

**COMBINED
COMMUNICATIONS ELECTRONICS BOARD**

**GATEWAY-TO-GATEWAY
IMPLEMENTATION GUIDE FOR
ACP 123/STANAG 4406 MESSAGING
SERVICES**

Draft



ACP 145

May 2003

Version 1.0 dated 1 May 2003

FOREWORD

1. The Combined Communications-Electronics Board (CCEB) is comprised of the five member nations, Australia, Canada, New Zealand, United Kingdom and United States and is the Sponsoring Authority for all Allied Communications Publications (ACPs). ACPs are raised and issued under common agreement between the member nations.
2. ACP 145, Gateway-to-Gateway Implementation Guide for ACP 123/STANAG 4406 Messaging Services, is an UNCLASSIFIED CCEB publication
3. This publication contains Allied military information for official purposes only.
4. It is permitted to copy or make extracts from this publication.
5. This ACP is to be maintained and amended in accordance with the provisions of the current version of ACP 198.

Draft

THE COMBINED COMMUNICATION-ELECTRONICS BOARD
LETTER OF PROMULGATION
FOR ACP 145

1. The purpose of this Combined Communication Electronics Board (CCEB) Letter of Promulgation is to implement ACP 145 within the Armed Forces of the CCEB Nations. ACP 145, GATEWAY-TO-GATEWAY IMPLEMENTATION GUIDE FOR ACP 123/STANAG 4406 MESSAGING SERVICE, is an UNCLASSIFIED publication developed for Allied use and, under the direction of the CCEB Principals. It is promulgated for guidance, information, and use by the Armed Forces and other users of military communications facilities.

2. ACP 145 is effective on receipt for CCEB Nations and when approved by the NATO Military Committee (NAMILCOM) for NATO nations and Strategic Commands.

Effective Status

Publication	Effective for	Date	Authority
ACP 145	CCEB	On Receipt	LOP

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

For the CCEB
Principals

N. CRAM
Squadron Leader
Permanent Secretary
to CCEB

TABLE OF CONTENTS

FOREWORD..... II

LETTER OF PROMULGATION..... III
 Effective Status III

RECORD OF MESSAGE CORRECTIONS.....IV

TABLE OF CONTENTS..... V

Figures..... VIII

Tables..... VIII

INTRODUCTION.....1-1
 Background 1-1
 Purpose of the document 1-1
 Scope of the document 1-1

ARCHITECTURE2-1
 General Overview 2-1
 Gateway..... 2-1
 Network..... 2-2
 Messaging..... 2-2
 Directory..... 2-2
 Security..... 2-2

MESSAGING SERVICES3-1
 Management Services 3-1
 Procedures 3-1
 Naming and Addressing 3-1
 Priority Handling..... 3-1
 Notifications 3-1
 Distribution Codes..... 3-2
 Audit and Logging 3-2
 Address List (AL) Expansion..... 3-2
 Gateway Handling Policy..... 3-2
 Transport Envelope 3-2
 Approved P772 Content 3-3
 Quality of Service..... 3-3

DIRECTORY SERVICES4-1
 Introduction 4-1
 Standards 4-1
 Management 4-1

Procedures 4-2

Schema 4-2

MMHS support..... 4-3

PKI management support..... 4-3

Gateway support..... 4-4

Directory Information Base..... 4-4

Security..... 4-5

 Confidentiality..... 4-5

 Integrity..... 4-5

 Security domains..... 4-5

QoS..... 4-5

SECURITY SERVICES.....5-1

 Services..... 5-1

 Computer Network Defence..... 5-1

 Protocols..... 5-2

 Messaging Protocols..... 5-2

 Certificate Management..... 5-3

 Certificate Generation..... 5-4

 Certificate Distribution..... 5-4

 Root Certificate Distribution..... 5-4

 Intermediate CA Certificate(s) Distribution..... 5-4

 Gateway Certificate Distribution..... 5-5

 Lifecycle..... 5-5

 Root Certificate Renewal..... 5-5

 CA Certificate Renewal..... 5-6

 Gateway Certificate Renewal..... 5-6

 Revocation Notification..... 5-6

 Public Key Certificates..... 5-7

 Public Key Certificate Profiles..... 5-8

 Public Key Certificate Fields..... 5-9

 Public Key Certificate Extensions..... 5-11

 Public Key Certificate Checking..... 5-14

 Certificate Revocation Lists..... 5-14

 Certificate Revocation List Profiles..... 5-14

 Certificate Revocation List Fields..... 5-14

 Certificate Revocation List Entry Extensions..... 5-16

 Certificate Revocation List Extensions..... 5-17

 Certificate Revocation List Checking..... 5-18

 Cryptography..... 5-18

 Hash..... 5-19

 133.2 Digital Signature..... 5-21

 DSA with SHA-1..... 5-21

 Parameters..... 5-23

 RSA with SHA-1 (PKCS #1 version)..... 5-25

 Certificate..... **Error! Bookmark not defined.**

 Compromised Key Lists..... 5-27

Labelling.....	5-27
Security Label	5-28
Security Policy Identifier	5-28
Security Classification.....	5-28
Privacy Mark.....	5-29
Security Categories	5-29
Implicit Tags	5-29
Annex A to Chapter Five.....	1
PICS PROFORMA for Signature Certificates.....	1
A.0 Signature Certificate Introduction.....	1
A.0.1 Description of Tables	1
A.0.2 Support Classifications.....	2
A.0.2.1 Static Capability.....	2
A.0.2.2 Dynamic Capability.....	3
Identification of the implementation.....	3
Appendix B to Chap 5.....	1
PICS PROFORMA for Certificate Revocation Lists.....	1
B.0 CRL Introduction	1
B.0.1 Description of Tables	1
B.0.2 Support Classifications.....	2
B.0.2.1 Static Capability.....	2
B.0.2.2 Dynamic Capability.....	2
Identification of the implementation.....	3
ANNEX C To Chapter Five.....	1
ASN.1 Module for Security Label.....	1
IMPLEMENTATION Testing.....	6-1
Overview	6-1
Objectives of G2G Testing.....	6-1
Test Items	6-1
Core functionality.....	6-1
Operational Scenario	6-2
Test Structure	6-2
Approach	6-2
Test INDEX.....	6-3
Accreditation:	6-7
Guards	6-7
Intruder Detection	6-7
Virus Protection.....	6-7
Protocols.....	6-7
Certificate Management	6-7

Cryptography.....	6-8
Labelling.....	6-8
Authentication.....	6-8
GLOSSARY.....	7-1
Standards and References	8-1
List of Effective Pages.....	9-1

FIGURES

Figure 1: Gateway Concept.....	2-1
Figure 2: Gateway Model.....	2-2
Figure 3: Directory Information Tree Structure	4-4
Figure 4: National Gateway PKI Architecture.....	5-4
Figure 5: G2G Certificate Types.....	5-8

TABLES

Table 5-1: Hashing Algorithm	5-20
Table 5-2: Algorithm.....	5-21
Table 5-3: Certificate	5-22
Table 5-4: Algorithm.....	5-26
Table 5-5: Certificate	5-27
Table 5-6: Identification of PICS	3
Table 5-7: Identification of Implementation and/or system.....	3
Table 5-8: Identification of system supplier and/or test laboratory client	4
Table 5-9: Identification of the CRL.....	4
Table 5-10: Global statement of conformance.....	4
Table 5-11: Self-Signed CA Signature Certificate.....	5
Table 5-12: Algorithm Identifier.....	5
Table 5-13: Extensions.....	6
Table 5-14: Standard Extensions.....	7
Table 5-15: Authority Key Identifier	8
Table 5-16: Key Usage.....	8
Table 5-17: Private Key Usage Period.....	8
Table 5-18: Certificate Policies.....	9
Table 5-19: Policy Mappings	9
Table 5-20: Basic Constraints	9
Table 5-21: Name Constraints.....	9
Table 5-22: General Subtrees.....	9
Table 5-23: Policy Constraints.....	9
Table 5-24: CRL Distribution Points	10
Table 5-25: Authority Information Access	10
Table 5-26: CA Signature Certificate.....	10
Table 5-27: Algorithm Identifier.....	11

Table 5-28: Extensions.....	11
Table 5-29: Standard Extensions.....	12
Table 5-30: Authority Key Identifier.....	13
Table 5-31: Key Usage.....	13
Table 5-32: Private Key Usage Period.....	13
Table 5-33: Certificate Policies.....	13
Table 5-34: Policy Mappings.....	13
Table 5-35: Basic Constraints.....	14
Table 5-36: Name Constraints.....	14
Table 5-37: General Subtrees.....	14
Table 5-38: Policy Constraints.....	14
Table 5-39: CRL Distribution Points.....	14
Table 5-40: Authority Information Access.....	15
Table 5-41: Gateway Signature Certificate.....	15
Table 5-42: Algorithm Identifier.....	15
Table 5-43: Extensions.....	16
Table 5-44: Standard Extensions.....	16
Table 5-45: Authority Key Identifier.....	17
Table 5-46: Key Usage.....	17
Table 5-47: Private Key Usage Period.....	17
Table 5-48: Certificate Policies.....	17
Table 5-49: Policy Mappings.....	18
Table 5-50: Basic Constraints.....	18
Table 5-51: Name Constraints.....	18
Table 5-52: General Subtrees.....	18
Table 5-53: Policy Constraints.....	18
Table 5-54: CRL Distribution Points.....	19
Table 5-55: Authority Information Access.....	19
Table 5-56: Common Fields.....	20
Table 5-57: Identification of PICS.....	3
Table 5-58: Identification of Implementation and/or system.....	3
Table 5-59: Identification of system supplier and/or test laboratory client.....	3
Table 5-60: Identification of the CRL.....	4
Table 5-61: Global statement of conformance.....	4
Table 5-62: CRL.....	4
Table 5-63: Algorithm Identifier.....	4
Table 5-64: Extensions.....	5
Table 5-65: CRL Extensions.....	5
Table 5-66: Authority Key Identifier.....	5
Table 5-67: Issuing Distribution Point.....	6
Table 5-68: CRL Entry Extensions.....	6
Table 5-69: Reason Code.....	6
Table 5-70: Common Fields.....	7
Table 6-1: Level 2 Testing.....	6-4
Table 6-2: Level 3A Testing.....	6-5
Table 6-3: Level 3B Testing.....	6-6

Table 6-4: Level 4 Testing6-7

Draft

CHAPTER 1

INTRODUCTION

Background

101. Military messaging services are an essential component of a modern Defence force command and control infrastructure. Military Messaging allows commanders at all levels to effectively execute their command function and provides a mechanism for the transmission of committal orders and instructions.

102. ACP 123/STANAG 4406, ACP 133 and this Implementation Guide (ACP 145) define the standards for messaging, security and directory services required to achieve Military Messaging based on X.400 technology. Due to differences in national implementations of messaging services and, the complexity of achieving full end-to-end security services between nations, messaging between Nations will be by way of gateway services with security services provided using Secure Multipurpose Internet Mail Extensions (S/MIME) Version 3 (V3) with its Extended Security Services (ESS).

Purpose of the document

103. The purpose of this document is to provide a consolidated reference of all policy, procedures, standards and agreements required for the implementation of the agreed ACP 123/STANAG 4406 Gateway-to-Gateway (G2G) architecture between Nations.

Scope of the document

104. This document details the requirements for the implementation of gateways between National ACP 123/STANAG 4406 based Military Message Handling systems. The implementation of gateways to legacy ACP 127 or 128 systems is beyond the scope of this document. It is not intended to duplicate the text of any other document rather, provide references to other documents where these exist. Only where policy, procedures, standards or agreements are not formally documented elsewhere will full text be included.

CHAPTER 2

ARCHITECTURE

General Overview

201 ACP 123/STANAG 4406 military Messaging interoperability between Nations will be achieved through the use of messaging gateways located in each nation. To achieve interoperability, nations agree to implement the elements of services based on the messaging, directory and security standards within ACP 123/STANAG 4406, ACP 133 and S/MIME V3 with Enhanced Security Services (ESS) defined in this ACP. The gateway concept is illustrated at Figure 1.

