INMARSAT CERTIFICATE PRACTICE STATEMENTE

ENTERPRISE PUBLIC KEY INFRASRCUTURE

Business Owner	Document Author	Approved by	Authorised by
Dimitar Stoyanov *Director* *Security Architecture and Engineering*	Stephen Savory *Security Operations Engineer* *Security Engineering*	Maurizio Caruso *Senior Director* *Security strategy, Governance and risk Management*	Graham Wright *Senior Vice President* *Global Security and Cyber*

DOCUMENT HISTORY

Issue	Reason for Change	Modified by	Date
0.1	Initial draft	Simon Cresdee	07/05/2021
0.2	First Review	Steve Savory	07/06/2021
0.3	Group Review	Steve Savory	23/06/2021

CHANGE CONTROL

Requests for changes to this document must be sent to the Secretary of the Security Policy Approval Board at PAB-Sec@inmarsat.com, providing details of the required change and the reason for the change being requested. The changes to the Policy have been captured in the respective response log maintained under the Security Policy Approval Board Teamspace.

REVIEW PERIOD

This document is to be reviewed within twelve months of issue and every twelve months thereafter. It may be subject to review at other times as dictated by changing operational or business needs, legal and regulatory obligations.

Table of Contents

ENTERPRISE PUBLIC KEY INFRASRCUTURE 1

1. INTRODUCTION 7

1.1. Overview 7

1.2. Document name and identification 7

1.3. PKI Participants 8
1.3.1. Certification Authorities 8
1.3.2. Registration Authority 8
1.3.3. Subscribers (End Entities) 9
1.3.4. Relying Party 9
1.3.5. Other Participants 9

1.4. Certificate Usage 10
1.4.1. Appropriate Certificate Uses 10
1.4.2. Prohibited Certificate Uses 10

1.5. Policy Administration 11
1.5.1. Organisation Administering this Document 11
1.5.2. Contact Person 11
1.5.3. Person Determining CPS Suitability for the Policy 11
1.5.4. CPS approval procedures 11

1.6. Definitions and Acronyms 11
1.6.1. Definitions 11
1.6.2. Acronyms 12

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 13

2.1. Repositories 13

2.2. Publication of Certification Information 13

2.3. Time or Frequency of Publication 14

2.4. Access Controls on Repositories 14

3. IDENTIFICATION AND AUTHENTICATION 15

3.1. Naming 15
3.1.1. Types of Names 15
3.1.2. Need for Names to be Meaningful 15
3.1.3. Anonymity or Pseudonymity of Subscribers 15
3.1.4. Rules for Interpreting Various Name Forms 16
3.1.5. Uniqueness of Names 16
3.1.6. Recognition, Authentication, and role of Trademarks 16

3.2. Initial Identity Validation 16
3.2.1. Method to Prove Possession of Private Key 16
3.2.2. Authentication of Organisation Identity 16
3.2.3. Authentication of Individual Identity 17
3.2.4. Non-verified Subscriber information 17
3.2.5. Validation of Authority 17

3.2.6. Criteria for Interoperation 17

3.3. Identification and Authentication for Re-Key Requests 17
3.3.1. Identification and Authentication for Routine Re-Key 18
3.3.2. Identification and Authentication for Re-Key after Revocation 18

3.4. Identification and Authentication for Revocation Request 18

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 19

4.1. Certificate Application 19
4.1.1. Who can submit a Certificate Request/Application 19
4.1.2. Enrolment Process and Responsibilities 19

4.2. Certificate Application Processing 19
4.2.1. Performing Identification and Authentication functions 19
4.2.2. Approval or Rejection of Certificate Applications 20
4.2.3. Time to Process Certificate Applications 20

4.3. Certificate issuance 20
4.3.1. CA Actions during Certificate Issuance 20
4.3.2. Notification to Subscriber by the CA of Issuance of Certificate 20

4.4. Certificate Acceptance 21
4.4.1. Conduct Constituting Certificate Acceptance 21
4.4.2. Publication of the Certificate by the CA 21
4.4.3. Notification of Certificate Issuance by the CA to other Entities 21

4.5. Key Pair and Certificate Usage 21
4.5.1. Subscriber Private Key and Certificate Usage 21
4.5.2. Relying Party Public Key and Certificate Usage 22

4.6. Certificate renewal 22
4.6.1. Circumstance for Certificate Renewal 23
4.6.2. Who May Request Certification Renewal 23
4.6.3. Processing Certificate Renewal requests 23
4.6.4. Notification of New Certificate Issuance to Subscriber 23
4.6.5. Conduct Constituting Acceptance of a Renewal Certificate 23
4.6.6. Publication of the renewal certificate by the CA 23
4.6.7. Notification of Certificate Issuance by the CA to other Entities 23

4.7. Certificate Re-Key 23
4.7.1. Circumstance for Certificate Re-Key 23
4.7.2. Who May Request Certification of a New Public Key 24
4.7.3. Processing Certificate Re-Keying Requests 24
4.7.4. Notification of New Certificate Issuance to Subscriber 24
4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate 24
4.7.6. Publication of the Re-Keyed Certificate by the CA 24
4.7.7. Notification of Certificate Issuance by the CA to Other Entities 24

4.8. Certificate modification 24
4.8.1. Circumstances for Certification Modification 25
4.8.2. Who May Request Certificate Modification 25
4.8.3. Processing Certificate Modification Requests 25
4.8.4. Notification of New Certificate Issuance to Subscriber 25
4.8.5. Conduct Constituting Acceptance of Modified Certificate 25
4.8.6. Publication of the Modified Certificate by the CA 25
4.8.7. Notification of Certificate Issuance by the CA to Other Entities 25

4.9. Certificate Revocation and Suspension 25

4.9.1. Circumstances for Revocation 26
4.9.2. Who can Request Revocation 26
4.9.3. Procedure for Revocation Request 26
4.9.4. Revocation Request Grace Period 27
4.9.5. Time within which the CA must Process the Revocation Request 27
4.9.6. Revocation Checking Requirement for Relying Parties 27
4.9.7. CRL Issuance Frequency 27
4.9.8. Maximum Latency for CRLs 27
4.9.9. On-line Revocation/Status Checking Availability 28
4.9.10. On-line Revocation Checking Requirements 28
4.9.11. Other Forms of Revocation Advertisement Available 28
4.9.12. Special Requirements Re-Key Compromise 28
4.9.13. Circumstances for Suspension 28
4.9.14. Who can Request Suspension 28
4.9.15. Procedure for Suspension Request 28
4.9.16. Limits on Suspension Period 28

4.10. Certificate Status Services 28
4.10.1. Operational Characteristics 28
4.10.2. Service Availability 28
4.10.3. Optional features 28

4.11. End of subscription 28

4.12. Key Escrow and Recovery 29
4.12.1. Key Escrow and Recovery Policy and Practices 29
4.12.2. Session Key Encapsulation and Recovery Policy and Practices 29

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 30

5.1. Physical controls 30
5.1.1. Site Location and Construction 30
5.1.2. Physical Access 30
5.1.3. Power and Air Conditioning 30
5.1.4. Water Exposures 30
5.1.5. Fire Prevention and Protection 31
5.1.6. Media Storage 31
5.1.7. Waste Disposal 31
5.1.8. Off-Site Backup 31

5.2. Procedural Controls 31
5.2.1. Trusted roles 31
5.2.2. Number of Persons Required per Task 34
5.2.3. Identification and Authentication for Each Role 34
5.2.4. Roles Requiring Separation of Duties 35

5.3. Personnel controls 35
5.3.1. Qualifications, Experience, and Clearance Requirements 35
5.3.2. Background Check Procedures 35
5.3.3. Training requirements 36
5.3.4. Retraining Frequency and Requirements 36
5.3.5. Job Rotation Frequency and Sequence 37
5.3.6. Sanctions for Unauthorised Actions 37
5.3.7. Independent Contractor Requirements 37
5.3.8. Documentation Supplied to Personnel 37

5.4. Accounting Logging Procedures 37
5.4.1. Types of Events Recorded 37
5.4.2. Frequency of Processing Log 40
5.4.3. Retention period for Audit Log 40

5.4.4. Protection of Audit Log 41
5.4.5. Audit Log Backup Procedures 41
5.4.6. Audit Collection System (internal vs. external) 41
5.4.7. Notification to Event-Causing Subject 42
5.4.8. Vulnerability assessments 42

5.5. Records Archival 42
5.5.1. Types of Records Archived 42
5.5.2. Retention Period for Archive 43
5.5.3. Protection of Archive 43
5.5.4. Archive Backup Procedures 43
5.5.5. Requirements for Time-Stamping of Records 43
5.5.6. Archive Collection System (internal or external) 43
5.5.7. Procedures to Obtain and Verify Archive Information 43

5.6. Key Changeover 43

5.7. Compromise and Disaster Recovery 43
5.7.1. Incident and Compromise Handling Procedures 44
5.7.2. Computing Resources, Software, and/or Data Corruption 44
5.7.3. Entity Private Key Compromise Procedures 44
5.7.4. Business continuity capabilities after a disaster 44

5.8. CA or RA termination 44

6. TECHNICAL SECURITY CONTROLS 46

6.1. Key Pair Generation and Installation 46
6.1.1. Key pair generation 46
6.1.2. Private Key Delivery to Subscriber 46
6.1.3. Public Key Delivery to Certificate Issuer 46
6.1.4. CA Public Key Delivery to Relying Parties 46
6.1.5. Key Sizes 46
6.1.6. Public Key Parameters Generation and Quality Checking 46
6.1.7. Key Usage Purposes (as per X.509 v3 key usage field) 46

6.2. Private Key Protection and Cryptographic Module Engineering Controls 47
6.2.1. Cryptographic Module Standards and Controls 47
6.2.2. Private Key (n out of m) multi-person control 47
6.2.3. Private Key Escrow 47
6.2.4. Private Key Backup 47
6.2.5. Private Key Archival 47
6.2.6. Private Key Transfer into or from a Cryptographic Module 47
6.2.7. Private Key Storage on Cryptographic Module 48
6.2.8. Method of Activating Private Key 48
6.2.9. Method of Deactivating Private Key 48
6.2.10. Method of Destroying Private Key 48
6.2.11. Cryptographic Module Rating 48

6.3. Other Aspects of key Pair Management 49
6.3.1. Public Key Archival 49
6.3.2. Certificate Operational Periods and Key Pair Usage Periods 49

6.4. Activation data 49
6.4.1. Activation Data Generation and Installation 49
6.4.2. Activation Data Protection 49
6.4.3. Other Aspects of Activation Data 49

6.5. Computer Security Controls 49
6.5.1. Specific Computer Security Technical Requirements 50

6.5.2. Computer Security Rating 50

6.6. Life Cycle Technical Controls 50
6.6.1. System Development Controls 50
6.6.2. Security Management Controls 50
6.6.3. Life Cycle Security Controls 50

6.7. Network Security Controls 51

6.8. Time-Stamping 51

7. CERTIFICATE, CRL, AND OCSP PROFILES 52

7.1. Certificate Profile 52
7.1.1. Version Number(s) 52
7.1.2. Certificate Extensions 52
7.1.3. Algorithm Object Identifiers 52
7.1.4. Name Forms 52
7.1.5. Name Constraints 53
7.1.6. Certificate Policy Object Identifier 53
7.1.7. Usage of Policy Constraints extension 53
7.1.8. Policy Qualifiers Syntax and Semantics 53
7.1.9. Processing semantics for the critical Certificate Policies Extension 53

7.2. CRL profile 53
7.2.1. Version number(s) 53
7.2.2. CRL and CRL entry extensions 53

7.3. OCSP profile 53
7.3.1. Version Number (s) 53
7.3.2. OCSP Extensions 53

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 54

8.1. Frequency or Circumstances of Assessment 54

8.2. Identity/Qualifications of Assessor 54

8.3. Assessor's Relationship to Assessed Entity 54

8.4. Topics Covered by Assessment 54

8.5. Actions taken as a Result of Deficiency 55

8.6. Communication of Results 55

9. OTHER BUSINESS AND LEGAL MATTERS 56

10. ANNEX A – DEFINITIONS 57

11. ANNEX B – ACRONYMS 59

12. REFERENCES 60

1. INTRODUCTION

This Inmarsat Intermediate Certificate Practice Statement (II-CPS) defines the operational and management practices used within the Inmarsat Intermediate Certification Authority (CA) and Registration Authority (RA) that manages all certificate requests from all Issuing CAs within the 3rd tier. Inmarsat engineering services will manage the Certification Authority (CA) operation, issuing and managing certificates within the Intermediate tier in accordance with the overarching governance, Inmarsat Certificate Policy (ICP).

The Intermediate tier has two CA services, for Production and Non-Production. This CPS shall encompass both CA servers within the 2nd tier.

The ICP is overarching governance controlled by Inmarsat PKI Management Group (**IPMG**) for the overall usage of digital certificate(s) for issuance to computers, applications, and devices.

This II-CPS defines criteria for the issuance and management of X.509 digital certificates being created and issued for live service, pertaining to Subscribers/End-Entities (Issuing CA tier) within the Inmarsat environment. The Intermediate Certificate Authority servers will be granted on acceptance of this II-CPS, to issue to internal Issuing CAs within the 3rd tier, excluding external replying parties.

