern Ireland, and the United States of America
CJMIEA	Combined Joint Military Information Exchange Annex
CP	Certificate Policy, the policy and requirements underlying the establishment and operation of a PKI, which indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements
CPS	Certification Practice Statement
CRL	Certificate Revocation List
Cross-Certification	The establishment of a trust relationship between two CAs achieved by each signing the other CA's public key in a certificate
Cross-Certificate	A certificate issued under either subparagraph 4.2.2 or 4.4.9 of this CJMIEA
{Acronym for Nation A Designation}	{Enter text that denotes what acronym stands for, e.g., DoD for The Department of Defense of the United States of America}
{Acronym for Nation B Designation}	{Enter text that denotes what acronym stands for, e.g., AUS DoD for Australian Department of Defence}
{CCEB Nation A} Interoperability CA	{Description of Nation A's Interoperability CA that will be cross-certified with Nation B's Interoperability CA }
{CCEB Nation B} Interoperability CA	{Description of Nation B's Interoperability CA that will be cross-certified with Nation A's Interoperability CA }

Military Information and Data	Military Information and Data, in any format or medium, required to permit military strategic and operational command staffs to train, test, exercise, plan and conduct Combined or Coalition operations, as defined in the CJM3IEM
OCSP	Online Certificate Status Protocol
Participant	A signatory to this CJMIEA
PKI	Public Key Infrastructure, a system established to issue, maintain and revoke certificates, and the processes and procedures governing their issue
Relying Party	An entity that has received and relies on a PKI certificate and a digital signature verifiable with reference to a public key listed in that certificate.
Subscriber	An approved entity to whom a PKI certificate has been issued, that is named or identified in that certificate, and that holds a private key that corresponds to the public key listed in that certificate

3.2. References to a paragraph or Schedule are to a paragraph of or Schedule to this CJMIEA, references to this CJMIEA include its Schedules and references in a Schedule to a paragraph are to a paragraph of that Schedule.

4. Objective and Scope

4.1 Scope

4.1.1. The exchange of Military Information and Data under this CJMIEA will take place in accordance with the CJM3IEM.

4.1.2. The Participants will establish a PKI trust relationship through Cross-Certification in accordance with their respective CPs as listed in Schedule 1 to this CJMIEA, in order to permit secure, identity-assured communications and information exchange between them.

4.1.3. Any Cross-Certification between the Participants under the Cross-Certification arrangements, and any reliance upon a Cross-Certificate issued as a result of such Cross-Certification, will be limited to the support of communications and information exchange between the Participants through their officials and employees, military personnel, and authorised eligible contractors for Military Information and Data exchange purposes in accordance with the CJM3IEM.

4.1.4. The Participants will not undertake any communication or exchange of Military Information and Data under this CJMIEA for any purpose other than the purpose specified in subparagraph 4.1.3 of this CJMIEA.

4.1.5. The Participants will ensure that their respective PKIs, and the Cross-Certification arrangements between them, are consistent with the requirements of and definitions in ACP 185 and support the following:

4.1.5.1. Identity authentication;

4.1.5.2. Integrity;

4.1.5.3. Confidentiality; and

4.1.5.4. Non-repudiation.

4.2. Cross-Certification

4.2.1. Each of the Participants hereby confirms that, prior to entering into this CJMIEA, it has undertaken the following actions:

4.2.1.1. both independently and together with the other Participant, completed technical testing of its respective PKI in a test environment to confirm that interoperability can be established between the Participants;

4.2.1.2. compared its own CP against the mapping criteria and guidance for Cross-Certification as specified in the relevant provisions of ACP 185 and recorded a formal self-assertion of its own CP's level of equivalence and compliance with such criteria and guidance. The formal self-assertion will be made available to the other Participant;

4.2.1.3. discussed with the other Participant the results of the formal self-assertions made and, in relation to any areas of non-compliance by either of them with ACP 185, determined which, if any, of the areas of non-compliance will be mutually acceptable areas of non-compliance. Each Participant will record any areas of non-compliance that are mutually acceptable to the Participants in a statement that will be made available to the other Participant;

4.2.1.4. determined with the other Participant a process for the exchange of cross-certificates.