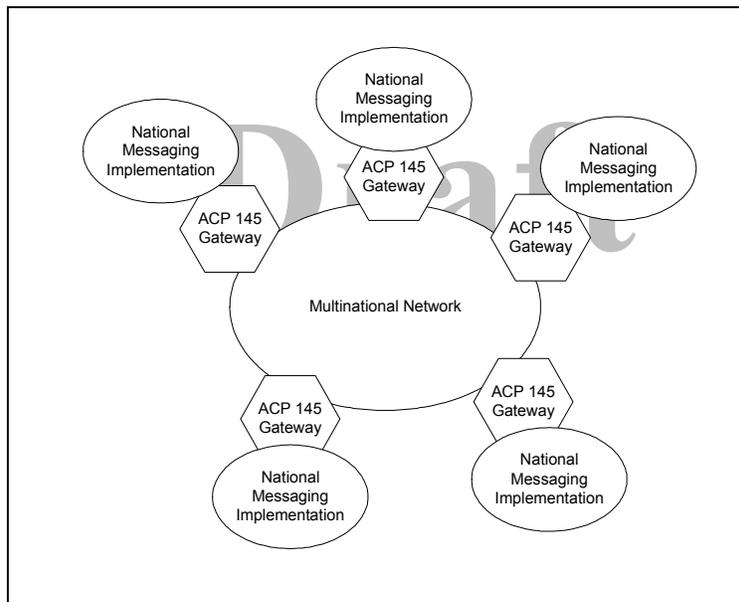


Figure 1: Gateway Concept

Gateway

202 The gateway allows Nations to be unconstrained as to their National messaging implementation by having National specific gateway functions on one side and ACP 145 specific functions on the other. The primary set of common functional capabilities provided at the gateway that are consistent among all nations are:

- P772 (as per ACP 123/STANAG 4406)
- S/MIME signature with ESS label (as per ACP 145)
- X.400 message transport (as per ACP 123/STANAG 4406)
- Directory services (as per ACP 133)

203 The gateway concept is further illustrated in Figure 2.

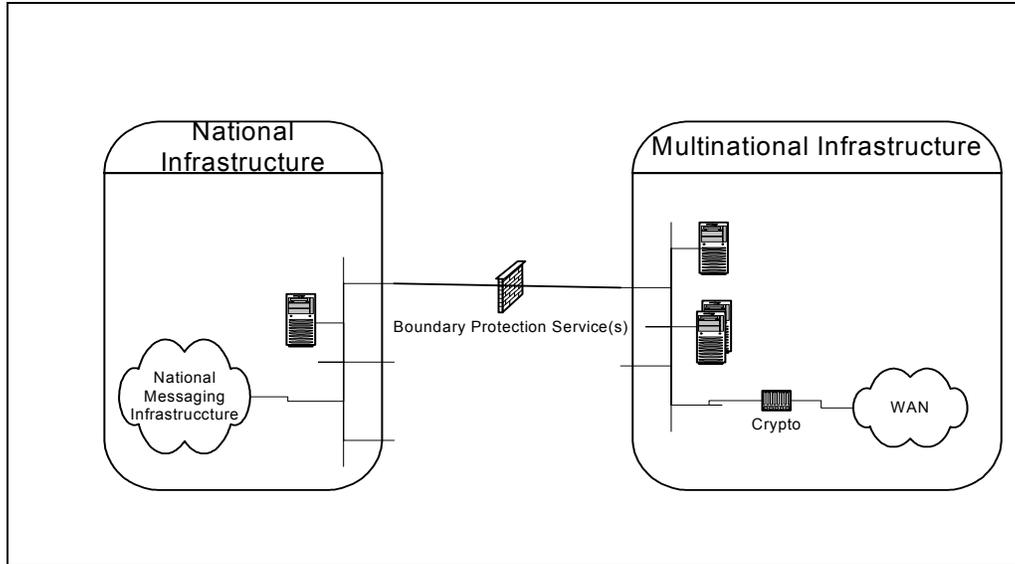


Figure 2: Gateway Model

Network

204 Any secure TCP/IP network can be used to provide network services for messaging services between National gateway infrastructures. The network will allow Information Domains to be established in support of multinational and bilateral operations between the nations.

Messaging

205 Messaging services between nations will be based on a single security domain structured architecture. The architecture has the flexibility to establish multiple domains to meet allied and coalition requirements.

Directory

206 Directory services will be provided.

Security

207 Applications layer messaging security services between national environments are provided by S/MIME V3 with ESS. Application layer security services are further enabled by either a nationally provided or coalition provided Public Key Infrastructure (PKI).

208 Confidentiality services are to be provided by the network. Nations are responsible for the provision of appropriately evaluated Boundary Protection Services (BPS). BPS includes but is not limited to content checking, virus scanning, intrusion detection and releasability checking.

209 Application layer messaging security services are defined in the Security Chapter of this document.

210 The Accreditation Authorities in each nation will accredit their national components of any shared or affiliated elements of the information domains, in order to operate as classified networks.

Draft

CHAPTER 3

MESSAGING SERVICES

Management Services

301. To achieve G2G ACP 123/STANAG 4406 interoperability, nations agree to implement the required management services. Some of these gateway management services will result from bilateral interoperability efforts among nations.

Procedures

302. To achieve G2G ACP 123/STANAG 4406 interoperability, nations agree to implement the required support procedures. Specifically, nations agree that for messages that have been successfully processed by the recipient national gateway (i.e., the message has not been blocked at the national gateway) that nation will adopt best effort procedural processes to deliver the message to the intended recipient. Circumstances may still exist, however, where non-delivery reports (NDRs) will be returned. In some cases this may require nations to use manual intervention which will have a resource impact on nations.

303. Nations agree that ACP 123 message instructions would be supported across national boundaries (see ACP 123 clause 207.g).

Naming and Addressing

304. Messages exchanged between national gateways shall comply with the naming and addressing requirements of ACP 123. In addition, the directory-name field shall be provided for each recipient of the message. The value of each directory-name provided shall consist of the X.500 distinguished name corresponding to that recipient in the ACP 145 directory.

Priority Handling

305. Nations agree to implement technical or procedural mechanisms to handle inbound ACP 123 messages in accordance with the message precedence defined in ACP 123 clause 413.

Notifications

306. For the most part, it is expected that nations will not implement identical ACP 123 solutions however, most nations will likely choose to implement most or all of the ACP 123 notifications/reports Elements of Service (EoS). Between nations, these national solutions will result in varied MTS and thus, there will be a need for a simple solution to military notifications. Nations have agreed to support the following Elements of Service (EoS):

- Delivery Report (DR) and Non-Delivery Report (NDR) (See ACP 123 clause 302)

- Receipt Notification (RN) (see ACP 123 clause 202.ag)

307. Nations agree to use best effort to deliver a message received by a recipient gateway and that if a message can not be delivered, that a NDR will be generated to the originating gateway. Nations agree that a NDR could be generated by the recipient national GW or beyond. One of the criteria for the origination of a NDR is time out. Nations agree to generate a NDR to the originating national gateway if a message has not been delivered within the recipient nation for a specified period of time. This period of time will be based on grade of delivery defined in ACP 123 clause 302. Notwithstanding, this proposed limitation on the exchange of notifications between national gateways, there would remain procedural mechanisms that could be utilized to provide positive confirmations between users (e.g., originator requesting an acknowledgement from a recipient that the message was received and understood).

Distribution Codes

308. As per ACP123 clause 207 f, the population of the distribution code element of service is optional and there is no defined requirement for a recipient gateway to distribute based on a distribution code. Therefore, it is expected that some nations will choose not to use this capability. However some nations rely on it for local distribution as well as providing backwards compatibility with ACP127 systems. Therefore, nations agree to support the transfer of distribution codes through gateways.

Audit and Logging

309. ACP 123 clause 3.11 defines the audit and logging requirements for Military Messaging.

Address List (AL) Expansion

310. ALs will only be expanded within the source domain. Due to the residual risk that source domain AL expansion could result in secondary AL expansion within a recipient domain, nations should implement either procedural (e.g., identification of external domain AL in the X.400 OR address) or technical mechanisms (e.g., ensure that a national gateway will not originate messages from an external domain OR address) to prevent secondary AL expansion to another nation.

Gateway Handling Policy

311. Nations agree to only pass formal ACP 123 messages across their boundary. ACP 127 or JANAP 128 formatted messages will not be passed through the gateway.

Transport Envelope

312. The transport envelope is defined in ACP 123 and the use of this transport mechanism with SMIME is further defined in draft-ietf-smime-x400transport-04.txt. Nations agree to use the security services defined in this ACP to transport the content type defined in ACP 123 across national boundaries.

Approved P772 Content

313. The OID for P772 is: id-nato-mmhs-cont-mm88 {1.3.26.0.4406.0.4.1}. National gateway handling policies may restrict some message content including attachment types (e.g. Executables, Word documents containing macros, etc.) from entering or leaving a national system. This presents a potential denial of service issue and may require nations to agree to a set of acceptable contents. It is anticipated that some of the content restriction will be based on bilateral agreements.

Quality of Service

314. Nations accept that circumstances may arise in which message delivery times might exceed that required by its precedence, however, there is no information to determine how or when. This should be managed using normal engineering development for sizing network.

Draft

CHAPTER 4

DIRECTORY SERVICES

Introduction

401. The directory will store communication information (MMHS, email and general contact information for organizations, organizational role and organizational people), offer a certificate and certificate revocation list repository for the gateway, exchange this information with other Nations through replication services, and protect the integrity and confidentiality of the directory data.

402. The Directory consists of a number of national Directory Service Agents (DSAs) that collectively hold the multinational Directory Information Tree (DIT) for the domains. The DSAs, which belong to the individual nations, cooperate to make the whole DIT available to international and national users. The distribution of information between these DSAs and internal systems is a national responsibility, as is the amount of information provided from a nation into the multinational directory.

403. It is anticipated that directory support for formal messaging systems will include a minimal set of information that will be shared with all nations. In particular, a subset of ACP 133 schema necessary to support ACP 145 will be defined later. Specific requirements such as for support to the gateway-to-gateway PKI are addressed in that annex. Also, supplementary information may be shared between nations on a bilateral basis.

404. The directory service will be based on the following:

- User access to Directory information will only be performed at, or behind each nation's own border DSA, and the method of access is defined by the nation.
- Everyone with access to the network will be granted read and search access to shared information.
- Only authorized directory managers (persons or applications) will be given access to add, delete and change their own directory entries.

Standards

405. The Directory Service will be based on a replication service using either the X.500 DISP protocol or a meta-directory based LDAP access or using messaging services to transport LDIF files containing National DITs or updates between Nations.

Management

406. Management of the multinational directory service nodes is a National responsibility and should include the following:

- Reliability
- Backup
- Resilience and redundancy
- Availability
- Production and management of nations' data including the integrity, timeliness, and quality of data
- Performance decisions (e.g. indexing).
- Firewalls and Border Protection Devices in accordance with network defined procedures

407. The following management functions require international agreement and coordination between all connected Nations:

- Multinational Schema
- High level DIT structure
- Multinational data dictionary
- Replication agreements
- Directory hubs (if required)
- Data integrity

408. These issues are detailed in the appropriate national and international ConOps for the network to which the ACP 145 service is to be connected.

Procedures

409. **Mastering of common entries:** Certain data held in the directory is not specific to a single Nation, but still needs to be made accessible to all directory users. An example of this shared data could be a Coalition Task Force structure allowing a common Orbat reflecting information derived from multiple Nations. In these cases, one Nation (often the lead Nation in the Coalition) would master this data, and share it alongside their National data. Where this happens, the mastering Nation is responsible for managing the shared information in exactly the same way as it manages its National data.

Schema

410. Directory support requires the storage and retrieval of information to facilitate communication to organizational units, organisational roles, and formal message address

lists. In addition, the directory will be used to publish Public Key information needed by the messaging gateway.

411. Three distinct uses of the directory have been identified to support ACP 145. These uses are addressed in the following:

- MMHS support;
- PKI management support; and
- Gateway support.

MMHS support

412. Directory requirements for military messaging are DN, OR, AL and, the 'description' attribute is highly desirable. It is not necessary to hold attributes associated with ACP 127/128 systems.

413. The following ACP 133 defined schema objects have been identified to support this function:

- **Organizational Unit entries** - Formal messages will be addressed to national organizations. ACP 133 has defined an **aCPOrganizationalUnitRuleEdB** content rule for this purpose. When using this content rule the entry must contain a **descriptive organisational unit or RDN**, and an **O/R address**.
- **Organizational Role entries** – Formal messaging may also be addressed to role-based entries within an organization. ACP 133 has defined an **aCPOrganizationalRoleRuleEdB** content rule for this purpose. When using this content rule the entry must contain a **descriptive common name or RDN**, and an **O/R address**.
- **Formal Messaging Address Lists** – In accordance to ACP 100 a nation will be responsible for establishing formal message address lists. The Directory service will be used to publish these lists amongst the nations. ACP 133 has defined an **addressListRuleEdA** content rule for this purpose. When using this object class the entry must contain a name as defined in ACP 100 for the address list in the **common name** attribute, the distinguished names of action members of the address list in the **member** attribute, and the distinguished names of information members of the address list in the **copyMember** attribute. The owner of the address list will need to assure that entries exist for members contained in the address lists being published by the nations.

PKI management support

414. A PKI or PKIs will be established for the national messaging gateways. The directory service will support the use of PKI(s) between gateways by publishing the information necessary for path validation of gateway certificates and the distribution of

Certification Authority’s certificate revocation list (CRL). Certificate Authority entry distinguished names shall align with the name stored in the issuer field of the CA certificate.

415. **Root CA entry** – This object must be based on an structural object class which can incorporate the pkiCA auxiliary object class. This entry is used to store the CRL and ARL. Because the Root CA certificate is distributed in a secure out-of-band mechanism, the cACertificate attribute must not be populated in the directory.

416. **Intermediate CA entry** - This object must be based on an structural object class which can incorporate the pkiCA auxiliary object class. This entry is used to store the certificate and CRL.

Gateway support

417. Currently, directory support for the ACP 145 gateway entities is limited to gateway PKI support, although future requirements may emerge and will then be incorporated.

418. **Messaging Gateway PKI support** – ACP 133 has extended many of the standard object classes to enable PKI. However, to reduce the number of object class that needs to be supported by applications, it is advised that the userCertificate attribute is used to hold the gateway certificate in one of the following object class:

aCPOrganizationRoleRuleEdB or **aCPOrganizationalUnitRuleEdB**.

Directory Information Base

419. The Directory naming will be based on the country naming context. While the nations are ultimately responsible for their individual DIT structure the diagram below describe the current high level DIT structure. Adherence to this high level DIT will ensure interoperability and replication of directory data. Lower level DITs will reflect national implementation and will differ.