Note: *Clarification of Subscribers/End-Entities and Relaying Parties is document further within this II-CPS document.*

This II-CPS and its operation will be approved by **IPMG** allowing the Intermediate CA to become the trusted anchor of the hierarchical trust model that all Issuing CAs including their end-entities will inherently trust these Intermediate-CAs. It is implied that all subscribers within the Inmarsat hierarchy trust the Inmarsat Root CA.

1.1. Overview

The new Inmarsat certificate environment will provide x.509 certificates secure web services, data channels and trust identification. These service types are the primary subscribers for certificates.

This Inmarsat Intermediate CPS (II-CPS) describes the Inmarsat certificate service, which operates under the Inmarsat Certificate Policy (ICP) governance, and describes the service certificate, governance, management and provides capabilities for supporting the overall Intermediate CA service:

- Certificate Authority (CA)
- Registration Authority (RA)
- Validation Authority (VA) (Repository servers)

The Intermediate Certificate Authority is based on OpenSSL Certificate Services, using nCipher nShield Connect Hardware Security Modules (HSM) which is a network based HSM. The Intermediate CA server will be a standalone service and shall not have any local network connections. All methods of data transfer to the Intermediate CA server shall be approved and managed by network controls.

If used USB drive shall and must be virus scanned prior to inserting to the local management device, prior to data transfer to the Intermediate CA server. USB drive may only be used for CSR transfer to the off-line Root CA.

1.2. Document name and identification

This document is referred to as the '**Inmarsat – Intermediate CA Certificate Practice Statement**'. Currently level of publication is as follows: **Live**

The registered Object Identifier (OID) of this CPS is **1.3.6.1.4.1.1840.60.2.1**

It is explicitly prohibited to assert any policy OID not listed above within any certificate.

The certificate server deployment shall use the following associated OIDs for 2048 key lengths and SHA256 hashes:

Policy Name	Assigned OID
Medium Level Assurance	1.3.6.1.4.1.1840.60.2.1

Table 1 - Policy OIDs Used

1.3. PKI Participants

There are two (2) main participant roles within this Intermediate CA certificate services deployment: CA service owners and local RA operators. Both roles are operated by authorised personnel within the respective trusted roles. **See Section** Error! Reference s ource not found. [*Error! Reference source not found.*]

This section provides a hierarchical overview and defines the relationships between Inmarsat Intermediate CA services and owners, and the governance of the Inmarsat PKI Management Group (**IPMG**). These participants are described in **Section** Error! Reference s ource not found. [*Error! Reference source not found.*].

1.3.1. Certification Authorities

The Inmarsat Intermediate certificate environment is the 2nd tier of a three-tier hierarchy. Certificate Authority referenced within this Intermediate CA CPS are the Inmarsat Intermediate CA service.

Note: Other Intermediate CAs if permitted by the **IPMG** outside of this CPS, shall be under the governance of the Inmarsat Certification Policy governing all Inmarsat certificate services.

Inmarsat Certificate Intermediate tier service governance, is operated by Inmarsat PKI Management Group (**IPMG**), and deemed responsible for the following:

- Creation and subsequent updates to the Inmarsat Certificate Policy (ICP)
- Identifying the need for this CPS pertaining to intermediate CA services and ensuring creation and updated as and when required
- Review this Certification Practice Statements (CPS) participants to ensure compliance with the Inmarsat Certificate Policy
- Review the results of compliance audits ensuring Inmarsat Intermediate Certificate Authority participants are meeting the requirements as stipulated in approved CPS document(s)
- Direct the Certificate Authority participants regarding corrective actions or other measures that might be appropriate such as revocation of CA certificates

1.3.2. Registration Authority

The Intermediate service local Registration Authority (RA) is delegated to IT Security Engineering operators:

- Identification of all certificate recipients and their sponsor prior to issuance, in accordance with the general policy defined in the ICP and as specified within this II-CPS
- Verification of key-pair ownership
- Submission of certificate requests for processing and creation

- Maintenance of a suitable audit mechanism, acceptable to the **IPMG**, to demonstrate continued compliance with this CPS

The local Registration Authority (RA) is responsible for validating all requests for certificate revocation and relaying the authorised request for specific certificate revoke.

The certificate service does not provide an interface for Sponsors to allow certificate enrolment, without using the Inmarsat Intermediate RA service. A Sponsor of any Inmarsat Intermediate CA is responsible and accountable issuing certificates in accordance with certificate policy asserted within the certificate.

The Validation Authority (VA) service operated as part of the CA service also includes Repository services. The VA service is used to host certificate status information, this being Certificate Revocation and Authority Information.

1.3.3. Subscribers (End Entities)

A Subscriber is the entity whose name appears as the Subject Name within the certificate. The key usage and any associated extended key usage are in accordance with the certificate policy asserted within the certificate.

Direct recipient of the Intermediate CA service is that of the Issuing CA services. However, the subscribers/End-Entities who shall consume certificate services are defined as follows:

- **Applications**: Such as web services requiring Transport Layer Security (HTTPS), or secure data channels using Virtual Private Network using IPsec (VPN) (IP Security)
- **Computer**: workstation, server, laptop or any other mobile computer for client or server authentication
- **Devices**: hardware items requiring a certificate to provide trusted networking capability such as 801.1x

1.3.4. Relying Party

A Relying Parties (RR) will be all end-entities that have received a signed digital certificate from the Inmarsat certificate service. Within Inmarsat environment validation of any issued digitally signed certificates using the certificate revocation path for verification of revocation status. Inmarsat Certificate Service (from all Certificate Authorities) will make available to Relying Parties the most current revocation status i.e., revocation information is within date and is accessible.

Note: Currently this CPS does not have any external Relying Parties outside of Inmarsat. If requirement changes this CPS must be updated to reflect change

A certificate must not be trusted if it is found to be invalid for any reason, or cannot be accessed, processed, or authenticated. Reliance must be made on the relying party's operating system or application capability of chaining and checking a certificates validation status.

A Relying Party shall use information in the certificate (such as certificate policy identifiers or key usage statements) to determine the suitability of the certificate for a particular use.

For Relying Parties: Use of REVOKED certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new Revocation data should be obtained is a determination to be made by the relying party and the system Accreditor.

1.3.5. Other Participants

Inmarsat Policy Management Group (**IPMG**). A body established by Inmarsat to be responsible for the following:

- Creation and update of the Inmarsat Certification Policy (ICP)
- Identifying the need for other CPS pertaining to other Inmarsat CA services and ensuring CPS's are created and on-going review cycle
- Approve CPS of any Inmarsat CA service participants following review by the **IPMG**, to ensure compliance with the ICP
- Reviewing the results of compliance audits to determine that Inmarsat CA service participants are adequately meeting the stipulations of approved CPS documents, and direct the participants regarding corrective actions, or other measures that might be appropriate, such as revocation of CA certificates

Certificate Manufacturing (CM) this is not a strict PKI role, but is part of the overall CA service owners and resides alongside the local Registration Authority. The CM role of activities are for the purpose of this CPS are performed by the IT Security Group are as follows:

- Respond to authorise valid request(s) for issuance by processing a certificate request in accordance with the appropriate certificate profiles, containing the subject identity and other information that have been defined in the request
- Respond to authorised requests that have been processed and awaiting approval to be issued
- Publishing to requestors their certificates and make available to the Subscribers and Relying Parties upon request
- Respond to authorised revocation request by publishing details of the revoked certificate within certificate service; revocation status information will be issued to the Validation Authority, in the form of an update Certificate Revocation List (CRL)

The Certificate Authority server are based on Ubuntu Server, using OpenSSL certificate services. Each CA Intermediate server will connect through to an nCipher nShield Connect Hardware Security Module (HSM) to support the management and storage of the CA's private key.

1.4. Certificate Usage

Inmarsat certificate service shall use digitally signed certificates for identity of other CA servers.

Usage assurance level will be medium assurance in accordance with the Inmarsat Certification Policy (ICP)

1.4.1. Appropriate Certificate Uses

CA service is limited to providing certificates to support to further CA server services:

- Certificate Signing, CRL Signing

This Intermediate CA service is prohibited from signing any direct End-Entity certificate request. This Intermediate CA service is limited to signing only CA servers classified as Intermediate or Issuing status and approved by the **IPMG**.

1.4.2. Prohibited Certificate Uses

Use of certificate(s), other than those listed in the **Section 1.4.1** [***Appropriate Certificate Uses***] are prohibited. All subscribers (Issuing) to the Inmarsat certificate service are bound by these limitations of certificate usage. Any Relying Parties shall not engage in any transaction where a certificate issued by the Inmarsat Intermediate CA is used, or proposed for use, for any purpose not listed in **Section 1.4.1** [***Appropriate Certificate Uses***].

Certificate use will be verified by the Intermediate CA local RA prior to submission for a new certificate. Any certificates required outside of the above governance will be required to seek allowance from the **IPMG** policy.

1.5. Policy Administration

1.5.1. Organisation Administering this Document

Inmarsat IT Security group as service owners in conjunction with **IPMG** are responsible for the implementation, assurance, and day-to-day management of the certificate environment. This includes documents, infrastructure equipment and personnel.

1.5.2. Contact Person

Questions and comments regarding this CPS should be directed to:

Object	Description
Person	Cert Admin
Department	Global Security Group
Address	99 City Road, London, EC1Y 1AX
Electronic Mail	certadmin@inmarsat.com

Table 2 – II-CPS Contact Person

1.5.3. Person Determining CPS Suitability for the Policy

This Intermediate CA CPS is produced by Inmarsat IT Security team and is approved by the **IPMG**. **IPMG** are responsible for determining the suitability of this Intermediate CA CPS document.

1.5.4. CPS approval procedures

Prior to submission of this II-CPS to **IPMG**, it shall be peer reviewed and versioned accordingly to editorials.

Approval procedures are as follows:

- II-CPS will be submitted to the **IPMG** for ratification and approval
- If rejected by **IPMG** will provide comments directing to areas of non-compliance or areas of concern. Uplift in version of this II-CPS reflecting comments and changes
- Document reviewed by IT Security Engineering prior to re-submission to **IPMG**
- If acceptance is given, **IPMG** will recommend approval to the contact defined in table 6 by means of written confirmation.

1.6. Definitions and Acronyms

This section lists all the definitions and acronyms including their meaning that will be used within this II-CPS.

1.6.1. Definitions

Definitions are in **Annex A**

1.6.2. Acronyms

Acronyms are located in **Annex B**

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Repositories

Certificate service repositories are managed by the Intermediate CA service owners who operate the overall Intermediate CA management and issuance. The certificate repositories are part of the Validation Authorities (VA) which are hosted on behalf of the Intermediate CA service. These AWS S3 buckets are available throughout the Inmarsat organisation and publicly for Inmarsat customers.

All repositories are available for access 24x7 by all consumers and end-entities of the Inmarsat certificate service.

2.2. Publication of Certification Information

Information about regarding the Inmarsat Intermediate CA certificate service shall be published to repositories, used to host, and publish certificate information such as this II-CPS, CA Intermediate server certificates and Intermediate CA Certificate Revocation List files plus any other information relating to the overall certificate service.

Note: *All Intermediate CA publish their own CRL and certificate. There will be an automated process using the repositories to host Intermediate CA service information making available to all end-entities and relying parties.*

Multiple repositories will publish the Intermediate CA certificate and CRL within the Inmarsat environment for End-Entities and relying parties to validate the certificate itself or download into their cert store for certificate chaining. This will be the AWS S3 buckets.

Note: *At the time of writing, the URL's listed may be subject to change.*

Intermediate CA certificate will be published via the Authority Information Access (AIA) URI:

Description	AIA Locations for URI
Inmarsat Prod Intermediate CA01	http://ca.inmarsat.com/inmintprodca01.crt
Inmarsat NonProd Intermediate CA01	http://ca.inmarsat.com/inmintnonprodca01.crt

Table 3 - AIA Locations URI

The Inmarsat ICP and this II-CPS will be available to all subscribers and end-entries.

Description	CPS URL
Inmarsat Prod Intermediate CA01	http://ca.inmarsat.com/inmintprodca01-cps.pdf
Inmarsat NonProd Intermediate CA01	http://ca.inmarsat.com/inmintnonprodca01-cps.pdf

Table 4 - CPS Location

It will be the responsibility of Intermediate CA service owners to verify that publication of CRL file is published and made available.

The certificate revocation lists (CRL) are available at the following locations:

Description	CDP Website URI
Inmarsat Prod Intermediate CA01	http://ca.inmarsat.com/inmintprodca01.crl

Inmarsat NonProd Intermediate CA01	http://ca.inmarsat.com/inmintnonprodca01.crl

Table 5 - CDP Locations for URI

2.3. Time or Frequency of Publication

Information that is available in repositories is published within the given time that is agreed with the authorities.

Type	Publication Requirement
Intermediate Certificate	Made available after CA server install or after re-new/re-key
Intermediate CA CRL	Every six (6) weeks
Certificate Policy	Made available post approval after updates
Certificate Practice Statement	Made available prior to certificate issuance

Table 6 - Frequesncy Publication

All CRL information is published to the Validation Authority repositories for publication to web services located on the VA server.

The CA servers will be configured as an automatic task unless a certificate revocation has taken place.

2.4. Access Controls on Repositories

Intermediate CA service owners are required to publish or remove not only CRL files, but also other file types, which are published as part of the certificate service. CA service owners who operate the day-to-day running will be granted publish rights for CRL repository location when a manual issue of the CRL is required.