4.2.2. As soon as reasonably practicable following the entry into effect of this CJMIEA, the Participants will each undertake the following activities:

4.2.2.1. the {Nation A} Interoperability Certificate Authority (CA) and the designated {Nation B} Interoperability CA will each sign a Certificate Signing Request (CSR) using their respective PKI private keys, and issue a Cross-Certificate to the other Participant; and

4.2.2.2. ensure that their respective communications and information systems networks are interconnected to allow communications supported by the Cross-Certification to be made between them in accordance with paragraph 4.3 of this CJMIEA.

4.2.3. The initial cross-certificate issued by each of the Participants in accordance with sub-subparagraph 4.2.2.1 of this CJMIEA will be valid for a period of 12 months beginning on the date that the cross-certificate is issued. Subsequent cross-certificates issued by the Participants in accordance with subparagraph 4.4.9 of this CJMIEA will be valid for a period of three (3) years.

4.2.4. A Participant may revoke any cross-certificate issued by it in the following circumstances:

4.2.4.1. where the other Participant has not complied with its responsibilities under the Cross-Certification arrangements, or under any of the documents or publications referred to in subparagraph 4.4.3 of this CJMIEA;

4.2.4.2. where there remain issues identified in a compliance audit conducted in accordance with subparagraph 4.4.10 of this CJMIEA and the Participants have neither found an acceptable solution for those issues nor established that any areas of non-compliance are acceptable;

4.2.4.3. at any time upon receipt by the issuing Participant of an authenticated request for revocation from the recipient Participant;

4.2.4.4. where the certificate of the {NATION A} Interoperability CA or the {NATION B} Interoperability CA has been compromised or revoked;

4.2.4.5 if the cross-certificate of either Participant’s principal Interoperability CA fails to operate in accordance with its CP; or

4.2.4.6. at any time in the sole discretion of the issuing Participant.

4.2.5. In each case where a cross-certificate is revoked under subparagraph 4.2.4 of this CJMIEA, the issuing Participant will immediately notify the recipient Participant of the revocation of the cross-certificate.

4.3 Communications

4.3.1. Communications between the Participants that are based on the cross-certificates issued under the Cross-Certification arrangements will be limited to communications between the respective Participant’s officials and employees, military personnel, and authorised eligible contractors for operational Military Information and Data exchange purposes in accordance with the CJM3IEM.

4.3.2. The levels of assurance at which each Participant will operate for the duration of the Cross-Certification arrangements contained in this CJMIEA will be those specified in Schedule 2 to this CJMIEA. The CP mapping table and the object identifiers for each Participant are specified in Schedule 2 to this CJMIEA.

4.4. Responsibilities of the Participants

4.4.1. Each Participant will identify and specify points of contact for incident response notification and for handling of operational problem resolution. Each Participant will provide such information to the other Participant.

4.4.2. Each Participant will notify the other Participant immediately if it becomes unable to comply with the Cross-Certification arrangements contained in this CJMIEA, in particular with the provisions of subparagraph 4.4.3 of this CJMIEA.

4.4.3. Each Participant will, at all times whilst this CJMIEA remains in effect, comply and maintain compliance with all the applicable requirements of ACP 185, its own CP, its own CPSs, and all regulatory and other requirements and procedures relating to the operation of its own PKI and those specific requirements set out in Schedule 1 to this CJMIEA.

4.4.4. If, after this CJMIEA enters into effect, a Participant becomes unable to meet any of the requirements stated in subparagraph 4.4.3 of this CJMIEA, that Participant will immediately inform the other Participant. The Participants may either confirm that the area of non-compliance is an acceptable area of non-compliance and request the other Participant to document the area of non-compliance in a statement, which will be made available to the other Participant, or, in the absence of such confirmation, the other Participant may revoke its cross-certificate in accordance with subparagraph 4.2.4 of this CJMIEA.

4.4.5. Each Participant will notify the other Participant immediately of any change it proposes to make to any part of its PKI that could have implications for interoperability between the Participants or affect the Cross-Certification arrangements, including the intention to cross-certify with another CCEB nation or to revoke the certificate of any applicable CA in the Participant's PKI. That Participant will notify the other Participant in sufficient time to enable it to assess the consequences and take any necessary action.

4.4.6. Where a Participant notifies the other Participant of its intention to cross-certify with a defence organisation of another CCEB nation, it will provide the other Participant with advance notice of the intended issuance of the cross-certificate to such other defence organisation at least ninety (90) days before such cross-certificate is issued.