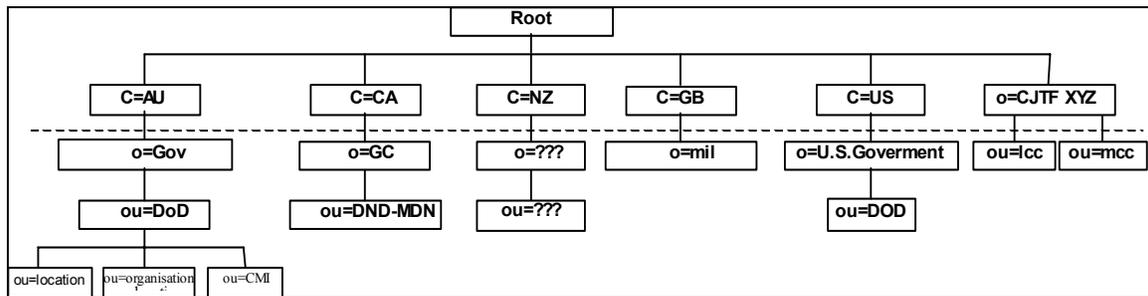


Figure 3: Directory Information Tree Structure

420. There is a requirement to replicate directory information between nations operating ACP 145 gateways to support their messaging interchange. The implementation will be dependent on a number of factors including support for multiple

security domains, network topology and security requirements. Alternatives could include X.525 DISP, meta-directory or LDIF file exchange.

Security

Confidentiality.

421. The network layer IP encryption ensures confidentiality of directory information replicated through the gateway. No further encryption will be used in the replication process.

Integrity.

422. Integrity and synchronization of data must be ensured as directory information is transferred between nations. This will depend on the implementation and could make use of hashing or other acceptable means.

Security domains.

423. If a need for multiple security domain is identified, nations will be responsible for sharing only the sub-set of information releasable to a particular security domain.

QoS

424. The DS will be designed for availability on a 24/7 basis. Availability of the national border DSAs is a national responsibility, but should avoid sustained down time. Temporary unavailability of a replication partner will not prevent local access to other nations' data, although some data may not be fully up to date. The quality and applicability of a nation's data is governed by the nation. However, each nation should endeavour to supply the necessary quantity and quality of data to support multilateral enabled applications.

CHAPTER 5

SECURITY SERVICES

Services

501. There are three application layer message security services. They are:

- Authentication of Origin
- Message Integrity
- Security Labels

502. The message security services are implemented through the combination of generating a single digital signature wrapper over the P772 content type with the Cryptographic Message Syntax (CMS) for authentication of origin and message integrity and the Extended Security Services for S/MIME (ESS) for Security Labels.

503. The following are the application layer directory security services:

- Directory will have unrestricted read access and access control will be established for writing/modifying data. In particular nations must insure that write access is denied to all on another nations' DIT copy.

Computer Network Defence

504. Computer Network Defence (CND) is the operational component of Information Assurance. CND will be conducted on the underlying bearer environment. This section will define the characteristics expected of the underlying bearer environment. This is driven by the Threat Analysis which is to be undertaken for formal messaging over the bearer network.

505. Actions taken to protect, monitor, analyse, detect, and respond to unauthorized activity within information systems and computer networks. Network CND will be conducted within a framework of CND activities/elements to include, but not limited to:

- Vulnerability analysis/assessment and intrusion detection
- Boundary protection (e.g., firewalls/ guards/ cryptography/ gateways/ biometrics/ account authentication)
- Compliance and audit reporting for Information Assurance alerts, advisories, bulletins, and patches
- Indications and warning
- Network health

- Infrastructure inventory
- Standard Operating Procedures to identify, report, manage, investigate and remedy security related incidents/intrusions

Protocols

Messaging Protocols

506. The NATO Profile for the use of S/MIME CMS and ESS (AppSy AHWG 0209/4-12), profiles the use of CMS, CMS Algorithms, Extended Security Services for S/MIME, Securing X.400 Content with S/MIME, and Transporting S/MIME objects in X.400. This clause modifies that document. It is a National decision whether the Gateway's CMS and ESS support is limited by removing support for optional services or by ensuring the services are not invoked though they are supported. The following lists the differences between this profile and the NATO profile:

- In clause 3.3.1, the certificate and CRL profile required is the NATO certificate and CRL profile. In its place this document uses the certificate and CRL profile specified in this document in paragraph 531. Note that the ACP 145 PKI profiles are identical to the NATO PKI Profiles.
- Clause 3.3.3.1 specifies the required signed attributes. This document requires support for signed attributes as specified in clause 3.3.3.1 except the following; however, these attributes could be supported internal to a nation or on a bilateral basis:
 - receiptRequest – is not supported because signed receipts between two well-defined end points over a link layer protected network is of dubious value.
 - mlExpansionHistory – is not supported because within the CCEB environment Address Lists (ALs) will be source side expanded thereby avoiding looping via procedural mechanisms. Note that the STANAG allows either source side or recipient side expansion.
 - contentHints – is not supported because only a single signed data is used between Gateways. Triple wrapping, signed data around encrypted data around a signed data, is not supported.
 - Note that signingTime, sMIMECapabilities, and sMIMEEncryptionKeyPreference are SHOULD support on origination and MUST support on reception. Though they are not required for support in the G2G architecture they are nevertheless "supported" to ensure standard's compliant products are not necessarily crippled to remove "support." Additionally, each may be supported on a bilateral basis.
- In clause 4, only clause 4.3.1 applies. Further, the directions for populating the fields in the essSecurityLabel attribute are specified paragraph 553 with additional

information provided by national documents. Note that the CCEB and NATO frameworks for the labelling structures are identical. Only the specific values that are included in the structure are different because the values are specific to a particular security policy (e.g., NATO, US GENSER, FR MUSE).

Certificate Management

507. Each Nation has a PKI to support internal national Public Key (PK) enabled applications. However, the evolving nature of National PKIs and the technically divergent National PKIs has lead many Nations to adopt a PKI that supports the G2G Architecture with Certificate Authorities (CAs) that are not subscribers of their National PKI. In order to minimize the risk associated with the use of evolving national PKIs, it is strongly recommended that nations deploy PKIs independent from their national PKIs to support their Gateway. Alternatively they may subscribe to another Nation's Gateway PKI.

508. The National Gateway PKI should be designed to minimize the amount of information that would need to be published to other nations. It is therefore recommended that the Gateway PKI should only consist of a root (self-siging entity), subordinate CA and the Relying Party, i.e., the National Gateway(s) (see Figure 4).¹

509. Trust is distributed amongst the National Gateways via the exchange of the National Gateway PKI's Root certificates (see below). The Root certificates are placed into a "trust file," which the Gateway uses during digital signature verification (see Figure 4). Only the Gateway PKI Root CA certificate is needed in the trust file because the Gateway who performed the signature includes the CA's certificate who issued their certificate in the message (see below).

¹ The Root CA might not directly issue the Gateway's certificate because some Certification Policies will require an off-line Root CA. Additionally, the CertP will likely require less frequent updates (on the order of once a month) of Root CA CRL directory entries compared to very frequent updates (on the order of hours) of CA CRL directory entries leading to a design that delegates Gateway certificate issuance to a CA other than the Root CA.

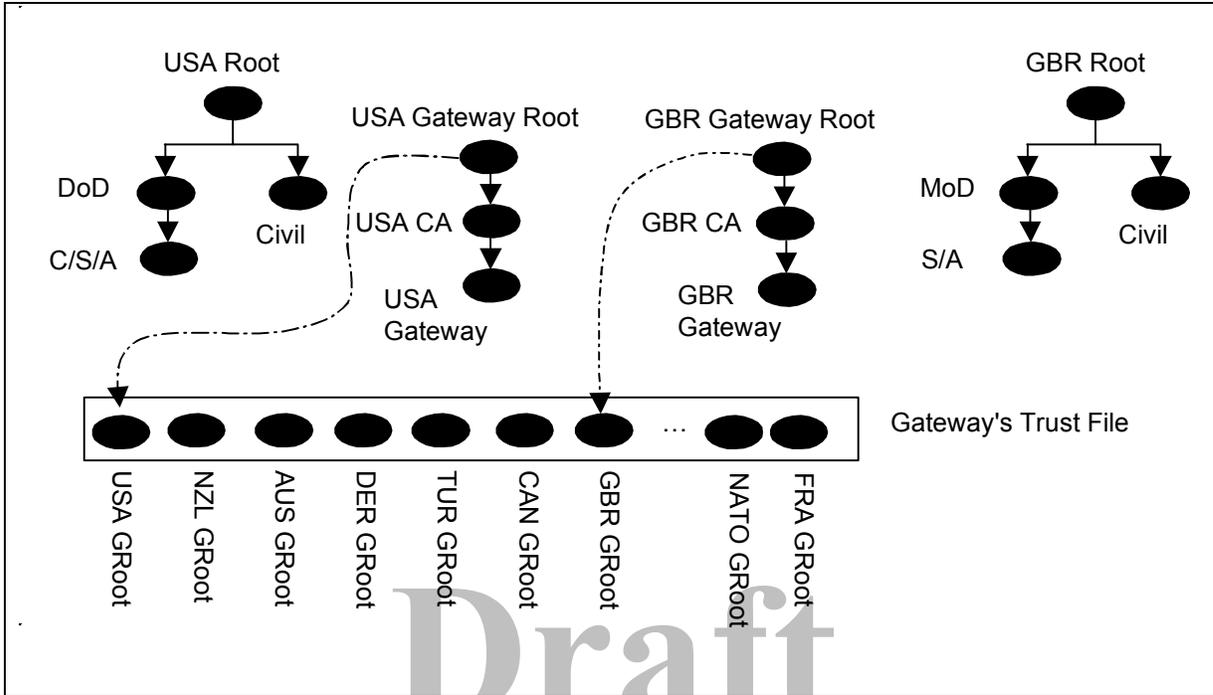


Figure 4: National Gateway PKI Architecture

Certificate Generation

510. The specific requirements for the Root CA certificate, Intermediate CA's certificate(s), and Gateway's certificate are included in paragraph 531. The processing requirements for RPs can be found in paragraph 532.

511. A PKI may have a number of levels. Implementation should not assume a particular level of hierarchy. The PKI architecture notes that implementations should not be constrained to process a particular number of levels within the PKI hierarchy and document them in the Authentication Framework

Certificate Distribution

Root Certificate Distribution

512. Distribution of the National Gateway PKI's Root Certificate is performed via the exchange of a floppy disk, CD, or some other bilaterally agreed mechanism, which contains the DER encoded public key certificate of the Nation's Gateway Root Certificate, in a diplomatic pouch.

Intermediate CA Certificate(s) Distribution

513. Distribution of Intermediate Gateway CAs certificate is done via two mechanisms. Including the CA's public key certificate in the SigningCertificate attribute with the signed S/MIME v3 generated by the Gateway as the primary distribution

method, as described in paragraph 506. The secondary method is the pkiCA X.500 directory attribute, as described in paragraph 415. The CA's public key certificate is included in the cACertificate attribute. Note that the CA's directory entry and the directory name contained in the CA's certificate issuer field must match.

Gateway Certificate Distribution

514. The Gateway's public key certificate is distributed in the CertificateSet.CertificateChoices.certificate field within signedData generated, as described in paragraph 506. This certificate will also be available in the directory gateway entry as described in the gateway support section of Chapter 4.

Lifecycle

515. All subscribers of the PKI may, at one time or another, require new certificates. Root CAs, Intermediate CAs, and Gateways may need new certificates to continue subscribing to the PKI after the validity date in their certificate passes, to resubscribe to the PKI after their certificate has been compromised, and to update some information bound in to the certificate (e.g., subject name or key). Various terms (e.g., renewal, rekey, update, reissue) are sometimes used to address the various scenarios but for simplicity this document will use the term renewal. Further, the procedures defined herein imply that the renewal process will result in a name being bound to new key (i.e., a new key will be generated for the public key certificate). Nations may choose to implement more complicated mechanisms for example where the public key is retained, but these more complicated mechanisms are not necessary to support the G2G architecture and hence are not described herein.

Root Certificate Renewal

516. To support Nation's Gateway Root Certificate expiration (i.e., current date is past the validity date in the certificate), a new self-signed certificate needs to be generated and distributed to the other nations via the procedure defined in paragraph 512. In order to ensure uninterrupted service, the new self-signed certificate should be generated and distributed at least one month prior to the end of the validity period of the operational certificate (this should be seen as the default period and can be negotiated on a bilateral basis). After the validity date passes on any operational Root CA certificate, it is not included in the CRL as it has not been revoked it just naturally expires.

517. To support Nation's Gateway Root certificate compromise, a new self-signed certificate needs to be generated and distributed via the procedures defined in 512. Further, revocation information for the Nation's Gateway Root, any Intermediate CA(s), and any Gateway certificates needs to be generated and distributed via the procedures in paragraphs 522 to 524 and these certificates needs to be reissued as in paragraph 510. In order to minimize the disruption to the service additional Root Certificates must be distributed with the operational certificate. The keys associated with the additional certificates should be stored separately from the key chosen for current operations to

remove the risk of multiple compromises. Note: this requires the National Gateway Root CA to be able to import and export private keys.