For the Intermediate CA service owners shall manually publish the CRL file allowing access to all subscriber/end-entities or Relying Parties. These non-CA servers have read-only access to validate a certificate revocation status or a CA server certificate.

Access control will be a Role Based Access Control limiting persons to manage each repository hosting any certificate information.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

This section identifies the naming and identification of the Inmarsat certificate issuance environment.

3.1.1. Types of Names

All certificates issued by the Inmarsat CAs will have an unambiguous, clearly distinguishable, and unique X.501 Distinguished Name (DN) in the certificate 'subject name' field in accordance with the Inmarsat CP.

Any DN used will be in the form of a X.501 *UTF8String* or *PrintableString* and will not be a null entry.

Optionally, each entity may use one or more alternative names via the *subjectAltNam*e, certificate extension field in accordance with RFC5280.

The subject names are constrained by the name constraints in the issuing CA certificate. Thus, all subject names in end-entity certificates issued by the CA will conform to the formatting shown below:

- O=Inmarsat, C=GB
- OU=Group Security, O=Inmarsat, C=GB
- OU=Group IT, O=Inmarsat, C=GB
- OU=PG, O=Inmarsat, C=GB

3.1.2. Need for Names to be Meaningful

All subscribers presenting a certificate request to the Inmarsat Intermediate CAs must ensure that the Subject Name is a meaningful Common Name (CN), Domain Naming Service (DNS) and/or Distinguished Name (DN). It must be unique and valid for the security domain the subscriber/end-entity resides in. The DNS name entry used for any certificate issued will have the fully qualified name displayed:

- *hostname*.XX.inmarsat.com
- *alias*.XX.inmarsat.com

Subject Alternate Name, if used must have the full DNS entry of the hostname and/or alias.

Issuing CA server names will be defined on every certificate as the issuer, and will be unique and meaningful when requesting its own certificate to the Intermediate CA.

The Common Name component of a Subject name shall always contain sufficient information to identify the end-entity uniquely, and unambiguously within the Inmarsat environment. The use of wildcard (*) certificates will not be issued by the Inmarsat CA service owners or local RA and are specifically forbidden by policy.

3.1.3. Anonymity or Pseudonymity of Subscribers

Inmarsat local Registration Authority will not accept or issue anonymous certificate request from end-entities without the consent of **IPMG**. Certificates with subject name using a Pseudonym requiring to be issued, must contain an individual reference that shall identify the end-entity that controls or maintains the private keys.

All requests will be within the Inmarsat environment and all end-entities shall register with the Inmarsat local RA prior to certificate request, removing the ambiguity of anonymity.

All and every certificate must be traceable to host and requestor (namely responsible person).

3.1.4. Rules for Interpreting Various Name Forms

All names used within certificates issued by the Inmarsat Intermediate CAs shall be interpreted in the context of the approved namespace, unique and unambiguous.

3.1.5. Uniqueness of Names

Inmarsat Intermediate Registration Authority will ensure that all names are unique within its scope, prior to issuance of any certificate. The CA servers cannot check duplicate subject names and therefore cannot reject duplicate subject names. The namespaces employed by the Inmarsat CA service owners are elaborated in **Section 7.1.5** [***Name Constraints***]

3.1.6. Recognition, Authentication, and role of Trademarks

Names used within the Inmarsat certificate environment have been agreed prior to implementation. There no trademarks issues with current names used within the Inmarsat CA service. IT Security Engineering CA service owners shall defer all matters relating to trademarks to the **IPMG**. Additionally, interested parties must be notified such as the local RA and device owners/sponsors.

3.2. Initial Identity Validation

This section contains the elements for the identification and authentication procedures for the initial registration of each subject type such as CA, RA, and other participants as subscribers.

3.2.1. Method to Prove Possession of Private Key

Possession of the private keys for the Inmarsat Intermediate CA servers are in line with CA implementation Procedures – **Prod Intermediate CA Key Signing Document**:

- Intermediate CA server shall produce a self-signed certificate – Date/time recorded for audit
- Intermediate CA server self-signed certificate shall be matched with private key that corresponds to the public keys
- Private Key is stored within the nCipher NShield Connect Hardware Security Module.

Certificate binds to a public key to the identity of the individual to assure Relying Parties that encryption or signing performed by the private key was done by the individual whose public key appears on the Certificate.

This II-CPS for the Inmarsat Intermediate CA shall only sign certificate Signing Requests (CSR) from intermediates CA services where the private key remains with the requesting intermediate. Public Key sent as part of the CSR, shall be paired upon receipt of a signed certificate. Intermediate CA service owners must satisfy themselves that the signed request matches that of the private key retained.

It will be the responsibility of the Inmarsat Intermediate RA to ensure certificate requests are returned to the requesting intermediate CA server. This paring shall provide device possession of private keys.

Manual creation of certificates prohibited within the constraints of this CPS.

3.2.2. Authentication of Organisation Identity

The authentication of organisational identity for devices that exist within the Inmarsat environment is deemed by virtue being either part of the directory service or an owned device within Inmarsat.

The Inmarsat RA shall validate requests by verifying:

- Application request type: Computer
- Its association to the within the Inmarsat environment/infrastructure
- Sponsor/Owner of the intermediate requesting a certificate

3.2.3. Authentication of Individual Identity

A Sponsor and/or Owner shall be an individual to whom the intermediate CA server(s) are attributable for the purposes of accountability and responsibility. The Intermediate CA for purpose of this CPS shall be owned as part of the Inmarsat infrastructure environment.

Intermediate CA service owners shall take steps to ensure that the sponsor and/or Owner is authorised to request on behalf of the intermediate CA service. Requests received from an intermediate outside the Inmarsat environment or systems will be rejected.

The Intermediate CA local RA shall keep a record of certificate requests submitted, and details of identification and authorisation checks used to authorise a request.

During first enrolment, all subscribers/end-entities will have been documented as and when their certificate is issued. The documented name source shall be used to verify existing subscribers for re-enrolment.

3.2.4. Non-verified Subscriber information

All Subscriber information on the request form and the certificate request file shall be verified. Non-verified Subscriber information or any subscriber information not compliant shall not have their certificate issued.

3.2.5. Validation of Authority

Certificates issued will not contain explicit or implicit organisation affiliations except where this Intermediate CA service owners have been authorised to act on behalf of organisation. For the Inmarsat certificate environment, the certificate issued shall be authorised to act on behalf of the Inmarsat organisation.

Only valid persons within the Inmarsat environment will be granted authority to submit requests to the CA service. All granted authorities shall be named and stated in each respective CPS for all certificate issuances.

All other rights and entitlements are related to the operation of the certificate server itself.

Authority persons:

- Requestors (persons who operate servers, devices)
- Submitters (persons who submit requests to this Intermediate CA service)
- Approvers (persons who approve the certificate submissions to this Intermediate CA service)

3.2.6. Criteria for Interoperation

There are no provisions in the scope of this Intermediate CA CPS for interoperation of the CA service with or to other external parties. Meaning cross-certification is not permitted.

Note: *In the event certificate cross-certification is permitted, this Intermediate CA CPS must be updated to reflect the change.*

3.3. Identification and Authentication for Re-Key Requests

Re-Key requests can be split into two sections, re-key for either intermediate CAs and/or end-entities.

The Intermediate CA re-key is the production of a new Self-signed Intermediate certificate. This shall extend the validity date.

3.3.1. Identification and Authentication for Routine Re-Key

A request for re-key of an intermediate certificate may only be made by the subscriber whose name appears within the certificate that was originally issued and remains unchanged in the Subject Name and SAN. The Intermediate CA local RA shall carry out identification validation checks as per the initial enrolment process.

3.3.2. Identification and Authentication for Re-Key after Revocation

Where the information contained in the Intermediate CA certificate has changed or there is a known or suspected compromise of the private key, the Intermediate CA service owner should apply for a new certificate as per any certificate registration. A certificate if still valid will be revoked after acceptance of a replacement certificate. Any change in the information contained in a certificate shall be verified by the Intermediate CA local RA before the Intermediate CA certificate is re-issued.

Any intermediate CA service owners requesting a re-key shall be authenticated by means of initial enrolment. They must be enrolled as a requestor and have validity to submit request.

3.4. Identification and Authentication for Revocation Request

Revocation for a certificate is a non-reversible process and the requestor must be 100% sure the certificate in question is no longer needed.

The list of entities that can request revocation is described in **Section 4.9.2** [***Who can Request Revocation***]. The local RA shall authenticate a request for revocation of a certificate by validating their authority using the same methods as for initial enrolment. To validate the agreement to revoke the Intermediate CA server certificate the **IPMG** must agree the request for revocation.

Requests for revocation of certificates shall be included in the accounting log as described in **Section** □.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

Management and issuance of certificates will be controlled by Intermediate CA service owners. This section only applies to only the Intermediate CA within the Inmarsat infrastructure environment.

4.1. Certificate Application

This section covers the requirements regarding certificate application:

- Who can submit a certificate request, such as a certificate subject to the local RA
- The enrolment process used to submit certificate applications
- Responsibilities in connection with this process.

4.1.1. Who can submit a Certificate Request/Application

An authorised sponsor/owner may request a X.509 certificate on behalf of an Issuing CA server **Section 3.2** [***Initial Identity Validation***].

Registration and issue of certificates will be controlled by local RA and CA service operators, respectively.

Submittance of an Issuing CA signing request must be an approved owner of any intermediate CA service.

4.1.2. Enrolment Process and Responsibilities

The Intermediate CA service owners will manage certificates for use by Inmarsat infrastructure environment. First time requests for enrolment, requests using the application or a computer-based certificate request process, via the local RA for Intermediate CA signing.

The Intermediate CA local RA are responsible for ensuring that certificates are only issued to intermediates whose identities have been confirmed. Sponsors who are authorised to request a certificate for the intermediates shall have verified the accuracy of the information in the request.

Responsibilities are defined in three areas:

- Sponsor/owner is responsible for ensuring that the end-entity is valid and authorised to participate in the Inmarsat environment.
- Local Intermediate RA operators are responsible for submitting requests to the Intermediate CA service for processing and then the issuance of certificate, having first validated the request.
- Intermediate CA service owners' team are responsible for processing correctly authorised certificate requests on the CA servers.

Manual enrolment takes place by the administrator who has been granted the right to generate a CSR and request a certificate, for the service being implemented.

4.2. Certificate Application Processing

This section is used to describe the procedure for processing certificate requests.

4.2.1. Performing Identification and Authentication functions

For each certificate request submitted by a sponsor the Inmarsat Intermediate CA local RA will verify that the information contained in the request is correct:

- Intermediate name has been disclosed by the sponsor
- Requested Subject and Subject-Alternative-Name(s) to be included in the certificate do not violate any namespace constraints

The certificate request type. i.e., Server Authentication or All Issuance/All Applications etc. Corresponds to the intermediate role/function, as notified by the sponsor. Certificate usage will be defined by the governing OID used within the attribute Key Usage/Extended Key Usage.

For a requested certificate, the owner would ordinarily be a person within the organisation operating the named computer.

The mechanisms for identification and authentication given in **Section 3.2** [***Initial Identity Validation***] will be used by the Inmarsat RA in determining the acceptability of the request.

4.2.2. Approval or Rejection of Certificate Applications

A certificate application will be approved by the Inmarsat Intermediate CA local RA subject to the requirements stated above **Section 4.2.1** [***Performing Identification and Authentication functions***].

A certificate application will be rejected if any of the requirements stated above in **Section 4.2.1** [***Performing Identification and Authentication functions***] cannot be satisfied.

A certificate application shall not be considered accepted until the certificate has been issued and published by the CA server.

All certificate applications are recorded by the Inmarsat Intermediate CA local RA and approval or rejection is logged against each request.

4.2.3. Time to Process Certificate Applications

There are three distinct elements to processing certificates. Initial enrolment, of the end-entity device, where the Certificate Signing Request (CSR) is created then placed in a queue for processing.

All certificate applications, submitted to the Inmarsat RA, will be returned to the Sponsor/Owner within an agreed timely manner. Time given does not include consultation between the Inmarsat RA and the Sponsor/Owner.

Working day shall be Mon-Fri 09:00hrs – 17:00hrs.

4.3. Certificate issuance

4.3.1. CA Actions during Certificate Issuance

Once the certificate application process is complete, and approved, the Inmarsat Intermediate CA local RA will submit the request to the CA Operators who will:

- For manual enrolment, create a certificate using the information contained in the off-line request, the CSR. CSR shall be processed against the respective certificate template if not stipulated in the request. Send the certificate to the RA for delivery to the requestor.
- Shall inspect and investigate failed certificate requests
- Validate, where values are included within the certificate request, that these are consistent with permitted values by the appropriate certificate profile.
- Update the accounting record to log the details of the enrolment.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

Where a certificate has been requested, a manual process by the Intermediate CA service owners will notify the sponsor/owners of the presented CSR from the local CA RA who in turn will notify the device owner of successful completion of the issuance. Notification can be made via e-mail or phone. It is the responsibility of the Intermediate CA local RA to arrange for the certificate to be passed to the Intermediate CA owner.

4.4. Certificate Acceptance

4.4.1. Conduct Constituting Certificate Acceptance

Conduct of the requestor will be deemed to constitute acceptance of the issued certificate. As such, conduct may include affirmative steps to indicate acceptance, actions implying acceptance, or a failure to object to the certificate or its content. Any failure of a certificate must be notified to the Intermediate CA local RA administrators and the requestor informed of actions.