4.4.7. Each Participant will, at all times whilst this CJMIEA remains in effect, operate at the levels of assurance specified in Schedule 2 to this CJMIEA.

4.4.8. Each Participant will revalidate the self-assertion on an annual basis after the initial self-assertion as required by the relevant provisions of ACP 185 in the same manner as described in subparagraph 4.2.1.2 of this CJMIEA, and will, on each occasion, make a formal self-assertion statement, which self-assertion statement will be made available to the other Participant. Each Participant will notify the other Participant upon completion of each such self-assertion.

4.4.9. Following the self-assertion undertaken in accordance with subparagraph 4.4.8 of this CJMIEA, and every three years thereafter, each Participant will sign and issue to the other Participant a new cross-certificate in accordance with the CCA.

4.4.10. Each Participant will ensure that compliance audits of the Interoperability CA of its PKI will be performed at the intervals and by an audit organisation as specified in the relevant provisions of ACP185, and that a summary of the results of each such audit will be promptly reported to the other Participant. If any such audit discloses significant issues in relation to the operation of that Participant's PKI, the Participant concerned will notify the other Participant immediately in accordance with the procedures set out in subparagraph 4.4.13 of this CJMIEA.

4.4.11. Each Participant will respond promptly to requests from the other Participant for information concerning its PKI.

4.4.12. Each Participant will provide to the other Participant copies of relevant certificates including the cross-certificates, CRLs, certificate status information, including OCSP information and any other information necessary to support interoperability between the Participants and the validation of all subordinate certificates linked to the cross-certificate. Such information will be published at the times specified in Schedule 3 to this CJMIEA. Interoperability CA Certificates will be reissued at the times specified in Schedule 3 to this CJMIEA.

4.4.13. In the event that either Participant suffers a compromise of, or a detrimental effect upon, any element of its PKI or its ability to enable PKI interoperability, it will immediately and securely notify the appropriate point of contact of the other Participant.

4.4.14. Each Participant will include in its PKI all the roles listed in the relevant provisions of ACP 185, unless it is specified in its self-assertion statement that a particular role will not be used.

4.4.15. Each Participant will verify the specified Subscriber information before including such information in Subscriber certificates. The Participants may mutually determine that email addresses will not be included in the verification requirement.

4.4.16. The Participants will specify in Schedule 3 to this CJMIEA the group and role certificates used in its PKI and how these are distinguished from Subscriber certificates.

4.4.17. Except as specified in Schedule 3 to this CJMIEA, the Participants will conduct, at a minimum, face-to-face authentication for each Subscriber in their respective PKI every 9 years for certificates issued at the medium assurance level and every 6 years for certificates issued at the medium hardware or high assurance levels.

4.4.18. If a Participant's CP permits suspension of certificates issued in relation to its PKI, that Participant will indicate the circumstances for certificate suspension in Schedule 3 to this CJMIEA, including who may request a suspension, the procedure to be followed for a suspension request, and any limits on a suspension period.

5. Schedule

5.1. This CJMIEA will enter into effect upon the date of the last signature and will remain in effect for a period of 5 years from the date of the last signature unless amended or extended by the written consent of both Participants, or terminated earlier in accordance with paragraph 11 of this CJMIEA.

5.2. Before the expiration of this CJMIEA, the Participants will review the Cross-Certification arrangements contained herein and may, by the written consent of both Participants, extend this CJMIEA for additional periods of up to five years each.

6. Financial Arrangements

6.1. The Cross-Certification arrangements will not impose any financial responsibilities on the Participants. Each of the Participants will bear the full costs, if any, of its own participation in the Cross-Certification arrangements. No funds will be transferred between the Participants, and there will be no jointly incurred costs between the Participants.

6.2. Each Participant will promptly notify the other Participant if it does not have adequate available funds to fulfil its financial responsibilities to maintain a PKI and cross-certificate in accordance with subparagraph 4.4.3 of this CJMIEA, and the Participants will consult on future actions to be taken under the Cross-Certification arrangements.

7. General

7.1. Observance of National Laws and Regulations

All the activities of the Participants under this CJMIEA will be carried out in accordance with their respective national laws and regulations, including their respective export control laws and regulations.