CA Certificate Renewal

518. To support Intermediate CA certificate expiration (i.e., current date is past the validity date in the certificate), a new certificate needs to be issued to the Intermediate CA and distributed via the procedure defined in paragraph 513. In order to ensure uninterrupted service, the new certificate should be generated and distributed two weeks prior to end of the validity period of the operational (this should be seen as the default period and can be negotiated on a bilateral basis). After the validity date passes on any operational Intermediate Certificate, it is not included in the CRL as it has not expired; it just naturally expires.

519. To support Intermediate CA certificate compromise, a new CA certificate needs to be issued and distributed via the procedures in paragraph 516. Further revocation notifications for the CA, any subordinate CA(s), and Gateway certificates must be generated and distributed via the procedures in paragraph 516 and these certificates needs to be reissued as in paragraph 510.

Gateway Certificate Renewal

520. To support Gateway certificate expiration (i.e., current date is past the validity date in the certificate), a new certificate needs to be issued to the Gateway and distributed via the procedure defined in paragraph 514. There is no need to generate a new Gateway certificate prior to the end of the validity date because the new Gateway certificate is distributed with the first signed message that uses the new Gateway certificate.

521. To support Gateway certificate compromise, a new Gateway certificate needs to be issued and distributed via the procedures in 514. Further revocation notifications must be generated and distributed via the procedures in paragraphs 522 to 524.

Revocation Notification

522. Revocation of a National Gateway PKI Root CA certificate is a catastrophic event that requires immediate action be taken by each of the National Gateway's Points of Contact (POC). In the event of a National Gateway Root CA revocation, all Nations with which the revoked National PKI Gateway Root CA certificate has been shared must be contacted to indicate that the Nation's Gateway Root CA certificate has been revoked. Each National POC needs to remove the compromised Root CA certificate from their Gateway's Trust File. The Nation whose Root CA certificate was revoked then needs to re-initialise their Gateway's PKI by generating a new private key, distributing the corresponding public key certificate (see paragraph 512), generating new CA

certificate(s), and Gateway certificate(s). Further, the new National Root CA certificate must issue and distribute a CRL indicating the old Root CA certificate is revoked.²

523. Likewise, revocation of any Intermediate CA certificate(s) that was used to issue a National Gateway certificate is a catastrophic event. In the event of an Intermediate CA revocation, all Nations with which the revoked Intermediate CA certificate has been shared must be contacted to indicate that the Intermediate CA certificate has been revoked. Each National POC needs to remove the compromised Intermediate CA certificate from their Gateway. The Nation whose Intermediate CA certificate was revoked then needs to re-initialise their Intermediate CA by generating a new private key, distributing the corresponding public key certificate (see paragraph 523) and Gateway certificate(s). Further, the CA, Root or Intermediate, that issue the Intermediate CA certificate must issue and distribute a CRL indicating the old Intermediate CA certificate is revoked.

524. If the Nation's Gateway certificate is issued directly from the National PKI Root CA, then it must generate a CRL. In the event of a Nation's Gateway revocation, all Nations with which the revoked Gateway certificate has been shared must be contacted to indicate that the Gateway certificate has been revoked. Each National POC needs to remove the compromised Gateway certificate from their Gateway. The Nation whose Gateway certificate was revoked then needs to re-initialise their Gateway by generating a new private key, distributing the corresponding public key certificate (see paragraph 512). Further, the Intermediate CA that issued the old Gateway certificate must issue and distribute a CRL indicating the old Gateway certificate is revoked.

525. Replication will generally happen every 24 hours unless operational constraints dictate otherwise. However, all CAs including Root CAs will be required to generate CRLs. If there are no revoked certificates the CAs are required to publish an empty CRL (i.e., a CRL with no revoked certificates). The directory entry for a particular CA contains the *certificateRevocationList* attribute in which all known revoked certificates will be included for at least one period beyond the revoked certificate's validity period, as per paragraph 3.3 of RFC 3280. The directory entry for a particular CA also contains the *authorityRevocationList* attribute in which an exact copy of the contents of the *certificateRevocationList* attribute will be stored. Note that the CA's directory entry and the directory name contained in the CA's CRL *issuer* field are the same.

526. The specific requirements for a CA's CRL generation are included in paragraphs 536 to 540. The processing requirements for RPs can also be found in those paragraphs.

Public Key Certificates

527. This section specifies the Version 3 (V3) X.509 certificates as described in Recommendation X.509 (1997) and profiled in RFC 3280. The certificate profiles documented in paragraph 531 for the CCEB are identical to the NATO certificate

² This requires that the product used to instantiate the Root CA does not always issue the same certificate serial number.

profiles. Three "types" of certificates are needed to support the G2G architecture. Three "types" of certificates are described herein and are as depicted in Figure 5 below.

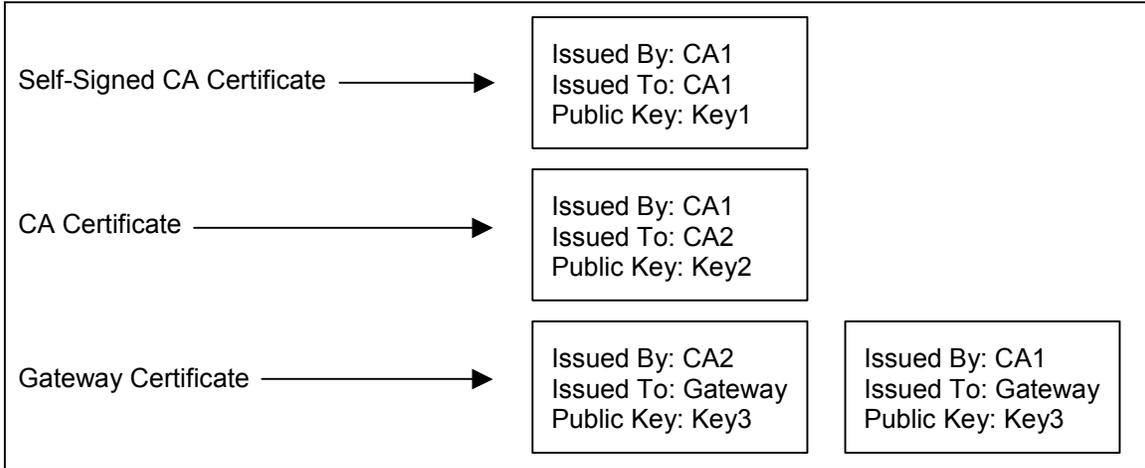


Figure 5: G2G Certificate Types

528. **Self-signed CA certificates:** – These certificates act as the trust anchors for each of the Nation's Gateways. They are generated by the National Gateway PKI's Root CA. As described in paragraph 507 they are exchanged between each Nation's gateway and are used by each Nation's gateway during digital signature verification. The private key corresponding to the public key in the certificate is used to generate the signature on the self-signed CA certificate and CA certificates.

529. **CA certificates:** – These certificates are issued by the CA with the self-signed CA certificate, and issue the Gateways' certificates. They are exchanged, as described in paragraph 509 and are used by each Nation's Gateway during digital signature verification.

530. **Gateway certificates:** – These certificates are either issued by self-signed CA certificates or by an intermediate CA. They are used by the National Gateways to verify digitally signed messages from the other National Gateways. The private key corresponding to the public key in the certificate is used to generate the digital signatures on messages.

Public Key Certificate Profiles[G2]

531. The "profile" contained within this document is considered to be compliant to RFC 3280. There following are additional constraints for National gateways:

- Processing version is restricted to Version 3 public key certificates. National Gateways only issue Version 3 certificates; therefore, it is unnecessary to support processing additional values for version and the corresponding differences between the certificates.

- Processing the following fields and extensions is technically required:
 - The *issuerUniqueIdentifier* and *subjectUniqueIdentifier* fields; however, Nations are not populating this field therefore there is no harm in not processing these fields.
 - The *subjectAltName* extension; however, Nations are placing a Distinguished Name (DN) in the *subject* field, are not required to populate the *subjectAltName* extension, and therefore there is no harm in not processing this field.
 - The *inhibitAnyPolicy* extension; however, Nations are not populating this extension therefore there is no harm in not processing these fields. Support for this extension is determined bilaterally.
- Processing the *authorityKeyIdentifier* and *subjectKeyIdentifier* extensions is required.
- Marking *keyUsage* as critical.
- Generating *authorityInfoAccess* is mandatory conditional on support for *cRLDistributionPoints*. Processing of *authorityInfoAccess* is determined bilaterally.

532. The following two paragraphs describe specific implementation details for public key certificate fields and extensions used to intercommunicate in this environment. CA implementation guidance is provided for generating each field and extension and Relying Party (RP) implementation guidance is also provided for processing each field and extension. The fields described in 533 are included in all certificates, while inclusion of the extension in 534 varies depending on the "type" of certificate. Annex A provides a detailed profile for the different certificates.

Public Key Certificate Fields

533. Public Key Certificate Fields are as follows:

- a. All certificates used within this environment shall indicate Version 3 (v3) by including the integer value of two (2) in the version field. RPs shall support processing this field, but they need only recognize Version 3 certificates.
- b. CAs shall include the certificate's *serialNumber* field in every certificate and it shall be a positive integer that is shorter than 20 octets and unique for a particular CA. This may be accomplished by the CAs maintaining and incrementing a counter to assign certificate serial numbers. RPs shall support processing this field.
- c. The **AlgorithmIdentifier** in the **signature** field shall include the OID as per Table 5-2 of the signature algorithm used to sign the certificate. Inclusion of the parameters is as per Table 5-1. The values included in this **AlgorithmIdentifier** field must be identical to those in the **AlgorithmIdentifier** field in paragraph k,

below. RPs shall support processing this field, but are minimally required to support value as specified in paragraph 544; however, additional values may be agreed bilaterally. RPs shall support processing this field; however, the parameters themselves are not used during signature verification.

- d. The issuer's **Name** in the **issuer** field shall contain the unique X.500 DN identifying the issuer. CAs and RPs are required to support the following standard naming attribute types: country, organization, organizational-unit, distinguished name qualifier, state or province name, common name, and serial number.
- e. The certificate validity period field contains two dates: **notBefore** and **notAfter**. Both the dates shall be expressed as Greenwich Mean Time (GMT) (Zulu). Both **notBefore** and **notAfter** may be encoded as either Coordinated Universal Time (**UTCTime**) or **GeneralizedTime**.³ Dates through the year 2049 shall be encoded as **UTCTime**, and dates in 2050 or later shall be encoded as **GeneralizedTime**. **UTCTime** shall include a two-digit year, two-digit month, two-digit day, two-digit hours, two-digit minutes, and two-digit seconds terminated by a "Z" (i.e., YYMMDDHHMMSSZ). **GeneralizedTime** shall include a four-digit year, two-digit month, two-digit day, two-digit hours, two-digit minutes, and two-digit seconds terminated by a "Z" (i.e., YYYYMMDDHHMMSSZ). The **UTCTime** year value shall be interpreted as follows:
- If YY is equal to or greater than 50, the year shall be 19YY.
 - If YY is less than 50, the year shall be 20YY.
- f. The **Name** in the **subject** field shall contain the X.500 DN of the subject. CAs and RPs are required to support the following standard naming attribute types: country, organization, organizational-unit, distinguished name qualifier, state or province name, common name, and serial number. Unique subject names are accomplished through careful assignment by CAs, as there are few Gateways.
- g. The **subjectPublicKeyInfo** field shall contain the subject's public key. CAs and RPs are required to generate and processing, respectively, the sub-fields of **subjectPublicKeyInfo** as follows (see paragraph 543):
- **algorithmIdentifier** shall include the algorithm's parameters in self-signed CA certificates and may include the parameters in CA and EE certificates. If

³ The Distinguished Encoding Rules (DER) allow several methods for formatting **UTCTime** and **GeneralizedTime**. All implementations shall use the same format to minimize signature verification problems. To ensure that **UTCTime** and **GeneralizedTime** values are consistently formatted:

1. The "Z" format and shall always be employed; a time differential shall never be employed.
2. The seconds field (even when it is '00') shall be present.
3. **GeneralizedTime** values shall not include fractional seconds.

parameters are included in this field they shall be used during signature verification.

- **subjectPublicKey** shall include the subject's public key.
- h. The **issuerUniqueIdentifier** field should not be generated within certificates used within the CMDE. No use for this field has been envisioned.
 - i. The **subjectUniqueIdentifier** should not be generated within certificates used in the CMDE. No use for the field has been envisioned.
 - j. The extension field shall be generated. See section 534 for a description of certificate extensions.
 - k. The issuer's signature shall be contained in the fields produced with the SIGNED Macro. The OID of the signature algorithm used to generate the signature shall also be included and must match the value present in paragraph c, above. Inclusion of the parameters is as per Table 5-1. However, these parameters shall not be used to verify signatures.

Public Key Certificate Extensions

534. Public Key Certificate Extensions are as follows:
- a. The **authorityKeyIdentifier** extension shall be included in Gateway and CA certificates to indicate which of the issuer's keys was used to sign the subject's certificate. It is optional in self-signed CA certificates. The **keyIdentifier** choice shall be used as the identifier method. Various methods exist for creating the value; however, the value in field is not regenerated by RP applications therefore CAs may either derived the value from the key or a method that generates a unique value be used. RPs shall support processing this extension.
 - b. The **subjectKeyIdentifier** extension shall be included in all certificates. The **keyIdentifier** shall be generated as specified above. RPs shall support processing this extension.
 - c. The **keyUsage** extension shall be included in EE and CA certificates, and it shall be marked as a critical extension. This extension constrains the keying material in the certificate to a specific purpose. CA certificates shall minimally have the **keyCertSign** bit set and may also have the **cRLSign**, **digitalSignature**, and **nonRepudiation** bit set. In EE certificates, the **digitalSignature** and **nonRepudiation** bits may both be set or not, but at least one of the bits must be set. Additionally, EE certificates may also have the **cRLSign** bit set. **keyEncipherment**, **dataEncipherment**, and **keyAgreement** shall not be set in either EE or CA certificates. There is no requirement on **encipherOnly** and **decipherOnly**. RPs shall support processing this extension.
 - d. The **extKeyUsage** extension is optional. This extension is optional because the envisioned uses for the key in the CMDE are encompassed by the **keyUsage** extension. RPs shall support processing this extension.