Once a requestor has received the certificate, the requestor must accept process and validate the new certificate. The Intermediate CA service owners do not know when manually enrolled certificate has been accepted. The requestor must notify the Intermediate CA local RA of acceptance and validation. Once accepted the Intermediate CA local RA will assume operational status on the certificate until expired or revoked.

4.4.2. Publication of the Certificate by the CA

Issued certificates are not published to the local file system.

Issued certificate can be published to a local directory service. (Public key one)

4.4.3. Notification of Certificate Issuance by the CA to other Entities

The **IPMG** will be notified upon successful acceptance of the intermediate certificate server's certificate.

The CA service will log issuance of certificates to its end-entities for audit purposes and presented to **IPMG** if required.

4.5. Key Pair and Certificate Usage

4.5.1. Subscriber Private Key and Certificate Usage

All subscribers shall protect their private keys from unauthorised use or disclosure by third parties and shall use their private keys only as specified in the key usage extension of the corresponding certificate.

The Intermediate CA pertaining to this II-CPS shall be bound by the terms within the Inmarsat Certificate Policy and the following statements.

- Shall provide accurate information at sub-ca registration, including all communications to the **IPMG**
- Key pair shall be generated within the local CA server connected HSM
- Possession of private shall be always established, during the service of the Intermediate CA servers. A CA service cannot start unless private keys are available and accessible
- Private Key shall be contained within a Hardware Security Module that is network attached
- The private HSM shall ensure that only the CA server whose subject name appears on the certificate shall have access to the private key

- Only the CA server and the nominated crypto custodian(s) shall have access to the private keys maintained within the HSMs
- No activation data shall be made to any authorised persons
- All CA server certificate's shall be used in accordance with the Inmarsat Certificate Policy, and shall notify the Inmarsat RA of any changes, since enrolment
- Issuing CA operators shall notify the **IPMG** of any deviation or compromise of the CA server's activation data or private key compromise
- The CA server cannot use an expired issuing CA certificate. A revoked certificate check can only be validated with the latest Intermediate Ca CRL file
- No persons operating the issuing CAs or unknown persons shall tamper, compromise or reverse engineer the technical lay down of the CA infrastructure.
- Registration of all issuing CAs shall not use any previous key pair to enrol. Re-enrolment may use the same private key for further certificate(s).

The Intermediate CA shall have its own subscribers/Issuing CAs, that must agree to terms of this Intermediate CA and be within governance of their own local CA CPS. The Intermediate CA authority shall give guidance to subscribers on the following agreements.

The Intermediates agrees with the subscriber agreement and will as follows:

- Accept all applicable terms and conditions contained within this document
- Use the private key for transactions relating to authorised Inmarsat business covering the certificate usage
- Notify the RA of any changes in the information submitted that might materially affect the trustworthiness of that certificate
- Cease using the certificate when it becomes invalid, revoked or expired
- Prevent the compromising, loss, disclosure, modification or otherwise unauthorised use of their private key
- Adhere to the extended key usage extensions that apply further limitations on the use of the private key
- Request the revocation of the certificate in case of an occurrence that materially affects the integrity of the certificate
- Only use certificates for legal and authorised purposes in accordance with this document

Note: *If this Intermediate CA signs directly to an issuing CA service, creating two tier hierarchy, the above list must apply.*

4.5.2. Relying Party Public Key and Certificate Usage

Relying Parties (RP) shall ensure that a public key certificate is used only for the following purposes:

- Accept all applicable terms and conditions contained within this document
- Ensuring that the public key in a certificate is used for the purposes indicated by the key usage extension only
- If the extended key usage extension is present and implies any limitation on the use of the certificate, those constraints shall also be observed
- Shall validate the certificate chain to the trusted Intermediate CA
- Trust the certificate after revocation and expiry checking has completed

4.6. Certificate renewal

Renewing a certificate means creating a new certificate without changing the subscriber or other participants' public key or any other information such as the same name, public/private key, and other information as the current one, but with a new extended validity period and a

new serial number. The current certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

The renewal of a certificate will generally occur when either the certificate is expiring or a change is required. The issuance of a new certificate containing an existing public key is permissible by **IPMG**. In general, renewal will always be a re-key of the private and public keys, retaining subscriber information such as subject name and SAN.

4.6.1. Circumstance for Certificate Renewal

Policy or constraint changes requested by the **IPMG**.

4.6.2. Who May Request Certification Renewal

IPMG may request a certificate renewal.

4.6.3. Processing Certificate Renewal requests

Intermediate CA service owners may process the renewal.

4.6.4. Notification of New Certificate Issuance to Subscriber

All subscribers of the Intermediate Certificate shall be informed by email or Inmarsat internal notification service.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Acceptance shall be granted upon signing of new CRL file, with private key, and that and end-entity can consume said CRL without issue.

4.6.6. Publication of the renewal certificate by the CA

Intermediate CA service certificate shall be published via the Validation Authority repository services. Intermediate certificate may also be published to any local directory service, such as Active Directory.

4.6.7. Notification of Certificate Issuance by the CA to other Entities

As aligned in 4.6.4.

4.7. Certificate Re-Key

The following elements related to an end-entity subscriber generating a new key pair and applying for the issuance of a new certificate that certifies the new public key.

4.7.1. Circumstance for Certificate Re-Key

A re-key of a certificate will generally occur when either the certificate is expiring, or a compromise of the private key. The Intermediate CA require re-keying of a certificate must initiate the same registration procedure as initial registration. The original key signing ceremony must be followed to generate a new key pair.

A certificate re-key will normally be required following a certificate revocation, unless such a revocation is performed because the certificate (and therefore the associated key-pair) is no longer required. A certificate re-key performed under these circumstances is treated as an initial request.

Certificate servers shall re-key their own certificates at 50% of their lifetime. The CA server will be re-keyed in the event of its private key being compromised. A re-key is not required if a change to the Intermediate CA policy is required, then same key pair will be retained.

A certificate re-key will normally be required following a certificate revocation unless such a revocation is performed because the certificate, and therefore the associated key-pair, is no longer required. A certificate re-key performed under these circumstances is treated as an initial request.

4.7.2. Who May Request Certification of a New Public Key

IPMG are entitled to request a routine re-key prior to the expiry of an existing certificate.

A manual enrolment may be required to validate changes in information within a new certificate such as subject name and CDP paths.

4.7.3. Processing Certificate Re-Keying Requests

A CA or RA's procedures to process re-keying requests to issue the new certificate are the same as the initial certificate issuance. The Intermediate local RA must check that the requesting device is still valid, the reason for re-key is valid and all information presented in the request is correct.

The Intermediate RA must notify the end-entities owners that successful re-key has been undertaken. And Intermediate CA server certificate re-issued all entities within the Inmarsat hierarchy.

4.7.4. Notification of New Certificate Issuance to Subscriber

When certificate is manually issued from a request queue by the CA administrators the issuers will send notification back to the requestor. Additionally, returning of the certificate will notify the requestor that the CA process is complete.

4.7.5. Conduct Constituting Acceptance of a Re-Keyed Certificate

For certificates issued failure, to object to the newly issued certificate or its contents constitutes acceptance of the certificate. The passage of time after delivery or notice of issuance of the certificate to the subscriber or the actual use of the certificate constitutes the subscriber’s acceptance.

4.7.6. Publication of the Re-Keyed Certificate by the CA

Certificates are published to repositories and local directories.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

The **IPMG** will be notified upon successful acceptance of any Intermediate CA certificate.

No other entities outside of the Inmarsat environment require to be notified of certificate issuance and or acceptance.

The certificate service shall log certificate issuance after a re-key, for audit purposes. This may be presented to **IPMG** upon request.

4.8. Certificate modification

This Inmarsat Intermediate CA CPS (II-CPS) does not support certificate modification. Owners wishing to modify a certificate will have to register for a new certificate as per the initial registration.

4.8.1. Circumstances for Certification Modification

Circumstances under which certificate modification can take place such as name change, role change or reorganisation resulting in a change in the DN will require a request to be sent to the RA. Inmarsat subscribers/end-entities are not permitted for modification; therefore, a new certificate will then be issued. New certificate constitutes new key pair and serial number.

Modification may only be permitted for the certificate server's certificate. The certificate server, certificate modification, will be under the direction of the **IPMG**. The changes for modification are:

- Name Constraints
- Policy OIDs
- Encoding.

4.8.2. Who May Request Certificate Modification

IPMG may request a modification to the CA server certificate.

4.8.3. Processing Certificate Modification Requests

Certificate modifications requesting regarding internal Inmarsat subscribers/end-entities, not stipulated.

4.8.4. Notification of New Certificate Issuance to Subscriber

Notification after modification for the CA server (subscriber) certificate shall be made by **IPMG**.

Notification of certificate issuance regarding internal Inmarsat subscribers/end-entities, not stipulated.

4.8.5. Conduct Constituting Acceptance of Modified Certificate

Acceptance of the new CA server certificate is deemed accepted on service start up. Notification of acceptance is made to **IPMG**.

Acceptance of certificate regarding internal Inmarsat subscribers/end-entities, not stipulated.

4.8.6. Publication of the Modified Certificate by the CA

CA server modified certificate shall be published to repositories, and local directory.

Publication of internal Inmarsat subscribers/end-entities not stipulated.

4.8.7. Notification of Certificate Issuance by the CA to Other Entities

Not stipulated within this document.

4.9. Certificate Revocation and Suspension

A certificate may be revoked prior to its expiry. A decision to revoke a certificate is made by the Registration Authority who are responsible for sending a revocation request to the CA operators for action. Initiation of the revocation process need not originate from the local RA but the local RA shall authorise the request. Creation and publication of CRL's and management of the certificate within the repository are the responsibility of the CA manager.

Suspension of a certificate is not permitted within this II-CPS and shall be deemed as a revocation.

4.9.1. Circumstances for Revocation

A certificate shall be revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid.

A certificate issued by the Inmarsat Root CA to any Inmarsat Intermediate CA server shall be revoked by the Root CA operators:

- Upon suspected or known compromise of the private key
- Upon suspected or known loss or compromise of the media holding the private key
- Upon decommissioning a device or application
- Following determination that registration information was invalid
- Upon termination of the need for a certificate
- A certificate issued to an end-entity/subscriber may be revoked by the Registration Authority:
- Upon termination of the need for a certificate
- When a certificate has been replaced following re-key or modification

A certificate issued by the Intermediate CA service to an Issuing CA service may be revoked by the Registration Authority:

- Upon termination of the need for a certificate
- When a certificate has been replaced following re-key or modification

The **IPMG**, at its discretion, may request revoke of a certificate when an end-entity/subscriber fails to comply with obligations set out in this II-CPS, any other agreement or applicable law. **IPMG** request the revocation of the CA server service certificates on the event of compromise, or suspected compromise.

4.9.2. Who can Request Revocation

All requests for revocation should be made to the Inmarsat Intermediate local Registration Authority.

The revocation of a certificate may be requested by:

- The owner who made the application for the certificate
- IT Security Officer or Cyber Group
- CA Operator/Administrator for any certificate issued at their request
- Registration Authority for any certificate
- **IPMG** for any certificate

4.9.3. Procedure for Revocation Request

Following the decision to revoke an Intermediate issued certificate the Intermediate local RA must be informed as soon as possible. A revocation request may be forwarded by email, telephone, or any other method that will achieve the objective of notifying the RA as soon as possible.

The originator of the revocation request will be verified in the same way as original owner identity verification. The RA will satisfy itself that:

- The request for revocation is made by an authorised source and verified. Preferably the owner
- The certificate to be revoked is unambiguously identified and verified
- The reason specified for revocation is one of those given in **Section 4.9.1** [***Circumstances for Revocation***].

Following the decision to revoke a certificate the RA is responsible for generating a Revocation Request. This request should be submitted to the CA operators from the RA as a formal notice and logged.

The RA shall record full details of all requests for revocation it receives including those it rejects. The accounting log shall include at minimum:

- Source of the request, including organisation and role title
- Date/time of the request being received and from whom
- Mechanisms used to determine that the request is acceptable, e.g. system investigation
- If applicable the reasons for rejection
- Reason for the request in a formal statement from the requester
- Confirmation that the key store of any token used to store a private key associated with a certificate has been zeroed
- Date/time of the Revocation Request being transmitted to the CA service owners

The target time interval to create a Revocation Request is one working day. Revocation time is reduced upon private key compromise to 1 hour.

Once a certificate has been revoked then manual, issuing of CRL's must take place immediately.

4.9.4. Revocation Request Grace Period

For all certificates, a revocation request must be made immediately upon discovery of the loss or potential compromise of a private key or its container. There is no defined grace period. Certificates will be revoked as soon as practicable following notification to the RA.

4.9.5. Time within which the CA must Process the Revocation Request

The CA operators will revoke a certificate immediately upon a valid request within the normal working day.

Revocation of a compromised certificate shall occur immediately whether inside or outside normal business and must process the revocation request by the end of the next working day.

Upon a certificate revocation, a new CRL will be published

4.9.6. Revocation Checking Requirement for Relying Parties

It is up to a Relying Party to verify the status of any certificate that it wishes to use. This should be done using the most up-to-date information available normally by reference to a current CRL published. The use of a cached CRL is permitted if it has not expired.

If it is not possible to determine the current revocation status of a certificate then the Relying Party must not accept the certificate.