7.2. Settlement of Disputes

Any dispute between the Participants, arising under or relating to the Cross-Certification arrangements or this CJMIEA, will be resolved only by consultation between the Participants and will not be referred to an individual, to any national or international tribunal, or to any third party for settlement.

7.3. Amendments

This CJMIEA may be amended only by the written consent of both Participants.

7.4. Claims and Liability

7.4.1. Each Participant waives any claim that it may have against the other Participant or any of the other Participant's personnel, servants or agents (which do not include contractors) for injury (including any injury resulting in death) or other loss or damage (including any resulting from the reliance of a Relying Party upon a cross-certificate) if such injury, death, damage or loss was caused by the acts or omissions of the other Participant or any of that other Participant's personnel, servants or agents (which do not include contractors) in the performance of official duties connected with this CJMIEA.

7.4.2. Each Participant will resolve third party claims arising from the acts or omissions of any officials, employees, servants or agents (other than contractors) done in the performance of official duties in connection with this CJMIEA in accordance with applicable international arrangements between the Participants and the Participants' national laws and regulations.

7.4.3. Contract claims involving a contractor of a Participant will be resolved by the contracting Participant in accordance with the terms of the relevant contract.

7.4.4. Neither Participant will have any liability to any Subscriber or Relying Party as a result of having issued a cross-certificate.

7.5. Disclosure of Information

All Military Information and Data exchanged under this CJMIEA will conform to the provisions of Sections V (Disclosure and Use of Information), VI (Controlled Unclassified Information), VII (Visits to Establishments), VIII (Security) and IX (Third Party Sales and Transfer) of the CJM3IEM.

7.6. Nomination of Representatives

Each Participant will nominate an action desk officer to represent that Participant under this CJMIEA.

8. Classification

8.1. All classified Military Information and Data exchanged under this CJMIEA will be handled in accordance with the provisions of Section VIII (Security) of the CJM3IEM. The highest classification of Military Information and Data to be exchanged under this CJMIEA is Secret.

9. Termination

9.1. This CJMIEA will terminate automatically upon the termination of the CJM3IEM.

9.2. This CJMIEA may be terminated at any time by the written consent of the Participants, who will consult at the appropriate level prior to the date of termination to ensure termination on the most equitable terms.

9.3. A Participant may withdraw from this CJMIEA at any time upon 60 days' written notification to the other Participant. The withdrawing Participant will continue to participate in this CJMIEA, including the Cross-Certification arrangements, until the date of its withdrawal.

9.4. A Participant may withdraw from this CJMIEA by notice in writing to the other Participant if the other Participant has not complied with its responsibilities under this CJMIEA or under any of the documents mentioned in subparagraph 4.4.3 of this CJMIEA, or if there are unresolved issues identified in a compliance audit conducted in accordance with subparagraph 4.4.10 of this CJMIEA.

9.5. Upon the termination of this CJMIEA, or the Cross-Certification arrangements contained herein, all cross-certificates will be revoked immediately by the Participant that issued such cross-certificates.

9.6. The rights and responsibilities of each Participant under Sections V (Disclosure and Use of Information), VI (Controlled Unclassified Information), VII (Visits to Establishments), VIII (Security), and IX (Third Party Sales and Transfer) of the CJM3IEM, and paragraphs 7.2, 7.4, 7.5, and 8 to this CJMIEA, will continue to apply notwithstanding the withdrawal of a Participant from or the termination or expiration of this CJMIEA.

The foregoing represents the understandings reached between the {Nation A} and the {Nation B} upon the matters referred to herein.

Signed in duplicate in the English language

For the {Nation A}	For the {Nation B}
______________________________	______________________________
Signature	Signature
______________________________	______________________________
Name	Name
______________________________	______________________________
Title	Title
______________________________	______________________________
Date	Date

SCHEDULE 1

CP VERSION DETAILS

Each Participant will list the title, date, and version numbers of their Respective PKI Certificate Policy and Certificate Practice Statements.