- e. The *privateKeyUsagePeriod* extension is optional. If the CA supports generation of this extension, then it may be included in signature certificates, but it should be included only where the CA stipulates a private key validity period. This extension is optional in the CMDE because validity periods for public and private keys are identical for both keys. RPs may support processing this extension.
- f. The *certificatePolicies* extension shall be included in EE and CA certificates and marked as non-critical. This extension is optional in self-signed CA certificates. The OIDs, as determined by National policy, for the applicable certificate policies shall be included in the *CertPolicyId* fields. Support for the *policyQualifiers* field is optional. RPs shall support processing this extension.
- g. The *policyMapping* extension is optional. If it is included it shall not be marked as a critical extension. This extension is not applicable to EE signature certificates (i.e., EE certificates) as per X.509 clause 12.2.2.7. RPs may support processing this extension.
- h. The *subjectAltName* extension is optional. If the CA generates it, it should not be generated as a critical extension. This extension should only be included when the CA chooses to stipulate use of alternate names. This extension must be included in a CRL issuer's certificate if the certificate was issued with a *cRLDistributionPoint* extension that includes *distributionPoint* or *cRLIssuer* field with a *uniformResourceIdentifier* name form. The only CCEB agreed name form is the X.500 DN contained in the *subject* field; therefore, this extension is not required for interoperability. RPs shall support processing this extension.
- i. The *issuerAltName* extension is optional. If the CA supports it, it shall never be generated as a critical extension. This extension should only be included when the CA chooses to stipulate use of alternate names. The only CCEB agreed name form is the X.500 DN contained in the subject field; therefore, this extension is not required for interoperability. RPs may support processing this extension.
- j. The *subjectDirectoryAttributes* extension is optional. If a CA supports generating this extension, it should be with the understanding that the attributes contained within the extension will likely be ignored by certificate-processing applications. RPs may support processing this extension.
- k. The *basicConstraints* extension shall be included in all CA certificates and it shall be marked critical except in self-signed CA certificates. Although processing of this extension in a "trusted" certificate is not required in the CMDE, there exists the possibility that some certificate chain processing developers may write their applications to require every certificate in a chain, including the "trusted" certificate (possibly a self-signed certificate), to assert that they are CAs in a basic constraints extension. For this reason, this extension shall be included in self-signed CA certificates. The *cA* BOOLEAN flag shall be set to true in the CA and self-signed CA certificates. The extension is optional in EE certificates; however,

- if a EE certificate has *keyUsage* as critical and *keyCertSign* not set, then the EE certificate should not be confused with a CA certificate (i.e., a certificate signed by an EE with a critical *keyUsage* extension and *keyCertSign* not set should be rejected as a CA certificate). RPs shall support processing this extension.
- l. The *nameConstraints* extension is optional in CA certificates. This extension may be used to restrict the names of subjects to a well-controlled name space. Values for *permittedSubtrees* and *excludedSubtrees* shall be included as required. *base* shall always be specified, *minimum* is always set to the default zero (0), and *maximum* is always omitted. The *base GeneralName* choice shall always be *directoryName*. When specifying a restriction of the form *directoryName*, the name restrictions shall use the same encoding as defined in paragraph 533.f for the *subject* field. RPs shall support processing this extension.
 - m. The *policyConstraints* extension is optional in CA certificates. The extension may be used by PKI entities to restrict the permissible policies that a certificate can be used for. If included in a CA certificate this shall include at least one *requireExplicitPolicy* or *inhibitPolicyMapping*. RPs shall support processing this extension.
 - n. The *cRLDistributionPoints* extension is optional. Nations may indicate the location of a CRL issued by an entity other than the issuing CA in *distributionPoint* using either *directoryName* or *uniformResourceIdentifier*. The name of the entity issuing the *distributionPoint* CRL is included in the *cRLIssuer* field. If the *distributionPoint* is present, then *cRLIssuer*, if present, must be a *directoryName* or *uniformResourceIdentifier*. If *distributionPoint* is not present and the *cRLIssuer* is present then the *cRLIssuer* must either be a *directoryName* or *uniformResourceIdentifier*. At minimum revocations for *reasons* of *keyCompromise* and *cACompromise* should be indicated. Although the standard allows this extension to be either critical or non-critical, it must never be generated as critical within the CMDE. RPs may support processing this extension.
 - o. The *authorityInfoAccess* extension shall be included in certificates if the *cRLDistributionPoints* extension is also included in the certificate (i.e., if the *cRLDistributionPoints* extension is included in a certificate, then the *authorityInfoAccess* extension must also be included) otherwise it is optional. Support for this extension by RPs is determined on a bi-lateral basis.
 - p. The *inhibitAnyPolicy* extension is supported in CA certificates on a bi-lateral basis.
 - q. The *subjectInfoAccess* extension is supported on a bi-lateral basis.
 - r. The *freshestCRL* extension is supported on a bi-lateral basis.

Public Key Certificate Checking

535. Section 6 of RFC 3280 specifies a procedure for performing certification path verification. An implementation shall be functionally equivalent to the external behaviour resulting from that procedure. The algorithm used by a particular implementation to derive the correct outputs from the given inputs is not standardized herein.

Certificate Revocation Lists

Certificate Revocation List Profiles

536. This section specifies the Version 2 (V2) X.509 Certificate Revocation List (CRL) as described in Recommendation X.509 (1997) and profiled in RFC 3280. One "type" of CRL is needed to support the G2G architecture. The "profile" contained within this document is considered to be compliant to RFC 3280 and is identical to the NATO CRL profile. The following are the additional constraints:

- All CAs are required to generate CRLs, as it is the agreed revocation mechanism for National Gateways.
- RFC 3280 requires the ability to process *version 1* CRLs; however, testing of this support is unnecessary, as all CRLs issued by CA supporting the G2G architecture will be issuing *version 2* CRLs.
- Processing *issuerAltName* is determined bilaterally. Inclusion of this extension is dependant on the CRL being pointed to by a *cRLDistributionPoint* extension in a certificate and as support for *cRLDistributionPoint* is not mandated by this profile then support is not required for interoperability.

537. The following two paragraphs describe specific implementation details for CRLs fields and extensions used to intercommunicate in this environment. CA implementation guidance is provided for generating each field and extension and Relying Party (RP) implementation guidance is also provided for processing each field and extension. The fields described in paragraph 538 and 540 are included in all CRLs, while inclusion of the extension in paragraph 539 varies depending on the "type" of certificate. Annex B provides a detailed CRL profile.

Certificate Revocation List Fields

538. CRL fields are as follows:

- a. CRLs created for use within this environment are based on the 1997 version of the X.509 standard. *version* shall have a value of 2.
- b. The *AlgorithmIdentifier* in issuer's *signature* field shall include the OID as per Table 5-2 of the signature algorithm used to sign the CRL. Inclusion of the parameters is as per paragraph 544. The values included in this

- AlgorithmIdentifier* field must be identical to those in the *AlgorithmIdentifier* field in paragraph h, below. RPs shall support processing this field, but are minimally required to support value as specified in paragraph 544; however, additional values may be agreed bilaterally. RPs shall support processing this field, however, the parameters themselves are not used during signature verification.
- c. The issuer's *Name* in the *issuer* field shall contain the unique X.500 DN identifying the issuer of the CRL. CAs and RPs are required to support the following standard naming attribute types: country, organization, organizational-unit, distinguished name qualifier, state or province name, common name, and serial number.
- d. CAs and RPs shall support the *thisUpdate* field. The CRL *thisUpdate* field contains one date that shall be expressed as Greenwich Mean Time (GMT) (Zulu). *thisUpdate* may be encoded as either Coordinated Universal Time (*UTCTime*) or *GeneralizedTime*.⁴ Dates through the year 2049 shall be encoded as *UTCTime*, and dates in 2050 or later shall be encoded as *GeneralizedTime*. *UTCTime* shall include a two-digit year, two-digit month, two-digit day, two-digit hours, two-digit minutes, and two-digit seconds terminated by a "Z" (i.e., YYMMDDHHMMSSZ). *GeneralizedTime* shall include a four-digit year, two-digit month, two-digit day, two-digit hours, two-digit minutes, and two-digit seconds terminated by a "Z" (i.e., YYYYMMDDHHMMSSZ). The *UTCTime* year value shall be interpreted as follows:
- If YY is equal to or greater than 50, the year shall be 19YY.
 - If YY is less than 50, the year shall be 20YY.
- e. CAs and RPs shall support the *nextUpdate* field. The CRL *nextUpdate* field contains one date that shall be expressed as Greenwich Mean Time (GMT) (Zulu). *nextUpdate* may be encoded as either Coordinated Universal Time (*UTCTime*) or *GeneralizedTime*.⁴ Dates through the year 2049 shall be encoded as *UTCTime*, and dates in 2050 or later shall be encoded as *GeneralizedTime*. *UTCTime* shall include a two-digit year, two-digit month, two-digit day, two-digit hours, two-digit minutes, and two-digit seconds terminated by a "Z" (i.e., YYMMDDHHMMSSZ). *GeneralizedTime* shall include a four-digit year, two-digit month, two-digit day, two-digit hours, two-digit minutes, and two-digit

⁴ The Distinguished Encoding Rules (DER) allow several methods for formatting *UTCTime* and *GeneralizedTime*. All implementations shall use the same format to minimize signature verification problems. To ensure that *UTCTime* and *GeneralizedTime* values are consistently formatted:

1. The "Z" format and shall always be employed; a time differential shall never be employed.
2. The seconds field (even when it is '00') shall be present.
3. *GeneralizedTime* values shall not include fractional seconds.

seconds terminated by a "Z" (i.e., YYYYMMDDHHMMSSZ). The *UTCTime* year value shall be interpreted as follows:

- If YY is equal to or greater than 50, the year shall be 19YY.
 - If YY is less than 50, the year shall be 20YY.
- f. CAs and RPs shall support the *revokedCertificates* field. The *revokedCertificates* field shall contain a sequence of revoked certificates, when the CA has revoked certificates. If the CA has no revoked certificate, but must generate a CRL, then the *revokedCertificates* will be omitted. The structure of this list shall be a sequence of certificate serial numbers, a *revocationDate*, and optional *crlEntryExtensions* (see paragraph 539). The revocation date expressed as Greenwich Mean Time (GMT) (Zulu), field may be encoded as either Coordinated Universal Time (*UTCTime*) or *GeneralizedTime*.⁴ Dates through the year 2049 shall be encoded as *UTCTime*, and dates in 2050 or later shall be encoded as *GeneralizedTime*. *UTCTime* shall include a two-digit year, two-digit month, two-digit day, two-digit hours, two-digit minutes, and two-digit seconds terminated by a "Z" (i.e., YYMMDDHHMMSSZ). *GeneralizedTime* shall include a four-digit year, two-digit month, two-digit day, two-digit hours, two-digit minutes, and two-digit seconds terminated by a "Z" (i.e., YYYYMMDDHHMMSSZ). The *UTCTime* year value shall be interpreted as follows:
- If YY is equal to or greater than 50, the year shall be 19YY.
 - If YY is less than 50, the year shall be 20YY.
- g. The *crlExtensions* shall be generated as specified in paragraph 540.
- h. The *issuer's signature* shall be contained in the fields produced with the SIGNED Macro. The OID of the signature algorithm used to generate the signature shall also be included. Inclusion of the parameters is as per paragraph 544. However, these parameters shall not be used to verify signatures.

Certificate Revocation List Entry Extensions

539. Certificate Revocation List Entry Extensions are:

- a. The *reasonCode* extension is optional for both processing and generating in a CRL entry. The following reasons for revocation shall be indicated if this extension is supported: *unspecified*, *keyCompromise*, *cACompromise*, *affiliationChanged*, *superseded*, and *cessationOfOperation*. Each entry on a *distributionPoint* may indicate whether the certificate was revoked for *keyCompromise* or *cACompromise*.
- b. The *instructionCode* extension is optional for both processing and generating in a CRL entry. Placing certificates on hold will not be recognized across

international boundaries. Implementations checking CRLs are only concerned with whether a certificate is on the CRL or not.

- c. The *invalidityDate* extension is optional for both processing and generating in a CRL entry. The invalidity date will not be recognized across international boundaries. Implementations checking the CRL are only concerned with whether a certificate is on the CRL not when the user may have considered the certificate invalid.
- d. The *certificateIssuer* extension is optional for processing and generating in a CRL entry. It shall be included in distribution point entries and it shall be marked as critical. The name form shall be *directoryName* and it shall be equal to the *issuer* field of the revoked certificate. This entry extension is optional in full CRLs (i.e., an authority does need to generate this extension in a CRL if it revokes all of its own certificates and no other authority's certificates.)