4.9.7. CRL Issuance Frequency

The Inmarsat Intermediate CA issues their CRL file at intervals of 4 weeks, plus overlap of 2 weeks.

4.9.8. Maximum Latency for CRLs

Intermediate CA latency is maximised at 6 weeks publishing of Intermediate CRL's are manual.

4.9.9. On-line Revocation/Status Checking Availability

Intermediate CA service does not offer or publish an online revocation status.

4.9.10. On-line Revocation Checking Requirements

No stipulation.

4.9.11. Other Forms of Revocation Advertisement Available

There are no additional CRL advertisements other than HTTP web services.

4.9.12. Special Requirements Re-Key Compromise

In the event of an end-entity certificate being compromised, the owner if aware of compromise will notify the RA immediately where the revocation process can take place.

4.9.13. Circumstances for Suspension

The Inmarsat CA service does not support the use of certificate suspension. Certificates will be revoked, and re-enrolment must take place.

4.9.14. Who can Request Suspension

Not stipulated within this document.

4.9.15. Procedure for Suspension Request

Not stipulated within this document.

4.9.16. Limits on Suspension Period

Not stipulated within this document.

4.10. Certificate Status Services

4.10.1. Operational Characteristics

All end-entities/relying parties will use HTTP protocol to gain information regarding the CA certificate status.

4.10.2. Service Availability

The CRL files are published to a highly available location, which is defined in as Certificate Distribution Points.

4.10.3. Optional features

Not stipulated within this document.

4.11. End of subscription

Once a subscription has ended, the all-expiring certificate will be revoked in accordance with the procedures at **Section 4.9** [***Certificate Revocation and Suspension***].

Where the subscription of the Inmarsat CA servers' own certificate has ended, all the valid certificates associated with the CA server will be revoked by under direction of the **IPMG**.

All HSM's will have all crypto material removed and the HSM's zeroised. Zeroing will constitute to a factory reset where all crypto partitions are reset, and all configuration removed. All associated ACS/OCS cards will become inoperative at the removal of the HSM configuration and partitions.

The certificate service and virtual machine computer accounts will be removed from all local directory services. All copies of the certificate server virtual machines removed from backup and local disk copies. Due to the nature of virtualisation technology, the hard disks used for certificate server virtual machines may also be sharing other servers and services. It is impractical to remove these hard disks until after the closure of the whole Inmarsat environment, or at a minimum the storage array the CA servers reside within. Upon closure all disks from the virtual machines shall be destroyed in line with Inmarsat security policies.

4.12. Key Escrow and Recovery

Storage of the private keys with a third party is not permissible within this CPS.

4.12.1. Key Escrow and Recovery Policy and Practices

Not stipulated within this document.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Not stipulated within this document.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

Describes non-technical security controls (that are, physical, procedural, and personnel controls) used by Inmarsat to securely perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, auditing, and archiving.

These non-technical security controls are critical to trusting the certificates since lack of security may compromise CA operations resulting for example, in the creation of certificates or CRL's with erroneous information or compromising the CA private key.

5.1. Physical controls

Physical security requirements for the Intermediate CA server containing the CA service are implemented in accordance with the Inmarsat Security Policy Framework. Security operating procedures are documented as appropriate in relevant Inmarsat Cyber Security controls.

5.1.1. Site Location and Construction

The Inmarsat Intermediate CA service consists of virtual Linux servers, network connected to each nCipher Connect HSM that are geographically separate locations to provide a recovery service in the event of HSM failure.

Each location is staffed 24/7.

5.1.2. Physical Access

Procedural measures, approved access lists are maintained on site with personnel given lock code entry. All other staff and visitors are under supervision when accessing the controlled areas containing the CA servers and associated equipment. A log of visitor access and activity to controlled areas is maintained.

All building access and secured areas are controlled by an assured and audited access control system. Secure areas are further segregated, controlled, and audited, where appropriate, by additional cabinet lock systems.

All sensitive material is secured in a suitable security container when not in use and is located off-site in the opposing computer room. The sensitive material covered by this practice includes:

- HSM access/control terminals
- HSM backups
- HSM Admin/Operator cards
- System software and backups

5.1.3. Power and Air Conditioning

The Intermediate CA servers require a minimal power consumption, for the duration of the key signing and future CRL and CSR signing.

Intermediate CA servers are part of a virtualised infrastructure within the Inmarsat datacentres and are provided with sufficient power and air conditioning as part of the Data Centre provisioning.

5.1.4. Water Exposures

Adequate protection is given to protect the Intermediate CA servers when in operation to prevent water exposure.

5.1.5. Fire Prevention and Protection

The Intermediate CA virtual servers hosted within each data centre, the DCs must be able to provide adequate fire resistance during a fire.

It will be deemed that in the event of a DC fire and disaster the protecting cabinet will be unrecoverable.

5.1.6. Media Storage

Storage media used (ACS and OCS cards) will be protected from physical access by a secure cabinet in conformance with Inmarsat cyber crypto storage.

5.1.7. Waste Disposal

All media used to operate or support the Inmarsat Intermediate CA service will be handled in accordance with the procedures given in security policies and as agreed with the system accreditor. Specific procedures relating to the handling of material associated with the CA environment are defined in the appropriate Inmarsat cyber operation and material handling.

5.1.8. Off-Site Backup

All Intermediate CA server backup material will be held at a separate location.

5.2. Procedural Controls

5.2.1. Trusted roles

Inmarsat defines a trusted role within this document as an individual who performs a task that is important for the security or continued operation of certificate services. These individuals are required to have passed the personnel checks as defined in **Section 5.3** [***Personnel controls***] and have the skills, experience and training required.

The trusted roles have the potential of introducing security breaches, unscheduled outages or compromise related incidents if not adequately performed whether accidental or malicious. The functions performed by these roles are integral to the overall trust of the Inmarsat certificate service.

Trusted personnel within Inmarsat include all company employees, contractors and consultants that have access to or control authentication, authorisation or cryptographic operations that may materially affect:

- Certificate enrolment process including approval, rejection, revocation, renewal and re-key
- All publishing to the repository service
- Handling of subscriber information or requests
- Auditing of the certificate services infrastructure components
- Auditing of software components used to manage and deliver the certificate service
- Backup and recovery of the Intermediate CA certificate services

Crypto Custodian:

- Role is available to control physical access to the Intermediate CA and HSM
- Control over the security at the location of the Intermediate servers which they control access to protecting cabinet
- Custody and control over the HSM backup material

The CA service enforces role separation for sensitive roles to limit accidental or malicious acts to undermine the integrity of the Inmarsat CA service. The certificate services implements two mechanisms in support of risk reduction:

- Delegation of administration model
- Splitting activities across multiple trusted roles

IPMG requires for certain tasks defined as 'sensitive tasks' that more than one participant to be present to carry out the task. Where this is required, the certificate service will implement m of n, which requires a minimum of two (2) participants to be present to carry out these sensitive tasks.

Note: (M = total of operators, N = operators required to complete a task, N is always smaller than M)

Trusted roles provide separation between the product/system administration, certificate management, key material, and audit functions. Each role is required to have separate logon accounts for audit and traceability; however, each logon account can be the same person, as it is the account that is separated not the person. Each account is a single person occupancy.

The certificate service defines several trusted Microsoft CA server roles as follows:

: CA Intermediate Administrators (OS and Hardware):

- Certificate server administrators are responsible for the configuration and operation of the Intermediate CA Ubuntu operating system
- Certificate server administrators will have the responsibility for backup and recovery of the Intermediate servers. Recovery will be in conjunction with the CA operators as access to the HSM will be required.
- CA server local administrators will have individual accounts for audit purposes
- All request for accounts such as 'requestors' logon accounts will be managed by these administrators

: CA Operators (Certificate Manager):

- CA operators will be responsible for the operation of certificate management, such as issuance and revocation
- CA operators will be responsible for manual updates of the CRL's published via the VA server
- Operators will have individual accounts for audit purpose
- Operators will have the authority to overall manage the certificate services and have access to the HSM for certificate management tasks. Such as backing up private keys from the HSM

: Registration Authority

- RA trusted roles will be defined in an administration document for handling certificate requests, the delivery of issued certificates to the requesting party
- Overall process will include verification of requestor, delivery of request to the CA operator's team for certificate creation and return of manufactured certificate for delivery to the Registration Authority, who in turn will verify the certificate and issue to the original requestor
- RA supports two roles, Registration Authority for the verification of certificate requests and revocations and RA auditor. The two RA roles are conducted by different persons to maintain the credibility of the system.

: Security Officer:

- Responsible as the custodian of all cryptographic material relating the operation of the certificate service

- All persons in operation of the certificate will be approved by the security office as individuals how have access to private key material

Trusted Role	High-Level Purpose	Detailed Purpose
Administrator	Configure and maintain the CA server	Assign all other CA roles and extensions Renew the CA certificate (M of N) Configure policy and exit module Stop and start the certificate service Read and delete single row in database Publish and configure CRL schedule
Certificate Operators	Approve certificate enrolment and revocation requests	Issue and approve certificates Deny Certificates Reactivate certificates placed on hold Renew certificates Read the CA Database Read the CA Configuration Install the Certificate Authority Renew CA Keys (M of N) Enable/Disable Role Separation
Audit	Configure, view, and maintain audit logs	Configure Audit Parameters View Audit Logs Read the CA Database Read the CA Configuration Deletion of Logs (M of N)
Backup	CA Server Recovery	Perform recovery of the Intermediate CA server

Table 7 - Certificate Service Trusted Roles

Other Trusted Roles: NShield Connect Hardware Security Module. The HSM roles are determined by the policies, technical features of the devices and the Service Operations. There are seven (7) trusted HSM roles defined in Table 8 - HSM Trusted Roles].

The Intermediate CA uses nCipher nShield Connect HSM. The nCipher HSMs have a concept of using smart cards as part of the protection. Using key protection, several security roles can be adopted and each of these roles have been allocated a colour marking. Table 8 - HSM Trusted Roles defines each protection key type as a role for an individual person to undertake.

The Admin Card set operator role including the use of ACS cards are owned by Crypto Custodian this is part of the M of N. Crypto officer undertakes all HSM related activities under an appropriate. The crypto officer is also responsible for account administration of unique accounts tied to either the:

- Administrator Card Role
- Operator Card Role

The creation of unique accounts tied to individual users on the HSM provides non-repudiation.

Trusted Role	High-Level Purpose	Detailed Purpose
Admin Card Set	Installation, Configuration and Administration	HSM Administration Set HSM Policy Manage Users (Non-Repudiation)
Operational Card Set	Use Cryptographic Objects	Partition Administration Key Generation & Signing Backup/Recovery
HSM User Roles		
Administrator	HSM Administration	Perform the full command set for the device

Table 8 - HSM Trusted Roles

5.2.2. Number of Persons Required per Task

Intermediate certificate services defining personnel per task these tasks are:

- Local Administration: Manages CA server
- Operational: can process certificates, can submit requests (RA)
- Registration Authority: can submit requests
- Auditing: can view security server logs and CA logs
- Security: will audit breaches and service impact

The minimum of two witnesses/operators required to complete any sensitive operation.

Sensitive operations include:

- Any activity requiring access to, or use of, the CA server private signing key
- Start and stop the CA service/server
- Backup and restore CA service

5.2.3. Identification and Authentication for Each Role

Users associate themselves within a particular role/function using a personal identifier and are member of a group account. There is a single incumbent per management account and each account has a unique password associated. Each User will be required to authenticate against the local operating system providing username and password. Each User will then have enough permission to carry out their tasks or operation.

The audit system ensures that any actions performed by a trusted account shall be identified against an individual. The audit trails include the full life cycle of request, create and deliver, and includes the movement of request between the RA team and the CA admin team (manufactures) and back to RA for delivery to the original requestor.

Intermediate CA local RA team do not have permissions to manufacture a certificate on any of the CA's. This in turn means that any CA management personal cannot be an interface for certificate approval as per an RA role.

Several checks in place to ensure that proper identification and authentications checks are performed to ensure that only authorised personnel are in each trusted role.

The service operations ensure that all assignments of an individual to a trusted role include the following checks:

- Trusted roles maintained by the certificate service owner defined in **Section 5.2.1** [***Trusted roles***]
- Training courses, qualification and completion certificates are maintained within service operations and operational security verify the individual has undertaken the training to assume a trusted role
- Verify the clearance level appropriate for the trusted role and in agreement with the local security office
- Incident is raised for every change made to the certificate service. The Incident names the individuals from the list of trusted roles
- Ensure role separation
- For physical access the local crypto custodian facilitate access in line with the permit for access and multi-person rules if an operation requires n of m persons

5.2.4. Roles Requiring Separation of Duties

A person employed within one of the roles defined in **Section 5.2.1** [***Trusted roles***] will not be simultaneously employed as an auditor with responsibility for the CA. Furthermore, no person undertaking an RA role will undertake any trusted role for the CA or VA.

Implementation of role separation of duty to prevent the following occurring:

- Persons involved with operational capacity to undertake a security audit role on the certificate infrastructure and service
- Persons perform a trusted role in the operation of the certificate service, will not undertake the RA role

5.3. Personnel controls

All personnel who require access to the certificate infrastructure must go through a vetting service to ensure they meet the requirements for their trusted role position.

All personnel requiring access to the service such as requestors will all so sign the appropriate System Operations, granting them a user logon account.