SCHEDULE 2

LEVEL OF ASSURANCE AND POLICY MAPPING

Each Participant will include the following:

- Definitions for each level of assurance that will be mapped
- An expected mapping table of their assurance levels and OIDs against the other Participants assurance levels and OIDs

SCHEDULE 3

PKI ARCHITECTURE AND OPERATION

Each Participant will include the following:

- Repository publication timescales and frequency
- CRL issuance frequency for Interoperability CA
- Details about Subscriber information that is included in Subscriber certificates that is not verified
- Use of group/role based certificates and how group/role certificates are to be distinguished from Subscriber certificates
- Face to face authentication requirements outside of the bounds described in subparagraph 4.4.17 of this CJMIEA
- If applicable, the parameters regarding the use of anonymous certificates
- Non conformances for each NDPKI in relation to the CPMC

CROSS-CERTIFICATION SIGNING CEREMONY TEMPLATE

Cross-Certification Signing Ceremony for the

{Country} Interoperability

{Date – DD/MMM/YYYY}

{Classification}

SECTION 1

CROSS-CERTIFICATION SIGNING CEREMONY

PURPOSE

Cross-Certification is the formal and reciprocal recognition of trust between the National Defence Public Key Infrastructure (NDPKIs) of two Combined Communications Electronics Board (CCEB) Member Nations.   Once the two NDPKIs have completed interoperability testing and signed a Cross-Certification Arrangement (CCA), the generation, exchange and signing of principal cross-certificates is achieved through a formally managed process known as a cross-certification signing ceremony.

The goal is for the cross-certified community to be able to trust that the procedures involved were executed correctly, and that the private key materials are stored securely. Security of the private key is important because it ensures that any signature made by that key is known to originate from a legitimate key ceremony, and not by an untrusted third party.

The purpose of this document is to record the witnessing of the cross-certification signing ceremony is to initialise the trust between the NDPKIs of {list the two nations}.

CEREMONY CONDUCT

The cross-certification signing ceremony is conducted on behalf of the {Nation} Policy Management Authority (PMA) and covers the generation of a signed principal cross-certificate for the {Country} Interoperability CA

The ceremony will be conducted in two phases:

1. Generation of the Cross-Certificate signing request will occur within the {Nation} Defence PKI Facility, {address} on {date}. The actual conduct of the generation activities will be undertaken by the {name of facility staff} PKI operators.
2. Signing of the Cross-Certificate will occur within the {Nation} Defence PKI Facility, {address} on {date}. The actual conduct of the signing activities will be undertaken by the {name of facility staff} PKI operators.

WITNESSES TO THE SIGNING EVENT

The following are the authorised witnesses who will be present at the generation and signing phases of the cross-certification signing ceremony.

Witness Name	Nation	Ceremony Phase
		(i.e. generation phase or signing phase)

All witnesses to the generation and signing phases will be required to sign the attached witness statement.

The original signed copy is to be stored within the {Country} PKI Facility and copies sent to the {Nation} PMA.

FUNCTION OF THE WITNESS

On behalf of {Nation} NDPKI, witnesses are confirming that the certificate details conform to the authorised Certificate Policy within the CCA – refer specifically to {Chapter X of - list the appropriate Certificate Policy},dated {Month/Year}, version {version number}, for the {Interoperability} CA Certificate Profile.

SECTION 2

WITNESS STATEMENT SIGNING CEREMONY

GENERATION OF THE CERTIFICATE SIGNING REQUEST

I ________________________________ of _____________________________ do hereby certify that:

a) On the <date>_____________, I attended the {Nation} Defence PKI Facility within the {Facility Name} which is part of the {Name of Defence Department}, at {Location}.

b) I was informed by __________________________, and believe it to be true that:

   i. The {Interoperability} CA servers shown to me were located in a secure cabinet within a secured room within the PKI Facility,

   ii. the {Interoperability} CA servers had been checked immediately prior to my attendance for viruses, worms, trojans and malicious codes, and none were found,

   iii. nothing had occurred since this check to change this belief that the servers were free of viruses, worms, trojans and malicious codes, and

   iv. the {Interoperability} CA servers are operating with dedicated hardware and software that would generate their own private and public keys.

c) Immediately, after being informed of this information by _____________________, I saw ________________________ operate the {Interoperability} CA server and this operation generated a Certificate Signing Request (CSR) with a Distinguished Name of: ____

d) At no time did I see the private keys of {CA Name}.

e) I viewed the generation of the CSR for {CA Name} and was informed that the resultant CSR incorporated the public key associated to the {CA Name} private key.

f) The fingerprint (hash value) of the CSR generated was ____.

g) I was informed by _________________, that the private key of {CA Name} is stored in a highly secure location (in the Hardware Security Module attached to the {Interoperability} CA {CA Name} machine) and I believe this.