Certificate Revocation List Extensions

540. CRL Extensions are as follows:

- a. The **authorityKeyIdentifier** extension shall be included in CRLs to indicate which of the issuer's keys was used to sign the CRL. The **keyIdentifier** field shall be used to identify the key. The identifier shall be constructed as described in paragraph 534 a, which describes the certificate's **authorityKeyIdentifier** extension. All RPs shall support processing this extension.
- b. The *issuerAltName* extension is optional for both processing and generating. It shall never be generated as a critical CRL extension. It must be included with a *uniformResourceIdentifier* name form in a distribution point CRL if the distribution point CRL was identified in the *cRLDistributionPoint* extension with the *uniformResourceIdentifier* name form. The only CCEB agreed name form is the X.500 DN contained in the *issuer* field; therefore, this extension is not required for interoperability.
- c. The *cRLNumber* extension shall always be included in CRLs. CRLs issued by Nations will include all certificates and updated at time specified in the *nextUpdate* field; therefore, this extension is not required for interoperability purposes. However, for interoperability with the Internet Public Key Infrastructure (IPKI) profile (defined in RFC 3280) all CRLs shall include this extension and all RPs shall support processing this extension.
- d. The *issuingDistributionPoint* extension is optional for both processing and generating. It shall always be included in CRLs issued by an entity other than the certificate issuer. This extension shall always be marked as critical. The *distributionPoint* field may indicate alternative name forms of the *distributionPoint* using either the *directoryName* or *uniformResourceIdentifier* name form. This *issuingDistributionPoint* extension may also indicate the CRL does not *onlyContainsUserCerts* and *onlyContainsCACerts* (i.e., use the default

- values); indicate *onlySomeReasons* of *keyCompromise* and *cACompromise*; and set *indirectCRL* to true if some revoked certificates in CRLs are issued by an entity other than the certificate issuer, and to false otherwise. This extension shall be absent in the full CRLs (i.e., an authority does need to generate this extension in a CRL if it revokes all of its own certificates and no other authority's certificates.)
- e. The *deltaCRLIndicator* extension is optional for both processing and generating. CRLs that contain this critical CRL extension will be rejected by national infrastructures that do not support this extension. Use of this extension is discouraged due the large interoperability concerns. CRLs issued by Nations will include all revoked certificates; therefore, this extension is not required for interoperability purposes.
 - f. The *freshestCRL* extension is supported on a bi-lateral basis and shall only point to a delta CRL.

Certificate Revocation List Checking

541. Section 6 of RFC 3280 specifies a procedure for performing certification path verification, which includes verification of CRLs. An implementation shall be functionally equivalent to the external behaviour resulting from that procedure. The algorithm used by a particular implementation to derive the correct outputs from the given inputs is not standardized herein.

Cryptography

542. This section specifies algorithm information which must be consistent and interoperable between the National Gateways. The goals of this section are to:

- Capture implementation details, design choices, and standard references for the algorithms used in the G2G () Architecture;
- Specify standards documents, OIDs, and implementation details (as required) for other Government and commercial algorithms.

543. At the application layer, currently only two algorithms are required to enable the agreed security services: a hash algorithm and a digital signature algorithm. Specific information for the agreed hashing, Secure Hash Algorithm (SHA-1), and digital signature algorithms, Digital Signature Algorithm (DSA) and RSA Algorithm⁵, are included herein. Implementations are to support **generating one and support verifying both, as per RFC 3270.**

⁵ Note that there are two versions of the RSA Algorithm commonly referred to as the X9 version and PKCS v1.5. The version included herein is the PKCS v1.5 certificate.

Hash

544. SHA –1 is the approved hashing algorithm.

Draft

Specification	<p>FIPS PUB 180-1, Secure Hash Standard</p> <p>17 April 1995</p> <p>NIST</p>
OID	<p>iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) SHA-1(26)</p> <p>1.3.14.3.2.26</p> <p>PARAMETER NULL</p> <p>NIST OSI Implementers Workshop, Security Special Interest Group</p> <p>Stable Implementation Agreements: Part 12 - OS Security, June 1995</p> <p>NULL parameters shall never be present when an id-sha1 Algorithm Identifier is encoded.</p> <p>(future) X9.57, Appendix C</p>
Block size	512-bits, 64-bytes
Hash value size	160-bits, 20-bytes
Padding	<p>512-bits, 64-bytes</p> <p>A message has length $l < 2^{64}$. Before it is input to the SHA-1, the message is padded on the right as follows:</p> <ol style="list-style-type: none"> a. "1" is appended. Example: if the original message is "01010000", this is padded to "010100001". b. "0"s are appended. The number of "0"s will depend on the original length of the message. The last 64-bits of the last 512-bit block are reserved for the length l of the original message. c. Obtain the 2-word representation of l, the number of bits in the original message. If $l < 2^{32}$ then the first word is all zeroes. Append these two words to the padded message. <p>The padded message will contain $16 * n$ words for some $n > 0$. The padded message is regarded as a sequence of n blocks $M(1), M(2), \dots, M(n)$, where each $M(i)$ contains 16 words and $M(1)$ contains the first characters (or bits) of the message.</p>

Table 5-1: Hashing Algorithm

Digital Signature

DSA with SHA-1

<p>Specification</p>	<p>FIPS PUB 186, Digital Signature Standard 19 May 1994 NIST</p>
<p>OID</p>	<p>iso(1) member-body(2) us(840) x9-57(10040) x9algorithm(4) id-dsa-with-sha1(3) 1.2.840.10040.4.3 PARAMETER NULL American National Standard X9.57-199x Public Key Cryptography for the Financial Services Industry: Certificate Management 21 June 1996 NULL parameters shall never be present when an id-dsa-with-sha1 Algorithm Identifier is encoded. (future) X9.57, Appendix C</p>
<p>ASN.1 encoding</p>	<p>For the DSA, the contents octets of the signature BIT STRING shall be interpreted as being the DER encoding of the type: DSAsigvalue ::= SEQUENCE { r INTEGER s INTEGER} That is, the encoding of the sequence is wrapped inside a BIT STRING American National Standard X9.57-199x Public Key Cryptography for the Financial Services Industry: Certificate Management 21 June 1996</p>

Table 5-2: Algorithm

<p>OID</p>	<p>iso(1) member-body(2) us(840) x9-57(10040) x9algorithm(4) Id-dsa(1) 1.2.840.10040.4.1 DSAParameters ::= SEQUENCE{ prime1 INTEGER, -- modulus p prime2 INTEGER, -- modulus q base INTEGER -- base/generator g} American National Standard X9.57-199x Public Key Cryptography for the Financial Services Industry: Certificate Management 21 June 1996</p>
<p>Subject Public Key</p>	<p>DSAPublicKey ::= INTEGER -- public key y A DSAPublicKey y (an INTEGER) is converted to a subjectPublicKey BIT STRING in the obvious way: The most significant bit of y becomes the most significant bit of the BIT STRING so that the least significant bit of y becomes the least significant bit of the BIT STRING. American National Standard X9.57-199x Public Key Cryptography for the Financial Services Industry: Certificate Management 21 June 1996</p>
<p>Subject Public Key Length</p>	<p>The key shall be at least 1024 bits in length.</p>
<p>Key Usage Bits</p>	<p>digitalSignature May be true nonRepudiation May be true keyEncipherment Must not be true dataEncipherment Must not be true keyAgreement Must not be true keyCertSign May be true cRLSignMay be true enciperOnly No requirement decipherOnly No requirement</p>

Table 5-3: Certificate

545. The *AlgorithmIdentifier* field of *subjectPublicKeyInfo* is the only place in CCEB CMI compliant V3 X.509 certificates in which algorithm parameters will be present. CAs shall not populate the parameters in the signature field of the base certificate or in the SIGNED macro in the certificates or the CRLs.

546. If the DSA algorithm parameters are absent from the subject's DSA X.509 certificate, then the certificate issuer's DSA parameters apply. This inheritance strategy for certificate chain validation is documented in Annex A of this document.

Parameters

547. The DSA algorithms have optional parameters associated with their syntax, and are usually referred to as *p*, *q*, and *g*. The *AlgorithmIdentifier* field of *subjectPublicKeyInfo* is the only place in CCEB compliant V3 X.509 certificates in which algorithm parameters will be present. If the DSA algorithm parameters are absent from the subject's DSA X.509 certificate, then the certificate issuer's DSA parameters apply. This strategy validates certificate chains in which all certificates were generated in accordance with the inheritance strategy. The validation strategy will fail validation for certificate chains containing certificates that were generated by certification authorities that did not implement this inheritance strategy.

548. CAs may populate the parameters in the signature field of the base certificate or in the SIGNED macro in the certificates or the CRLs, but the values will be ignored.

549. Signatures in a chain of certificates shall be verified using the algorithm OID and parameters contained in two state variables: *algorithm*, and *parameters*. In addition, each application may optionally maintain a list of algorithm OIDs it recognizes as synonymous, *synonyms()*. Synonymous OIDs refer to the same cryptographic algorithm and the same parameter syntax.

550. It is an application-specific choice of how to maintain synonym lists. For example, they could be hard-coded arrays, or tables retrieved dynamically from configuration files.

551. The following rules describe how these state variables shall be determined and processed during certification path validation:

- The algorithm state variable and parameters state variable will be initialised to trusted values. These values could come from hard-coded values or configuration information. However, they are typically taken from the **algorithm** and **parameters**, of the **subjectPublicKeyInfo AlgorithmIdentifier** field in a trusted public key certificate. (This would be the first certificate in a path, and the signature on such a trusted certificate is not verified.)
- If the algorithm state variable is ever "null", signature verification fails. If the parameters state variable is ever "null" when the algorithm state variable contains an algorithm that requires the use of parameters for signature verification, then

signature verification fails. (If signature verification fails, the certificate path fails validation, and an alternate path should be sought.)

- For each certificate, the values in the *signature* field and in the *SIGNED* macro must be equal to *algorithm*, or an element of *synonyms(algorithm)*. If not, the certificate path fails validation (and an alternate path should be sought).
- If parameters are populated in a certificate's *signature* field or *SIGNED* macro fields, they must be verified to be identical to the *parameters* state variable. If a certificate is encountered which has parameters in the *signature* field or the *SIGNED* macro which are not identical to the *parameters* state variable, then the certificate is rejected, (and the certificate path fails validation, and an alternate path should be sought).
- If the *algorithm* state variable does not match the value of *algorithm* in the ***subjectPublicKeyInfo*** field of the certificate, or any *synonyms(algorithm)*, the *parameters* state variable will be set to "null". Additionally, the ***algorithm*** state variable will be set to equal the algorithm identifier in the ***subjectPublicKeyInfo*** field of the certificate.
- If the ***subjectPublicKeyInfo*** field of the certificate contains public key parameters, the *parameters* state variable will be set to equal the parameters of the ***subjectPublicKeyInfo*** field of the certificate. The process will be repeated from step 2 onward until the last certificate in the chain is validated.

RSA with SHA-1 (PKCS #1 version)

Specification	<p>PKCS #1 RSA Encryption Standard Version 1.5, 1 November 1993</p> <p>and</p> <p>FIPS PUB 180-1, Secure Hash Standard 17 April 1995 NIST</p>
OID	TBD
Hash Encapsulation	<p>A block type <i>BT</i>, a padding string <i>PS</i>, and the data <i>D</i> shall be formatted into an octet string <i>EB</i>, the encryption block.</p> <p style="text-align: center;">  $EB = 00 \parallel BT \parallel PS \parallel 00 \parallel D .$ </p> <p>The block type <i>BT</i> shall be a single octet -- value 01. The padding string <i>PS</i> shall consist of $k-3-\ D\$ octets -- they shall have value FF</p> <p>PKCS #1 RSA Encryption Standard Version 1.5, 1 November 1993</p>
ASN.1 encoding	<p>AN RSA signature (an INTEGER) is conveyed in a BIT STRING in the obvious way: the most significant bit of the INTEGER becomes the most significant bit of the BIT STRING, and the least significant bit of the INTEGER becomes the least significant bit of the BIT STRING.</p> <p>ISO/TC68/SC2/WG8 1997-08-18 ISO/WD-15782 Banking - Certificate Management</p>
Specification	<p>American National Standard X9.31-1997 Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA) July 28 1997</p> <p>and</p> <p>FIPS PUB 180-1, Secure Hash Standard 17 April 1995 NIST</p>
OID	<p>iso(1) identified-organization(3) oiw(14) secsig(3) algorithm(2) sha1WithRSASignature(29)</p>

	<p>1.3.14.3.2.29</p> <p>PARAMETER NULL</p> <p>NIST OSI Implementers Workshop, Security Special Interest Group Stable Implementation Agreements: Part 12 - OS Security, June 1995</p>
<p>Hash Encapsulation</p>	<p>HEADER PADDING H(M) TRAILER</p> <p>The Header is a fixed length nibble -- hexadecimal value x'6'</p> <p>The Padding is a variable length field, consisting of the string of hexadecimal nibbles x'B' and where the rightmost nibble is always the hexadecimal value x'A'.</p> <p>The Trailer is a fixed length field of two bytes -- hexadecimal value x'33CC'</p> <p>American National Standard X9.31-1997 Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA) July 28 1997</p>
<p>ASN.1 encoding</p>	<p>AN RSA signature (an INTEGER) is conveyed in a BIT STRING in the obvious way: the most significant bit of the INTEGER becomes the most significant bit of the BIT STRING, and the least significant bit of the INTEGER becomes the least significant bit of the BIT STRING.</p> <p>ISO/TC68/SC2/WG8 1997-08-18 ISO/WD-15782 Banking - Certificate Management</p>

Table 5-4: Algorithm

<p>OID</p>	<p>iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1) 1.2.840.113549.1.1.1</p> <p>PARAMETER NULL</p> <p>PKCS #1 RSA Encryption Standard Version 1.5, 1 November 1993</p>
<p>Subject Public Key</p>	<pre>RSAPublicKey ::= SEQUENCE { modulus INTEGER, -- called n publicExponent INTEGER } -- called e</pre> <p>PKCS #1 RSA Encryption Standard Version 1.5, 1 November 1993</p>
<p>Subject Public Key Length</p>	<p>The key shall be at least 1024 bits in length.</p>
<p>Key Usage Bits</p>	<p>digitalSignature May be true nonRepudiation May be true keyEncipherment Must not be true dataEncipherment Must not be true keyAgreement Must not be true keyCertSign May be true cRLSign May be true encipherOnly No requirement decipherOnly No requirement</p>

Table 5-5: Certificate

Compromised Key Lists

552. Compromised Key Lists will not be used between nations.

Labelling

553. Labelling is based on the X.841 standard modified as below. In the CCEB context the only common labelling concepts are the hierarchical classifications, unclassified, confidential, secret, top secret, and indication that the message is releasable to another nation. There are markings that are exchanged on a bilateral basis that will need to be supported by National Gateways. Bilateral agreements ensure that Nation A's

markings are properly conveyed in Nation B's label, and vice versa. Values for the fields will be determined by National policy.