5.3.1. Qualifications, Experience, and Clearance Requirements

Personnel engaged in the operation of the Intermediate CA service shall be suitably trained in all aspects of the certificate delivery and life cycle. Regular reviews will identify any specific requirement's pertaining to the management of the CA service as and when appropriate.

Inmarsat Intermediate CA service owners will not be allowed to action any certificate creation until training has been undertaken.

Processes of certificate management and handling will be governed by the Registration Authority.

All personnel engaged on the operation of the certificate life cycle and management elements from within the Inmarsat certificate service will be authorised and approved access to CA servers.

5.3.2. Background Check Procedures

All personnel employed or contract, prior to the engagement of operation and administration within the certificate service will have has background checks by the respective companies covering the basic check:

Basic undertaken checks are as follows:

- Search of criminal records

- Check of credit/financial records
- Check of professional references
- Confirmation of previous employment
- Confirmation of most relevant educational and/or training

It is expected that the above basic checks will have been undertaken during employment. However, these checks must be carried for contractor working

5.3.3. Training requirements

Operational guidance documentation will be given to the Intermediate CA service owners staff for procedures of operations and tasks. Guidance given is not definitive and shall evolve, as new procedures are defined and/or current ones are amended.

Service owners shall ensure that all personnel performing operations and administration on the certificate service will have received comprehensive training to cover all aspects of duties, to include:

- Awareness of the overall certificate services security principles and delivery
- Understanding of Public Key Infrastructures: Architectures and Technology
- Security architecture: policies, authentication, authorisation, privacy, integrity and non-repudiation
- Maintenance of software and its operation and usage: Ubuntu long term service
- Certificate duties and responsibilities for each role: understanding basic cryptography
- Disaster recovery and business continuity procedures

Operational guidance documentation will be given to the Intermediate CA server administrators for checks and balances against operations. The guidance given is not a definitive document, shall be updated as new procedures occur or current ones need changing.

CA Server and Operator Training:

- Certificate utilities
- Backup and Recovery
- Role separation
- Advanced troubleshooting

nCipher HSM Training:

- Setup and basic administration of Security World
- Management Console and nCipher command shell
- Policy Management
- Licensing and Upgrades
- HSM Initialisation, Policy Configuration, and client installation (Security World)
- Admin, Operator and Monitor user, HSM Logs
- Backup and Recovery options
- nCipher card set overview and installation
- Performance testing, troubleshooting and best practice
- Resetting the Admin Password

Note: The above lists for the CA service and HSM training, is not exhaustive. Will provide the operator a good understanding of a nCipher service and Ubuntu operating system.

5.3.4. Retraining Frequency and Requirements

CA personnel will be trained as required when a change to the infrastructure or policies occurs. Notification of changes will precede actual change. Refresher training will be required at intervals when infrequent operations require action or personnel changes occur.

Any requirements that are imposed by the **IPMG** must be adhered to and the delivery of any new documentation. All new requirements for the Inmarsat CA service will be passed to the design authority for documenting and training whom in turn will deliver documentation and training to the CA operators.

5.3.5. Job Rotation Frequency and Sequence

Inmarsat will ensure that changes in staffing have no impact on the operational effectiveness or security of the certificate service.

Job rotation will occur, should a compromise of the system be detected and requires investigation without the individuals being aware.

No operational or security impact will occur within the certificate services during normal operation in the event of turnover/movement of staff: including personal holidays, sick leave and other out of office activities.

5.3.6. Sanctions for Unauthorised Actions

If an unauthorised action takes place, then appropriate action must be taken to ensure disciplinary or other actions are taken. Any action taken shall be documented against the violation and presented if required to the **IPMG**. All information must be declared and distributed to all interested parties, device owners, Service Management, and the Registration Authority. In cases where the unauthorised action brings into question the security of the CA or its issuance then the CA service must not process or issue further certificates until breaches have been noted and resolved.

5.3.7. Independent Contractor Requirements

All practices apply equally to Inmarsat personnel and/or contractors. All parties must adhere to this Intermediate CA CPS.

5.3.8. Documentation Supplied to Personnel

All personnel involved with the management and operation of the CA have full access to all documentation related to the following:

- Certificate design documentation
- Service operations and procedures
- CA and Registration Authority processes
- Work instructions and vendor operation manuals
- Inmarsat Certificate Policy and this Intermediate CA CPS

5.4. Accounting Logging Procedures

5.4.1. Types of Events Recorded

As a minimum, the following security events are recorded manually in the accounting log(s):

- All known or suspected violations of physical security
- Installation, modification or update of CA hardware and software
- Receiving, servicing (including re-keying/re-loading) or shipping of hardware security modules (HSMs)

- Initialisation, re-initialisation, zeroing, destruction, key generation event of any smartcard or other hardware token used

The following events are logged with the operating system that hosts the certificate service, for this deployment is Ubuntu long term service

- The start-up and shutdown of the CA server
- Login/logout from the host operating system
- Certificate creation/revocation messages sent and received
- Certificate creation and revocation events
- Any change to the CA software functions or configuration
- Key generation events
- Backup and restoration of a CA server database
- Specific auditable data identified for the registration process (see 3.2 [***Initial Identity Validation***])

For each event, the following information is recorded as a minimum:

- Type of event
  - Date and time of event
  - Identity of the operation being performed
  - The success or failure (along with reason for failure) of the event
  - Failure message of source, contents and destination if relevant

The following is a complete table list of events to be recorded:

Event	Intermediate CA server	RA system
Accounting System		
Any changes to accounting parameters, e.g. types of event logged	X	N/A
Any attempt to delete or modify accounting logs	X	N/A
Obtaining a third-party time stamp	X	N/A
Identity Proofing		
Successful and unsuccessful attempts to assume a role	X	
Value of maximum number of authentication attempts is changed	X	
Number of unsuccessful authentication attempts exceeds the maximum number of authentication attempts during user login	X	
Unlocking an account that has been locked because of unsuccessful authentication attempts	X	
Change of the type of an authenticator, e.g. from a password to smartcard	X	
Local Data Entry		
All security-relevant data that is entered in the system	X	
Remote Data Entry		
All security-relevant messages that are received by the system	X	
Data Export and Output		
All successful and unsuccessful requests for sensitive and security-relative information	X	X
Key Generation		
Generation of a key (excluding session and on-time use symmetric keys)	X	
Private Key Load and Storage		
The loading of a private key, including activation of an HSM containing a private key	X	

Event	Intermediate CA server	RA system
All access to Subscriber private keys retained for key recovery purposes	X	
Trusted Public Key Entry, Deletion and Storage		
All changes to trusted public keys, including additions and deletions	X	
Private Export		
The export of private and secret keys (excluding session keys)	X	
Certificate Issuance		
All certificate issuance requests sent and received	X	
Certificate Registration checks for subscribers	X	
All certificate issuance requests processed (successful and unsuccessfully)	X	
Certificate Revocation		
All certificate revocation requests sent and received	X	
All certificate revocation requests processed	X	
Configuration		
Any security-relevant changes to the configuration of the device, e.g. patches, configuration settings	X	
Account Administration		
Roles and users added or deleted	X	X
Access control privileges of an account or role are changed	X	X
Certificate Profile Management		
All changes to the certificate profiles	X	
Validation Authority Management		
All changes to VA server profile or configuration, including changes to certificate profile	X	
Certificate Revocation List Profile Management		
All changes to the certificate revocation list profile	X	
Miscellaneous		
Appointment of an individual to a trusted role	X	
Designation of personnel for multi-person control	X	
Installation of the operating system	X	
Installation of the PKI application	X	
Installation of hardware cryptographic modules	X	
Removal of hardware cryptographic modules	X	
Destruction of cryptographic modules	X	
System start-up	X	
Logon attempts to PKI application	X	X
Receipt of hardware/software	X	X
Attempts to set passwords	X	X
Attempts to modify passwords	X	X
Backup of the internal CA database	X	
Restoration from backup of the internal CA database	X	
File manipulation (e.g. creation, renaming, modification)	X	
Posting of any material to a PKI repository	X	
Access to the internal CA database	X	
All certificate compromise notification requests	X	X

Event	Intermediate CA server	RA system
Loading tokens with certificates	X	X
Shipment of tokens	X	X
Zeroing of tokens	X	X
Re-key of the component	X	X
Configuration Changes		
Hardware	X	
Software	X	X
Operating system	X	X
Patches	X	X
Security profiles		X
Physical Access/Site Security		
Personnel access to room holding component	X	
Access to the component	X	
Known or suspected violations of physical security	X	X
Anomalies		
Software error conditions	X	X
Software integrity check failures	X	X
Receipt of improper messages		X
Misrouted messages		X
Network attacks (suspected or confirmed)	X	X
Equipment failure	X	X
Electrical power outages	X	
Uninterruptible Power Supply (UPS) failures	X	
Obvious and significant network service or access failures	X	
Violations of security policy	X	X
Violations of CPS	X	X
Resetting operating system clock	X	

Table 9 - List of Recordable Events

5.4.2. Frequency of Processing Log

Accounting logs are reviewed every time the Intermediate CA servers are accessed. The event logging reviewed is focused on identifying security-related events. A log of the audit results shall be generated and made available for external auditing.

5.4.3. Retention period for Audit Log

The information generated on the Intermediate CA server is retained on that equipment until the information is archived. Deletion of the accounting log following archive is supervised by a security or audit officer whose role is not a CA operational role. Audit log data must be available for at least 12 months or until reviewed maintained within Inmarsat audit and accounting policies. This may then be archived in accordance with the procedures in **Section 0** [***Protection of audit logs*** is managed for both electronic and manual (paper) log entries. Electronic and paper audit logs operate in four forms:

- Electronic such as Ubuntu operating system (OS) events (System, Security and Application)
- Structured text-based log files (devices and applications)

- Syslog file or other HSM event collection
- Paper (Used in the operation of this Intermediate CA CPS)

Intermediate CA server OS Ubuntu system event management system is protected by the operating system. Audit collection applications consuming the operating system events shall protect from unauthorised personnel being able to view, modify, delete, or tamper with events.

Structured text-based log files are protected through access control list controlling access to view, modify and delete to a nominated audit group.

The Syslog files are protected by the same asserted protection as with structured text logs.

Any Paper based audit log protection against modification, destruction or theft is achieved by means of an approved lockable storage.

Archived audit logs shall be stored in a location separate to the source audited data. Storage within the same site is permitted, if the storage location is physically separate to the operational system (e.g., a different room or building or network).

Audit Log Backup Procedures].

5.4.4. Protection of Audit Log

Protection of audit logs is managed for both electronic and manual (paper) log entries. Electronic and paper audit logs operate in four forms:

- Electronic such as Ubuntu operating system (OS) events (System, Security and Application)
- Structured text-based log files (devices and applications)
- Syslog file or other HSM event collection
- Paper (Used in the operation of this Intermediate CA CPS)

Intermediate CA server OS Ubuntu system event management system is protected by the operating system. Audit collection applications consuming the operating system events shall protect from unauthorised personnel being able to view, modify, delete, or tamper with events.

Structured text-based log files are protected through access control list controlling access to view, modify and delete to a nominated audit group.

The Syslog files are protected by the same asserted protection as with structured text logs.

Any Paper based audit log protection against modification, destruction or theft is achieved by means of an approved lockable storage.

Archived audit logs shall be stored in a location separate to the source audited data. Storage within the same site is permitted, if the storage location is physically separate to the operational system (e.g., a different room or building or network).

5.4.5. Audit Log Backup Procedures

Audit logs are archived and should be removed to an offsite location at an interval less than 2 months. The process of recovering from a backup is designed to avoid loss of later accounting data where practical.

5.4.6. Audit Collection System (internal vs. external)

The audit collection system is both:

- Internal:

    - For audit events generated by the certificate services components including application and operating system and devices
- External:
    - For audit event records generated by Registration Authority
- For data centre and crypto manual security audit events stored by each operator

In the event auditing has failed, all operations are suspended until problem is rectified.

5.4.7. Notification to Event-Causing Subject

The event-causing subject is only informed of an event where this is deemed necessary to support maintenance, troubleshooting or fault rectification.

5.4.8. Vulnerability assessments

The CA implementation of the system will be in line with Inmarsat documentation, which indicates the assessment of vulnerability and approved by the system accreditor.

It will be assumed that the complete infrastructure of the Intermediate CA service will undergo appropriate security testing as part of an IT health check. This will be carried out prior to any live operation.

5.5. Records Archival

5.5.1. Types of Records Archived

Archive records detail at least the creation and revocation of certificates and sufficient information to establish the validity of the proper operation of the Intermediate CA server. This involves the archive of all accounting logs and other related records.

The Intermediate CA server archive records are intended to allow an audit to establish the proper operation of the system or the validity of any certificate (including those revoked or expired) issued by the CA server.

The following table is an overview of types of records that will be archived.

Data to be Archived	CA	RA
This Intermediate CA Certification Practice Statement	X	
Contractual obligations	X	X
System and equipment configuration	X	
Certificate requests	X	X
Revocation requests	X	X
Subscriber identity authentication data (Section 3.2.3)	X	X
Documentation of acceptance and receipt of certificates	X	X
Documentation of receipt of tokens	X	X
All certificates issued or published	X	
Record of re-key	X	X
All CRLs issued and/or published	X	
All audit logs	X	
Other data or applications to verify archive contents	X	X
Documentation required by compliance auditors	X	X
Accreditation documents and certificates	X	X

Table 10 - Records of Archive

5.5.2. Retention Period for Archive

The retention period for archived material shall be a minimum of 5 years or as directed by cyber security.