Witnesses Attending

I verify that the following witnesses were present during the generation of the CSR:

- Witness 1 {name / organisation / nation}
- Witness 2 {name / organisation / nation}
- Witness x {name / organisation / nation}

Signatures

{Witness 1}	{Witness 2}
Signature___________________________	Signature___________________________
Name:______________________________	Name:______________________________
Nation:_____________________________	Nation:_____________________________
Date_________________{DD/MM/YYYY}	Date_________________{DD/MM/YYYY}

SIGNING OF THE PRINCIPAL CROSS-CERTIFICATE

I ________________________________ of _____________________________ do hereby certify that:

a) On the <date>_____________, I attended the {Nation} Defence PKI Facility within the {Facility Name} which is part of the {Name of Defence Department}, at {Location}.

b) I was informed by __________________________, and believe it to be true that:

   i. The {Interoperability} CA servers shown to me were located in a secure cabinet within a secured room within the PKI Facility,

   ii. the {Interoperability} CA servers had been checked immediately prior to my attendance for viruses, worms, trojans and malicious codes, and none were found,

   iii. nothing had occurred since this check to change this belief that the servers were free of viruses, worms, trojans and malicious codes, and

   iv. the {Interoperability} CA servers are operating with dedicated hardware and software that would generate their own private and public keys.

c) I confirmed that the fingerprint (hash value) of the CSR used to generate the Principal Cross-Certificate was ____________________________________ and this has the same fingerprint as originally witness and recorded at the generation of the CSR.

d) Immediately, after being informed of this information by _____________________, I saw ________________________ operate the {Interoperability} CA server and generate a signed Principal Cross-Certificate, with a Distinguished Name of:______________________________________ and fingerprint (hash value) of: ______________________________________

e) The lifetime of the Principal Cross-Certificate that I witnessed being generated is from

____________________, to __________________.

f) At no time did I see the private keys of {CA Name}.

Witnesses Attending

I verify that the following witnesses were present during the signing of the Principal Cross-Certificate:

Uncontrolled copy when printed

- Witness 1 {name / organisation / nation}
- Witness 2 {name / organisation / nation}
- Witness x {name / organisation / nation}

Signatures

{Witness 1}	{Witness 2}
Signature____________________________	Signature____________________________
Name:______________________________	Name:______________________________
Nation:______________________________	Nation:______________________________
Date__________________{DD/MM/YYYY}	Date__________________{DD/MM/YYYY}

GLOSSARY OF TERMS AND ACRONYMS

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.

Bridge CA — A bridge CA acts as a trust point for multiple cross-certifications; normally a bridge CA will not have any subordinate CAs

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 Certificate
Certificate issued to a CA.

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.
End entity	The end entity is often termed a Subscriber.
Entity Certificate.	Certificate issued to a Subscriber or end-entity.
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 Escrow Server	Subsystem of a Certificate Authority which stores private keys associated with certificates with a key usage of key-encypherment or data-encypherment.
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/Defence 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.
Principal Cross-Certificate	A cross-certificate that contains a policy mapping.
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.

Root Certificate A certificate belonging to the trust anchor. The root of the certificate path.

Secondary Cross-Certificate A cross-certificate that does not contain a policy mapping.

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.

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.

Trust Anchor
The trust anchor for the path. This will always be a self-signed certificate – i.e. a root CA.

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.

ACRONYMS

ACP	Allied Communication Publication
AIA	Authority Information Access
CA	Certification Authority
CAS	Certificate Authority System
CCA	Cross-Certification Arrangement
CCEB	Combined Communications Electronics Board
CJM3IEM	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
CP	Certificate Policy
CPMC	CP Mapping Criteria
CPS	Certificate Practice Statement
CSA	Certificates Status Authority
CSR	Certificate Signing Request
DN	Distinguished Name
DoD	Department of Defence
DSA/DSO	Defence Security Authority/ Defence Security Organisation
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IP	Internet Protocol

KES	Key Escrow Server
LDAP	Lightweight Directory Access Protocol
NDPKI	National Defence PKI
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure (X.509)
PMA	Policy Management Authority
RA	Registration Authority
RDN	Relative Distinguished Name
RFC	Request for Comments
RSA	Rivest, Shamir, Adleman (encryption algorithm)
SHA	Secure Hash Algorithm