554. There is no requirement to use the label for routing.
555. The P772 header security label will not be supported between nations.
556. National Gateways will generate a message security label and place it into the S/MIME v3 ESS SecurityLabel attribute as described in the following paragraphs.
557. Any security label that cannot be interpreted or is unmarked will be assigned the highest classification of the receiving system and will not be marked as releasable outside that system.

Security Label⁶

558. The basic label format used is the ESS security label defined in RFC 2634 *Enhanced Security Services for S/MIME* (<http://www.ietf.org/rfc/rfc2634.txt>). Note that segments of ASN.1 are repeated only for illustration, and are not formally defined by this standard.

```
ESSSecurityLabel ::= SET {
    security-policy-identifier    SecurityPolicyIdentifier,
    security-classification SecurityClassification OPTIONAL,
    privacy-mark    ESSPrivacyMark OPTIONAL,
    security-categories    SecurityCategories OPTIONAL }
```

Security Policy Identifier

559. The security-policy-identifier is an object identifier (OID) registered Nationally that uniquely identifies the National security policy. This OID will be created for the security policy, and registered by the National Security Object Registrar.

560. SecurityPolicyIdentifier ::= OBJECT IDENTIFIER

Security Classification

561. The integer corresponding to the sensitivity of the data object will be entered into the security-classification field in the label. Values, other than those defined below and unmarked, will be agreed on a bi-lateral basis. The named values below will be used for the classifications defined in ACP 123 clause 247.

⁶ Each nation recognizes other nations security labels and associated handling requirements on a bilateral basis. The semantics of the security label will be determined by the relevant security policy under which the label was generated. The labeling policy could be a common policy such as NATO or CCEB, or could be left to nations to use their own. The mechanism for this is outside the scope of this document.

```
SecurityClassification ::= INTEGER {
    unmarked (0),
    unclassified (1),
    restricted (2),
    confidential (3),
    secret (4),
    top-secret (5) } (0..ub-integer-options)
```

```
ub-integer-options INTEGER ::= 256
```

Privacy Mark

562. There is no plan for CCEB Nations to use the privacy-mark field. However, National systems may encounter the PrintableString "CLEAR" to represent the ACP 123 Clear Service in this field.

```
ESSPrivacyMark ::= CHOICE {
    pString      PrintableString (SIZE(1..ub-privacy-mark-length)),
    utf8String   UTF8String (SIZE(1..MAX))}
```

```
ub-privacy-mark-length INTEGER ::= 128 -- as defined in X.411
```

Security Categories

563. The security-categories field in National security label contains the encoding of the security categories in a marking. It will be a combination of integers and bit strings. The following defines the abstract syntax of the security categories to be used by CCEB Nations.

Implicit Tags

564. Refer to Annex 3

ANNEX A TO CHAPTER FIVE

PICS PROFORMA FOR SIGNATURE CERTIFICATES

Signature Certificate Introduction

A 1. This appendix provides the Profile for the Signature Certificates (self-signed CA, CA, and end entities) for use in this environment. The structure for the Certificate is defined in the 1997 version of ITU-T X.509 | ISO/IEC 9594-8.

A 2. The supplier of an implementation that claims to conform to ITU-T Rec. X.509 | ISO/IEC IS 9594-8 is required to complete a copy of the PICS Proforma provided in Sections A.1 through A.5 and is required to provide information necessary to identify both the supplier and the implementation.

Description of Tables

A 3. The “Item” and “Notes” columns are provided for cross-referencing. The numbers in the “Item” column are the row numbers. The numbers in the “Notes” column indicate the table numbers followed by the “item” number enclosed in parentheses. These two columns are used together to point to sub-elements. The “Notes” column also refers to additional information supplied in the last row of the table.

A 4. The “Protocol Elements” column refers to the name of ASN.1 fields taken from the X.500 recommendations.

A 5. In each table, the “Base” column reflects the level of support required for conformance to the base standard⁷. The level of support refers to the support classification for the “Base” column. The “Base” column is broken into “Proc.” (i.e., processing) and “Gen.” (i.e., generation) columns. The “Proc.” column reflects the level of support required by compliant certificate processing and using entities who process certificates. The “Gen.” column reflects the level of support required in compliant signature certificates (i.e., the information that is included in the certificate). The types of signature certificates include: (i.e., self-signed CA (see A.2), CA (see A.3), and end-entities (see A.5). When the CA acts as an End Entity (e.g., when a CA verifies the signature on a message), then the “Proc.” column applies.⁸

A 6. The “Support” column is provided for completion by the supplier of the implementation as follows:

⁷ If the CCEB defined a certificate extension, field, or attribute not in the base standard (i.e., X.509), the classification for the “Base” column is –.

⁸ “Proc.” columns in the PAA, PCA, CA, External Domain, and EE certificate tables are identical.

- Y the protocol element is fully supported (i.e., supporting the requirements of the m support classification)
- N the protocol element is not fully supported, further qualified to indicate the action taken on receipt of such an element as follows:
ND - the element is discarded/ignored
NR - the PDU is rejected
- – or blank the protocol element is not applicable

Support Classifications

A 7. Each of the protocol elements listed in section A.2⁹, A.3, A.4, and A.5 are designated as having a support requirement of mandatory or optional. Where protocol elements are nested (i.e., the elements contain sub-elements), the requirement to support the nested element is relevant only when the immediately containing (parent) element is supported.

A 8. To specify the support level of the protocol elements, the following terminology is defined.

Static Capability

A 9. The following classifications are used to specify static conformance (i.e., capability).

- **mandatory support (m):** Implementations claiming to create certificates shall be able to generate the protocol element. Implementations claiming to process certificates shall be able to receive the protocol elements and perform all associated procedures (i.e., implying the ability to handle both the syntax and the semantics of the element) as relevant.
- **optional (o):** Implementations claiming to create certificates are not required to support generation of the protocol element. If support is claimed, the element shall be treated as if it were specified as mandatory support, and the sub-elements, if present, shall be supported as specified. Implementations claiming to perform processing of certificates shall ignore the protocol element and continue processing of the certificate.
- **conditional (c):** Implementations shall support the protocol element under the conditions specified. If the conditions are met, the protocol element shall be treated as if it were specified as mandatory support. If these conditions are not

⁹ (U) Implementation of clause A.2 is dependent on National policy. Formatting the trusted public key as a self-signed certificate is dependent on National policy (see clause 2.4 of the CMI Authentication Framework).

met, the protocol element shall be treated as if it were specified as optional support (unless otherwise stated).

- **not applicable (-)** : This element is not applicable in the particular context in which this classification is used.

Dynamic Capability

A 10. The following classifications are used to specify dynamic conformance (i.e., behaviour).

- **required (r)**: The information for this protocol element must be populated upon certificate generation.

Identification of the implementation

Item	Question	Response
1	Date of statement (DD/MM/YYYY)	
2	PICS serial number	
3	System conformance statement cross reference	

Table 5 A-1: Identification of PICS

Item	Question	Response
1	Implementation name	
2	Implementation version	
3	Machine name	
4	Machine version	
5	Operating system name	
6	Operating system version	
7	Special configuration	
8	Other information	

Table 5-6: Identification of Implementation and/or system

Item	Question	Response
1	Organization name	
2	Contact name(s)	
3	Address	
4	Telephone number	
5	Telex number	
6	Fax number	
7	E-mail address	
8	Other information	

Table 5-7: Identification of system supplier and/or test laboratory client

Item	Question	Response
1	Title, reference number and date of publication of the standard	
2	CRL Version Number	

Table 5-8: Identification of the CRL

Item	Question	Response	Comments
1	Are all mandatory base standards requirements implemented?		Note 1
<p>Note 1: Answering “No” to this section indicates non-conformance to the information object specification. Unsupported mandatory capabilities are to be identified in the IO-ICS, with an explanation of why the implementation is non-conformant. Such information shall be provided in A.8, “Other information”.</p>			

Table 5-9: Global statement of conformance

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	signed	m	m	m	mr			
2	toBeSigned	m	m	m	mr			
3	version	m	m	m	mr			
4	serialNumber	m	m	m	mr			
5	signature	m	m	m	mr			See Table 5-11 Note 2
6	issuer	m	m	m	mr			See ACP 133
7	validity	m	m	m	mr			
8	notBefore	m	m	m	mr			See Table 5-55 (1)
9	notAfter	m	m	m	mr			See Table 5-55 (1)
10	subject	m	m	m	mr			See ACP 133
11	subjectPublicKeyInfo	m	m	m	mr			
12	algorithm	m	m	m	mr			See Table 5-11
13	subjectPublicKey	m	m	m	mr			
14	issuerUniqueIdentifier	o	o	m	o			
15	subjectUniqueIdentifier	o	o	m	o			
16	extensions	o	o	m	mr			See Table 5-12
17	algorithmIdentifier	m	m	m	mr			See Note 2
18	encrypted	m	m	m	mr			

Note 2: Population of the “parameter” sub-field is not recommended, as the values in this field will be ignored (see [paragraph ?](#)).

Table 5-10: Self-Signed CA Signature Certificate

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	algorithm	m	m	m	mr			
2	parameters	m	m	m	mr			Note 3

Note 3: The parameters p, q and g shall be present in the self-signed CA certificate (see [paragraph ?](#)).

Table 5-11: Algorithm Identifier

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	extnID	m	m	m	mr			Note 4
2	critical	m	m	m	mr			d(false)
3	extnValue	m	m	m	mr			

Note 4: The support requirements for self-signed CA certificate extensions are listed in A.2.2.1.

Table 5-12: Extensions

Draft

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen	Proc.	Gen.	Proc.	Gen.	
1	authorityKeyIdentifier	o	o	m	o			See Table 5-14
2	subjectKeyIdentifier	o	o	m	mr			
3	keyUsage	o	o	m	o			See Table 5-15
4	extKeyUsage	o	o	m	o			
5	privateKeyUsagePeriod	o	o	o	o			See Table 5-16
6	certificatePolicies	o	o	m	o			See Table 5-17
7	policyMappings	o	o	o	o			See Table 5-18
8	subjectAltName	o	o	m	o			See Table 5-55 (1), Note 5
9	issuerAltName	o	o	o	o			See Table 5-55 (1), Note 5
10	subjectDirectoryAttributes	o	o	o	o			
11	basicConstraints	o	o	m	mr			See Table 5-19 Note 6
12	nameConstraints	o	o	m	o			See Table 5-20
13	policyConstraints	o	o	m	o			See Table 5-22
14	cRLDistributionPoints	o	o	o	o			See Table 5-23 Note 5
15	authorityInfoAccess	o	o	c1	c2			See Table 5-24
16	inhibitAnyPolicy	o	o	c1	c1			
17	subjectInfoAccess	o	o	c1	c1			
18	freshestCRL	o	o	c1	c1			
<p>c1: Support for this extension is determined on a bilateral basis.</p> <p>c2: If cRLDistributionPoints is included in the certificate then m, else o.</p> <p>Note 5: Although the standard allows this extension to be either critical or non-critical, it must never be generated as critical within this environment</p> <p>Note 6: This extension must not be generated as critical in self-signed CA certificates.</p>								

Table 5-13: Standard Extensions

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	keyIdentifier	c3	c3	m	mr			Note 7
2	certIssuer	c4	c4	o	o			
3	certSerialNumber	c4	c4	o	o			

c3: If certIssuer or certSerialNumber is not supported then m, else o.
c4: If keyIdentifier field is not supported then m, else o.
Note 7: The authorityKeyIdentifier shall carry the KMID in keyIdentifier.

Table 5-14: Authority Key Identifier

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	digitalSignature	o	o	m	m			Note 8
2	nonRepudiation	o	o	m	m			Note 8
3	keyEncipherment	o	o	–	–			
4	dataEncipherment	o	o	–	–			
5	keyAgreement	o	o	–	–			
6	keyCertSign	o	o	m	mr			
7	cRLSign	o	o	m	m			Note 8
8	encipherOnly	o	o	–	–			
9	decipherOnly	o	o	–	–			

Note 8: Procedures for setting this bit are in clause 1.1.2.c.