Records will be kept in a simple format such as CSV or TXT/RTF with the capability of being read at the end of archived period.

5.5.3. Protection of Archive

Archives shall be managed using secure physical storage. This may include using cryptographic protection. Within the physical storage protection, environmental aspects will be considered such as humidity, temperature, and electromagnetism.

Once data and/or information are archived, its accessibility will be limited to authorised personnel. These will be key system management personnel, CA operators and system security officers.

5.5.4. Archive Backup Procedures

Archives shall be managed with replicas being held off site to the primary archive source. The archives will be maintained with the same integrity as the primary data archive.

5.5.5. Requirements for Time-Stamping of Records

Wherever practical a trusted source of system time should be used see **Section 0** [***The*** Intermediate CA server has a status of on-line, but is protected by networks security ACLs and local a firewall.

Time-Stamping]. All data and records will be timed stamped with local time and date.

System directory support the certificate service will gain its time source from an external source.

5.5.6. Archive Collection System (internal or external)

Not stipulation within this Intermediate CA CPS.

5.5.7. Procedures to Obtain and Verify Archive Information

Archived information 6-months old will be inspected by the security officer and or system-based administrators. The inspection will provide evidence of accessibility and application software accessing the archive is still valid.

Archive inspection material will be mounted within the system to maintain the integrity but will not affect the operational system.

Whenever practicable a digital signature is used to affirm the integrity and authenticity of archival records.

5.6. Key Changeover

Intermediate CA server may be expected at 50% of the initially self-signed certificate lifetime to be renewed. At the end of the validity period of any Intermediate CA certificate there must not be any active certificates that depend on for public keys.

5.7. Compromise and Disaster Recovery

Guidance on disaster recovery for the local Information System as well as incident handling and reporting procedures.

5.7.1. Incident and Compromise Handling Procedures

If an actual or suspected compromise of the private key assigned to a CA server occurs this is to be reported immediately via the IT Security Incident handling processes identifying immediate response actions for compromise of CA server keys.

Incidents and procedures will be maintained in the service management and disaster recovery planning.

5.7.2. Computing Resources, Software, and/or Data Corruption

CA service administrators maintain a complete backup of certificate server components. These are the CA database, CA server log files and Operating System. This enables recovery of a component or system, following data corruption through accidental or malicious means.

Restoration procedures will be that of an actioned disaster recovery process. Levels of corruption and service loss will be acted on in degrees of severity such as loss of service, loss of server and loss of infrastructure. Each element will constitute as part of the recovery plan held within service management.

Prior to any recovery the corruption point will need to be known as backups after the corruption point are not valid and shall be disregarded.

5.7.3. Entity Private Key Compromise Procedures

Intermediate CA: In the event of a compromise, occurring with the Intermediate CA private key, the certificate will be removed from all Inmarsat CA servers. Once the compromise is resolved, it will be expected that a new key pair will be generated and distributed to all issuing CAs. This means all issuing CAs will require re-keying. All Compromised Intermediate CA will be removed from all certificate store locations, repository servers and directory.

5.7.4. Business continuity capabilities after a disaster

Business continuity for the CA certificate service is incorporated into the Business Continuity Plan for the overall Inmarsat infrastructure service.

The split-site nature of the CA server's provision ensures that certificate issuance is supported following loss of a single site. Capability supports the recreation of a CA server from backup materials to allow continuity of service. In addition, it is possible to extend the lifetime of existing CRL's by any of the CA servers re-signing with access to the Private Key material.

5.8. CA or RA termination

IPMG will inform the CA service owners with at least 30 days before the cessation of service of any CA server if not being replaced.

At the termination of service all keys, audit logs and other archived material will be retained.

The Intermediate CA server will not be terminated until all certificates in issue have either been revoked or replaced with an equivalent certificate issued by an alternative CA server. All certificates issued by the CA server will be revoked and that fact published on consecutive CRLs for a period of 30 days prior to cessation of service.

A communication plan to subscribers and relying parties informing them of the status of the Intermediate CA:

- Preservation of all CA archives and records
- Continuation of subscriber support

- Continuation of revocation services including CRLs and VA
- Revocation of unexpired, unrevoked certificates of end-entity
- Publishing of long life CRL’s with revoked certificates
- Destruction and disposal of all private keys

6. TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1. Key pair generation

Intermediate CA server key pairs are generated within nCipher nShield Connect Hardware Security Module (HSM) operating in a FIPS 140-2 Level 3 mode. Key pair generation is performed by a FIPS 140 certified key generator using entropy derived from an internal hardware random number generator. Access to the private key is controlled using a 2-factor authentication mechanism (i.e. HSM hard tokens) also known as Admin Card Set (ACS)

The Intermediate CA server generates a key pair, and for the certificate to be signed by the Inmarsat Root CA is at the top of the Inmarsat certificate hierarchy.

The Intermediate Key pair generation:

- Intermediates will always maintain their private keys within the devices own cryptographic store. This private/public key will be used to sign the request
- Intermediate CA subscriber/End-Entity are the Issuing CA servers

6.1.2. Private Key Delivery to Subscriber

It will be assumed all Private keys are generated within the end-entities internal crypto service and must remain bound within the crypto store. Therefore, there is no requirement for delivery of private keys.

6.1.3. Public Key Delivery to Certificate Issuer

Public keys are delivered to the CA service by use of the Certificate Management Protocol (CMP) certificate request (RFC 2510) or PKCS#10. These mechanisms always include proof of possession of the associated private key.

6.1.4. CA Public Key Delivery to Relying Parties

Delivery of the Intermediate CA public key to end-entities/subscribers, who are regarded as part of the certificate hierarchy, will have this certificate installed into their local crypto store. The Intermediate CA certificate will be made available within the VA repository service.

Manually enrolled end-entities will have the Intermediate CA certificate manually installed prior to operational service. If a relying party needs either of these certificates provided, they should apply to the Inmarsat RA.

6.1.5. Key Sizes

CA Intermediate server shall use a (SHA256) 4096-bit RSA key.

CA end-entities/subscribers use (SHA256) 2048-bit RSA keys.

6.1.6. Public Key Parameters Generation and Quality Checking

All keys used within the CA Intermediate server is generated in cryptographic modules certified FIPS 140-3. The FIPS certification includes certification for RSA key generation to the requirements of ANSI X9.31-1998 and FIPS 186-2.

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

The CA servers issue certificates to support the X.509 *keyUsage* field (and associated *extendedKeyUsage* field) fully state the intended purposes of the key.

The Intermediate CA shall use the following OIDs:

- 2.5.29.37.0 - Any Extended Key Usage
- 2.5.29.32.0 – Any Policy

6.2. Private Key Protection and Cryptographic Module Engineering Controls

6.2.1. Cryptographic Module Standards and Controls

All hardware cryptographic modules used within the Intermediate CA service meet minimum standards, identified, and approved by the **IPMG**. The products in use are compliant with FIPS 140-2 or 3 (*Security Requirements for Cryptographic Modules)* evaluated at various levels as allowed by the **IPMG**.

All cryptographic modules are operated in such a manner that the private key is never output in plain text. Private key must always remain unexportable.

6.2.2. Private Key (n out of m) multi-person control

Section 5.2.2 [***Number of Persons Required per Task***] identifies the number of persons required to provide certain trusted roles. These roles extend to control over the private key used by specific critical infrastructure components. In the circumstances where multi-person (N of M) controls are stipulated, **N** is **2** and **M** is **6**. Access to the CA server private key requires at least two personnel to load the key into the HSM prior to use.

The authentication components for each key are stored in separate locations to prevent unauthorised combination of the components.

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

M of N is detailed within the Key Signing Ceremony conducted for generating the Intermediate CA server key pair.

6.2.3. Private Key Escrow

No, private key escrow service is offered by any CA service or associated services within the Inmarsat certificate service.

The certificates issued by the CA Intermediate server service is not intended for encryption of data at rest and therefore there is no business continuity reason to support private encryption key recovery mechanisms.

6.2.4. Private Key Backup

Private key, which is maintained within this Intermediate CA CPS, CA certificate server. The CA certificate server private keys are maintained within the nCipher nShield Connect HSMs and cloned to a second nCipher nShield Connect HSM to protect key pair loss.

6.2.5. Private Key Archival

Not stipulated within this Intermediate CPS.

6.2.6. Private Key Transfer into or from a Cryptographic Module

For the CA service hardware cryptographic modules key generation takes place within the module. Transfer into and out of hardware, cryptographic modules use the same mechanisms for backup. A private key never exists outside of a cryptographic module in an un-encrypted state or plain text.

Private keys can be restored to another HSM cryptographic module of the same type in the event of:

- HSM failure
- Private Key corruption
- Disaster: Power loss, partition loss

6.2.7. Private Key Storage on Cryptographic Module

Intermediate CA server private keys will be stored within nCipher nShield Connect Hardware Security Module for protection. These comply with FIPS 140-2 Level 3.

6.2.8. Method of Activating Private Key

Activation of the private key within a cryptographic module will always be protected by a suitable authentication mechanism. These mechanisms are:

- Passphrase protected secrets in M of N configuration – complex, not guessable

Section 6.4.1 [***Activation Data Generation and Installation***] covers the requirements governing the quality of these mechanisms.

Intermediate CA private keys shall only be activated by Intermediate CA custodian staff, enabling the nCipher nShield Connect HSM associated with CAs private key using OCS and Passphrases.

6.2.9. Method of Deactivating Private Key

Cryptographic modules that have been activated must remain protected. Modules must not, remain unprotected at any time without deactivation. Deactivation may be achieved using software control command, physical removal of power. Hardware cryptographic modules shall always be removed from the system when not in use.

Private keys maintained in end-entities can be deactivated by means of powering down that end-entity. Utilising command lines to remove certificate and associated private keys or simply resetting the hardware device.

6.2.10. Method of Destroying Private Key

Private keys shall be destroyed when no longer required (including lifetime expiry and revocation). For software cryptographic modules, this shall be performed by overwriting the data using an approved wiping mechanism. For hardware cryptographic modules, a ‘zeroing’ mechanism shall be used.

nCipher HSM’s undergoing a factory reset shall have all previous configuration and private keys permanently erased.

Under certain circumstances, physical destruction of smartcards that are no longer required, or have reached the end of their useful life may be required.

6.2.11. Cryptographic Module Rating

Section 6.2.1 [***Cryptographic Module Standards and Controls***] covers Cryptographic Module Rating.

6.3. Other Aspects of key Pair Management

6.3.1. Public Key Archival

Not stipulated within this document.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

The following lifetimes are the maximum as defined by the Inmarsat Certificate Policy:

- Root CA – 30 Years
- Intermediate CAs – 15 Years
- Issuing CAs – 7 years
- End-Entities – 1, 2, 3 or 4 Year(s)

6.4. Activation data

6.4.1. Activation Data Generation and Installation

Access to private keys within cryptographic modules is protected by activation data. **Section 6.2.8** [***Method of Activating Private Key*Error! Reference source not found.**] identifies t he permitted mechanisms for activation data. Where non-biometric mechanisms are adopted, an approved password shall be used.

nCipher module activation, password used to log into the local server desktop is complex. The HSM Security World is auto generated by the HSM and consists of sixteen (16) characters. The HSM card set passphrase is a set of alphanumeric characters manually generated by applying the following rules:

a. Passphrase entries shall be a minimum of 8 digits in length
    - Passphrase must be complex, containing at least 1 uppercase, lowercase number, and symbol.
b. User passwords shall be random strings, not based on a dictionary word nor personally related to the subscriber

The card set key protection device is called a called ACS/OCS. The cards are used in every aspect in controlling the HSM

Data Type	Generation Criteria	Passphrase Changeable
Admin Card Set	8 Character, Complex	Yes
Operational Card Set	8 Character, Complex	Yes

Table 11: nCipher NShield Connect Overview

6.4.2. Activation Data Protection

Activation data shall be treated in the same manner as long-term system access passwords. This shall be protected by cryptographic storage and/or physical access such as secure cabinets. All data shall be secured to prevent compromise.

6.4.3. Other Aspects of Activation Data

Where a certificate re-key is performed in conjunction with an existing cryptographic module the activation data shall be changed at the same time.

6.5. Computer Security Controls

6.5.1. Specific Computer Security Technical Requirements

Intermediate CA server shall include the following functionality provided either by the operating system or through a combination of operating system, application, or physical safeguards:

- Access control to CA server services and roles
- Enforced separation of duties
- Identification and authentication of roles and associated identities
- Use of cryptography for session communication and database security
- Archival of CA and End-Entity history and audit data
- Audit of security related events
- Trusted path for identification of roles and associated identities
- Recovery mechanisms for Keys and the CA system
- Enforcement of domain integrity boundaries for security critical processes

All access to hardware configuration will be protected by local BIOS password.

6.5.2. Computer Security Rating

Computer hardware and deployment will meet Inmarsat security standards providing the following as a minimum:

- self-protection
- process isolation
- discretionary access control
- a protected audit record

6.6. Life Cycle Technical Controls

6.6.1. System Development Controls

Certificate service will be in procession of a test model system, which will be used for any patch update testing prior to commissioning for live usage.

System management will fully utilise an offline model office and will ensure full backups are completed and verified prior to any maintenance work such as patching.

6.6.2. Security Management Controls

Intermediate servers use OS Ubuntu shall provide security controls on access and changes.

Configuration and System management shall be used to maintain the integrity of the system and notify any changes to the system administrators. Configuration management can be used to roll back any unauthorised changes maintaining the system baseline.

All equipment used within the certificate services will have:

- Limited Access to nCipher network HSMs
- Access to Intermediate CA server limited by local credential controls

6.6.3. Life Cycle Security Controls

All equipment used within the environment has been procured, delivered, and commissioned in a manner designed to reduce the risk of a compromise and the integrity of the services it provides as part of the overall Inmarsat infrastructure.

Equipment update or repair shall be conducted in a manner compatible with the above objective.

6.7. Network Security Controls

The Intermediate CA server has a status of on-line, but is protected by networks security ACLs and local a firewall.

6.8. Time-Stamping

The Intermediate CA server does not support or provide a Time Stamping Service as defined in RFC 3161 *Time Stamp Protocol.*

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate Profile

The CA servers issue certificates for use with a single given certificate profile to meet the needs and issuance. The certificate profile will not use the default templates created at the time of a CA server installation.

7.1.1. Version Number(s)

The CA servers only issues X.509 version 3 certificates.

7.1.2. Certificate Extensions

The CA servers include all the extensions defined in the Inmarsat Interface Specification for each type of certificate. In addition, some private extensions include:

- *extendedKeyUsage* extension. Specifically, this is a control for the export of private keys to a backup medium.

The certificate extensions used generically as follows:

- KeyUsage - Classified as critical
- BasicConstraints - Classified as critical
- CertificatePolicies - Classified as non-critical
- SubjectAlternativeName - Classified as non-critical
- CRLDistributionPoint - Classified as non-critical
- Subject Key Identifier - Classified as non-critical
- Authority Key Identifier - Classified as non-critical
- extKeyUsage - Classified as non-critical
- Auth. Information Access - Classified as non-critical

7.1.3. Algorithm Object Identifiers

The CA servers comply with the requirements of the Inmarsat Interface Specification with respect to the use of algorithm object identifiers. The OID's utilised are:

Signature Algorithm	Sha256WithRSAEncryption RSA-2048 SHA-2	[iso(1) member-body(2)us(840)rsadsi(113549) pkcs(1) pkcs-1(1) 1] – OID 1.2.840.113549.1.1.11
Accepted subject key generation algorithm	RSAEncryption RSA-2048	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1] – OID 1.2.840.113549.1.1.1

Table 12 - Object Identifiers

7.1.4. Name Forms

Certificates issued by the Intermediate CA service shall include Subject name, containing an X.501 Distinguished Name (DN) conformant with X.501. The DN is formatted so that the common name Relative Distinguished Name (RDN) contains the fully qualified domain name of the device.

- The common name RDN contains the fully qualified domain name of the end-entity
- example: cn=my-server,o=Inmarsat,c=gb

Where applicable certificates issued by the CA Server may also contain a *subjectAlternativeName* of the forms permitted by the naming policy.

7.1.5. Name Constraints

Name constraints shall comply with PKIX standards.

7.1.6. Certificate Policy Object Identifier

The CA servers issue certificates to end-entities and policy marked as non-critical. The policy identifier shall be set to 'Inmarsat CPS' OID 1.3.6.1.4.1.1840.60.2.1

7.1.7. Usage of Policy Constraints extension

Not stipulated within this CPS.

7.1.8. Policy Qualifiers Syntax and Semantics

The CA Server includes a URI for the Inmarsat CP document as a policy qualifier in all of the certificates it issues.

7.1.9. Processing semantics for the critical Certificate Policies Extension

The *certificatePolicies* extension shall be marked as critical for issuing CA certificate extensions. Relying Parties should be aware that they may use a certificate in an inappropriate manner if this extension is ignored by noncompliant software.

7.2. CRL profile

The CA Server publishes certificate revocation lists that conform to the specification contained in the Inmarsat Interface Specification.

7.2.1. Version number(s)

The CA Server only publishes X.509 version 2 certificate revocation lists.

7.2.2. CRL and CRL entry extensions

The rules for inclusion, assignment of values and criticality of extensions are defined in the Inmarsat Interface Specification. No variation on these profiles will be employed by the Inmarsat CA service.

7.3. OCSP profile

7.3.1. Version Number (s)

The profile is defined in RFC 6960. It is also compatible with RFC 5019.

7.3.2. OCSP Extensions

The Validation Authority supports signed requests and the NONCE extension.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency or Circumstances of Assessment

The frequency and extent of audits are to be determined by the **IPMG** on a case-by-case basis. The **IPMG** shall have the free and unrestricted right to audit and inspect, staff, documents, and data of any component of the Inmarsat CA service. For the purposes of evaluating that component's compliance with the terms of this Certificate Practice Statement.

On an annual basis the Inmarsat CA service operators shall either, (i) certify to the **IPMG** that it always has during the period in question complied with the requirements of this practice statement. Alternatively, (ii) provide to the **IPMG** details of any periods of non-compliance and explain the reasons why the Inmarsat CA service has not complied with the CPS.

8.2. Identity/Qualifications of Assessor

The auditor/assessor shall have such qualifications that accord with best commercial practice or as required by law.

In addition, any person or entity either internal or external to undertaking a compliance inspection shall possess significant experience with PKI and cryptographic technologies as well as the operation of relevant CA server software.

The **IPMG** are responsible for ensuring that an appropriate person or organisation performs the compliance audit or inspection in accordance to the Inmarsat CP and any imposed **IPMG** policies.

8.3. Assessor's Relationship to Assessed Entity

Aside from the audit, function the auditor and audited party shall not have any current or planned financial, legal, or other relationship that could result in a conflict of interest. If a potential conflict of interest should arise at any time for the assessor, it will be reported to the **IPMG** for advice/action.

8.4. Topics Covered by Assessment

The audit should assess that:

- This Intermediate CA CPS governs the Inmarsat CA Intermediate service describing in sufficient detail technical, procedural and personnel policies and practices of the component and that those practices meet the requirements of the Inmarsat Certificate Policy.
- Intermediate CA service implements and complies with the technical, procedural and personnel practices and policies described in this Intermediate CA CPS.

The topics covered by a compliance and/or conformance audit should include:

- Physical security
- Documentation and process
- Vetting of operational personnel
- Technical security measures
- Privacy, including compliance with Data Protection laws

The **IPMG**, if appropriate shall give advance notice to Intermediate CA service owners (of not less than 10 working days) the aspects of the CA service that will be audited for any given inspection.

CA service owners shall co-operate with the auditor and shall afford the auditor all reasonable assistance and access to premises, staff, documentation, and data. The CA service owners shall provide a full text version of this Intermediate CA CPS when required for the purposes of any audit, inspection, accreditation, or if required any cross-certification.

8.5. Actions taken as a Result of Deficiency

Irregularities found resulting from a scheduled audit, Intermediate CA service owners shall be informed in writing immediately. Intermediate CA service owners shall submit a report to the auditor or directly to the auditor for the remedial action to be taken in response to the identified deficiencies. This report shall include a time for completion to be approved by the auditor or by the **IPMG** as appropriate. The **IPMG** shall be kept always informed by the Intermediate CA service owner's team.

Remedial action may include suspension or revocation of the issuing CA certificates as defined in **Section 4.9** [***Certificate Revocation and Suspension***].

Where Intermediate CA service owners team fail to take appropriate action in response to the identified deficiencies the **IPMG** shall be informed and shall take the appropriate action according to the severity of the deficiencies, which shall include:

- Noting the deficiencies but allowing the CA service to continue operations until the next planned or newly scheduled inspection
- Allow the CA service to continue operations for a determined number of days pending correction of any problems prior to revocation
- Revoking the issuing CA's certificate

8.6. Communication of Results

Audit results are treated as confidential. Unless otherwise specified in an applicable contract they shall be treated in accordance with **Section 9.3** of the **Inmarsat Certification Policy**.

The issuing CA servers do not cross-certify with any entities hence no stipulation is made here of other entities audit results.

9. OTHER BUSINESS AND LEGAL MATTERS

This document defers to the Inmarsat Certification Policy in other business and legal matters.

10. ANNEX A – DEFINITIONS

Term	Definition
Activation Data	Private data, other than keys, that are required to access cryptographic modules (i.e., unlock Private Keys for signing or decryption events)
Applicant	The Subscriber is sometimes also called an “applicant” after applying to a CA for a Certificate, but before the Certificate issuance procedure is completed
Authority Revocation List	A list maintained by the Intermediate-CA of the Certificates which it has issued that it has revoked prior to their stated expiration date.
CA Software	The application software used to operate the CA.
Certificate	An X.509 certificate as profiled in RFC5280 and issued under the Inmarsat PKI.
Certification Authority	Entities that issue Certificates under this Certificate Policy – This includes The Cryptographic Intermediate of Trust, Intermediate-CA and Sub-CA’s.
Certificate Policy	This set of rules governing the applicability of a Certificate to a particular community and/or class of application with common security requirements
Certification Practice Statement	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing Certificates, and providing access to them, in accordance with specific requirements (e.g., requirements specified in this Certificate Policy, or requirements specified in a contract for services)
Certificate Revocation List	A list maintained by a CA of the Certificates which it has issued that it has revoked prior to their stated expiration date.
Certificate Services Agreement	An agreement between the Intermediate-CA and a Sub-CA under which the Sub-CA undertakes certain obligations and liabilities to the Intermediate-CA in accordance with this Certificate Policy.
Certificate Status Services	A service that enables the user to determination of the status of a Certificate.
Certificate Subject Name	The field in an X.509 Certificate that holds the identity of the entity to whom a Certificate is issued.
Cross-Certificate	A Certificate issued between two Certification Authorities used to establish and indicate a trust relationship between them
Crypto Custodian	A Custodian is appointed at each location where crypto items are held and responsible for the management and accounting of all cryptographic items under their control. Where these items bear the CRYPTO or ACCSEC descriptors, the Custodian will usually be referred to as the CRYPTO or ACCSEC
Digital Signature	The result of a transformation of a message by means of a cryptographic system using private/public key pairs and Certificates such that the recipient of the message and signature can determine: (1) whether the transformation was created using the Private Key which complements the public key in the Certificate; and (2) whether the message has been altered since the transformation was made
Distinguished Name	X.501 Distinguished Name.
Eligible Certification Authorities	The bodies which are eligible to apply to become Certification Authorities within Inmarsat PKI

Term	Definition
Eligible Registration Authorities	The bodies which are eligible to apply to become Registration Authorities within the Inmarsat PKI
Eligible End-Entity Subscribers	The bodies which are eligible to apply to become Subscribers within the Inmarsat PKI
End-Entity	End-Entity Subscriber and End-Entity Subject
End-Entity Certificate	The final (lowest) Certificate in the chain of Inmarsat Certificate hierarchy
End-Entity Subjects	The devices that use the End-Entity Certificates
End-Entity Subscribers	The organisations or individuals responsible for End-Entity Certificates
Hierarchical Trust Model	A hierarchical trust model is one in which every key can be the subject of no more than one Certificate or Certificate request message
immediately	References in this document to immediately mean within 1 hour.
Intellectual Property Rights	Any copyright, patent, trade mark, service mark, design right, and any trade or business name or logo, or moral right, database right or know how (whether capable of registration or not in any country including the UK) and any such right in respect of which an application has been made to a competent authority.
Issuing CA	A CA that issues, or has issued, a Certificate
IT Health Check	IT Health Check is an independent check, consisting of a number of practical, expert tests, on an IT system or network to ensure that known security vulnerabilities which may compromise the confidentiality, integrity or availability of the information on that IT system or network have been adequately addressed or eliminated.
Object Identifier	A representation of the CP within the Certificate.
Private Key	The key which complements the key identified in the Certificate (the Public Key)

11. ANNEX B – ACRONYMS

Term	Expansion
ARL	Authority Revocation List
ASCII	American Standard Code for Information Interchange
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
ECDSA	Elliptic Curve Digital Signature Algorithm as specified in FIPS 186-2
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IETF	Internet Engineering Task Force
II-CPS	Inmarsat Intermediate Certificate Practice Statement
IPMG	Inmarsat PKI Management Group
IPsec	Internet Protocol Security. This is an IETF standard.
ISO/IEC	International Organization for Standardization (ISO) and the International Electrotechnical Commission
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OrgID	Organisational Identifier
PIN	Personal Identification Number
PKCS#10	Public Key Cryptography Standards (#10 – Certification request syntax)
PKD	Public Key Directory
PKI	Public Key Infrastructure
PKIX	Public-Key Infrastructure (X.509) working group
PMA	Policy Management Authority
RA	Registration Authority
RFC	Request for Comment
Intermediate-CA	Intermediate Certification Authority
RSA	Rivest, Shamir and Adleman Encryption/Signature Algorithm
SC	Security Check
SHA	Secure Hash Algorithm as defined in FIPS 180-3
SP	Service Provider
SSO	System Security Officer
Sub-CA	Subordinate Certification Authority
X.500	The set of ITU-T standards covering electronic directory services, reference [10]
X.501	A specification, detailing the information models in use in the X.500 Directory
X.509	A specification for the format of a Certificate

12. REFERENCES

All documents defined within this reference refer not only to the version specified but also to all subsequent amendments, revisions or versions.