Table 5-15: Key Usage

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	notBefore	m	c5	m	c5			
2	notAfter	m	c5	m	c5			

c5: Support for at least one of the components is m.

Table 5-16: Private Key Usage Period

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	policyIdentifier	m	m	m	mr			
2	policyQualifiers	o	o	m	o			
3	policyQualifierId	m	m	m	mr			
4	qualifier	o	o	m	o			

Table 5-17: Certificate Policies

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	issuerDomainPolicy	m	m	mr	mr			
2	subjectDomainPolicy	m	m	mr	mr			

Table 5-18: Policy Mappings

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	cA	m	m	m	mr			d(false)
2	pathLenConstraint	m	o	m	o			

Table 5-19: Basic Constraints

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	permittedSubtrees	m	o	m	mr			See Table 5-21
2	excludedSubtrees	m	o	m	m			See Table 5-21

Table 5-20: Name Constraints

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	base	m	m	m	mr			See Table 5-55 (5)
2	minimum	m	m	m	mr			d(0)
3	maximum	m	o	m	m			

Table 5-21: General Subtrees

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	requireExplicitPolicy	m	o	m	o			
2	inhibitPolicyMapping	m	o	m	o			

Table 5-22: Policy Constraints

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	distributionPoint	o	o	m	m			See Table 5-55 (17)
2	reasons	o	o	m	m			See Table 5-55 (20)
3	cRLIssuer	o	o	m	m			See Table 5-55 (4)

Table 5-23: CRL Distribution Points

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	accessMethod	o	o	m	m			Note 9
2	accessLocation	o	o	m	m			Note 9

Note 9: See clause 4.2.2.1 of RFC 3280 for support requirements for id-ad-calssuers.

Table 5-24: Authority Information Access

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	signed	m	m	m	mr			
2	toBeSigned	m	m	m	mr			
3	version	m	m	m	mr			
4	serialNumber	m	m	m	mr			
5	signature	m	m	m	mr			See Table 5-26, Note 10
6	issuer	m	m	m	mr			See ACP 133
7	validity	m	m	m	mr			
8	notBefore	m	m	m	mr			See Table 5-55 (1)
9	notAfter	m	m	m	mr			See Table 5-55 (1)
10	subject	m	m	m	mr			See ACP 133
11	subjectPublicKeyInfo	m	m	m	mr			
12	algorithm	m	m	m	mr			See Table 5-26
13	subjectPublicKey	m	m	m	mr			
14	issuerUniqueIdentifier	o	o	m	o			
15	subjectUniqueIdentifier	o	o	m	o			
16	extensions	o	o	m	mr			See Table 5-27
17	algorithmIdentifier	m	m	m	mr			See Table 5-26, Note 10
18	encrypted	m	m	m	mr			

Note 10: Population of the "parameter" sub-field is not recommended, as the values in this field will be ignored (see [paragraph 2](#)).

Table 5-25: CA Signature Certificate

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	algorithm	m	m	m	mr			
2	parameters	m	m	m	m			Note 11

Note 11: The parameters p, q and g should be present in the CA certificates (see [paragraph ?](#)).

Table 5-26: Algorithm Identifier

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	extnID	m	m	M	mr			Note 12
2	critical	m	m	M	mr			d(false)
3	extnValue	m	m	M	mr			

Note 12: The support requirements for CA certificate extensions are listed in A.3.2.1.

Table 5-27: Extensions

Draft

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	authorityKeyIdentifier	o	o	M	mr			See Table 5-29
2	subjectKeyIdentifier	o	o	M	mr			
3	keyUsage	o	o	M	mr			See Table 5-30, Note 13
4	extKeyUsage	o	o	M	o			
5	privateKeyUsagePeriod	o	o	O	o			See Table 5-31
6	certificatePolicies	o	o	M	mr			See Table 5-32
7	policyMappings	o	o	O	o			See Table 5-33
8	subjectAltName	o	o	M	c6			See Table 5-55 (1), Note 14
9	issuerAltName	o	o	O	o			See Table 5-55 (1), Note 22
10	subjectDirectoryAttributes	o	o	O	o			See Table 5-34
11	basicConstraints	o	o	M	mr			See Table 5-34, Note 13
12	nameConstraints	o	o	M	o			See Table 5-35
13	policyConstraints	o	o	M	o			See Table 5-37
14	cRLDistributionPoints	o	o	O	o			See Table 5-38 Note 14
15	authorityInfoAccess	o	o	c7	c8			See Table 5-39
16	inhibitAnyPolicy	o	o	c7	c7			
17	subjectInfoAccess	o	o	c7	c7			
18	freshestCRL	o	o	c7	c7			See Table 5-38

c6: If the CA issues certificates that include the cRLDistributionPoint extension's field distributionPoint with a uniformResourceIdentifier name form then support is mr, else o.

c7: Support for this extension is determined on a bilateral basis.

c8: If cRLDistributionPoints is included in the certificate then m, else o.

Note 13: This extension shall be critical.

Note 14: Although the standard allows this extension to be either critical or non-critical, it must never be generated as critical within this environment.

Table 5-28: Standard Extensions

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	keyIdentifier	c9	c9	M	mr			Note 15
2	certIssuer	c10	c10	O	o			
3	certSerialNumber	c10	c10	O	o			

c9: If certIssuer or certSerialNumber is not supported then m, else o.

c10: If keyIdentifier field is not supported then m, else o.

Note 15: The authorityKeyIdentifier shall carry the KMID in keyIdentifier.

Table 5-29: Authority Key Identifier

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	digitalSignature	o	o	M	m			Note 16
2	nonRepudiation	o	o	M	m			Note 16
3	keyEncipherment	o	o	–	–			
4	dataEncipherment	o	o	–	–			
5	keyAgreement	o	o	–	–			
6	keyCertSign	o	o	M	mr			
7	cRLSign	o	o	M	m			Note 16
8	encipherOnly	o	o	–	–			
9	decipherOnly	o	o	–	–			

Note 16: Procedures for setting this bit are in clause 1.1.2.c.

Table 5-30: Key Usage

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	notBefore	m	c11	M	c11			
2	notAfter	m	c11	M	c11			

c11: Support for at least one of the components is m.

Table 5-31: Private Key Usage Period

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	policyIdentifier	m	m	m	mr			
2	policyQualifiers	o	o	m	o			
3	policyQualifierId	m	m	m	mr			
4	qualifier	o	o	m	o			

Table 5-32: Certificate Policies

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	issuerDomainPolicy	m	m	m	mr			
2	subjectDomainPolicy	m	m	m	mr			

Table 5-33: Policy Mappings

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	cA	m	m	m	mr			d(false)
2	pathLenConstraint	m	o	m	o			

Table 5-34: Basic Constraints

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	permittedSubtrees	m	o	m	mr			See Table 5-36
2	excludedSubtrees	m	o	m	m			See Table 5-36

Table 5-35: Name Constraints

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	base	m	m	m	mr			See Table 5-55 (5)
2	minimum	m	m	m	mr			d(0)
3	maximum	m	o	m	o			

Table 5-36: General Subtrees

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	requireExplicitPolicy	m	o	m	o			
2	inhibitPolicyMapping	m	o	m	o			

Table 5-37: Policy Constraints

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	distributionPoint	o	o	m	m			See Table 5-55 (17)
2	reasons	o	o	m	m			See Table 5-55 (20)
3	cRLIssuer	o	o	m	m			See Table 5-55 (4)

Table 5-38: CRL Distribution Points

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	accessMethod	o	o	m	m			Note 17
2	accessLocation	o	o	m	m			Note 17

Note 17: See clause 4.2.2.1 of RFC 3280 for support requirements for id-ad-calssuers.

Table 5-39: Authority Information Access

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	signed	m	m	mr	mr			
2	toBeSigned	m	m	mr	mr			
3	version	m	m	mr	mr			
4	serialNumber	m	m	mr	mr			
5	signature	m	m	mr	mr			See Table 5-41, Note 18
6	issuer	m	m	mr	mr			See ACP 133
7	validity	m	m	mr	mr			
8	notBefore	m	m	mr	mr			See Table 5-55 (1)
9	notAfter	m	m	mr	mr			See Table 5-55 (1)
10	subject	m	m	mr	mr			See ACP 133
11	subjectPublicKeyInfo	m	m	mr	mr			
12	algorithm	m	m	mr	mr			See Table 5-41
13	subjectPublicKey	m	m	mr	mr			
14	issuerUniqueIdentifier	o	o	m	o			
15	subjectUniqueIdentifier	o	o	m	o			
16	extensions	o	o	mr	mr			See Table 5-42
17	algorithmIdentifier	m	m	mr	mr			See Table 5-41, Note 18
18	encrypted	m	m	mr	mr			

Note 18: Population of the “parameter” sub-field is not recommended, as the values in this field will be ignored (see paragraph ?).

Table 5-40: Gateway Signature Certificate

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	algorithm	m	m	m	mr			
2	parameters	m	m	m	m			Note 19

Note 19: The parameters p, q and g should be present in the Gateway certificates (see paragraph ?).

Table 5-41: Algorithm Identifier

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	extnID	m	m	M	m			Note 20
2	critical	m	m	M	m			d(false)
3	extnValue	m	m	M	m			

Note 20: The support requirements for Gateway certificate extensions are listed in A.4.2.1.

Table 5-42: Extensions

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	authorityKeyIdentifier	o	o	M	mr			See Table 5-44
2	subjectKeyIdentifier	o	o	M	mr			
3	keyUsage	o	o	M	mr			See Table 5-45, Note 21
4	extKeyUsage	o	o	M	o			
5	privateKeyUsagePeriod	o	o	O	o			See Table 5-46
6	certificatePolicies	o	o	M	mr			See Table 5-47
7	policyMappings	o	o	O	–			See Table 5-48
8	subjectAltName	o	o	M	o			See Table 5-55 (1), Note 22
9	issuerAltName	o	o	O	o			See Table 5-55 (1), Note 2
10	subjectDirectoryAttributes	o	o	O	o			
11	basicConstraints	o	o	M	o			See Table 5-49
12	nameConstraints	o	o	M	–			See Table 5-50
13	policyConstraints	o	o	M	–			See Table 5-52
14	cRLDistributionPoints	o	o	O	o			See Table 5-53, Note 21
15	authorityInfoAccess	o	o	c12	c13			See Table 5-54
16	inhibitAnyPolicy	o	o	c12	–			
17	subjectInfoAccess	o	o	c12	c12			
18	freshestCRL	o	o	c12	c12			See Table 5-53

c12: Support for this extension is on a bilateral basis.
 C13: If cRLDistributionPoints is included in the certificate then m, else o.
 Note 21: This extension shall be indicated as critical.
 Note 22: Although the standard allows this extension to be either critical or non-critical, it must never be generated as critical within this environment.

Table 5-43: Standard Extensions

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	keyIdentifier	c14	c14	Mr	mr			Note 23
2	certIssuer	c15	c15	O	o			
3	certSerialNumber	c15	c15	O	o			

c14: If certIssuer or certSerialNumber is not supported then m, else o.
c15: If keyIdentifier field is not supported then m, else o.
Note 23: The authorityKeyIdentifier shall carry the KMID in keyIdentifier.

Table 5-44: Authority Key Identifier

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	digitalSignature	o	o	M	m			Note 24
2	nonRepudiation	o	o	M	m			Note 24
3	keyEncipherment	o	o	–	–			
4	dataEncipherment	o	o	–	–			
5	keyAgreement	o	o	–	–			
6	keyCertSign	o	o	M	–			
7	cRLSign	o	o	M	o			Note 24
8	encipherOnly	o	o	–	–			
9	decipherOnly	o	o	–	–			

Note 24: Procedures for setting this bit are in clause 1.1.2.c.

Table 5-45: Key Usage

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	notBefore	m	c16	M	c16			
2	notAfter	m	c16	M	c16			

c16: Support for at least one of the components is m.

Table 5-46: Private Key Usage Period

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	policyIdentifier	m	m	M	mr			
2	policyQualifiers	o	o	M	o			
3	policyQualifierId	m	m	M	mr			
4	qualifier	o	o	M	o			

Table 5-47: Certificate Policies

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	issuerDomainPolicy	m	m	M	–			
2	subjectDomainPolicy	m	m	M	–			

Table 5-48: Policy Mappings

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	cA	m	m	M	mr			d(false)
2	pathLenConstraint	m	o	M	o			

Table 5-49: Basic Constraints

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	permittedSubtrees	m	o	M	–			See Table 5-51
2	excludedSubtrees	m	o	M	–			See Table 5-51

Table 5-50: Name Constraints

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	base	m	m	M	–			See Table 5-55 (5)
2	minimum	m	m	M	–			d(0)
3	maximum	m	o	M	–			

Table 5-51: General Subtrees

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	requireExplicitPolicy	m	o	M	–			
2	inhibitPolicyMapping	m	o	M	–			

Table 5-52: Policy Constraints

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	distributionPoint	o	o	M	m			See Table 5-69 (17)
2	reasons	o	o	M	m			See Table 5-69 (20)
3	cRLIssuer	o	o	M	m			See Table 5-69 (4)

Table 5-53: CRL Distribution Points

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	accessMethod	o	o	M	m			Note 25
2	accessLocation	o	o	M	m			Note 25

Note 25: See clause 4.2.2.1 of RFC 3280 for support requirements for id-ad-calssuers.

Table 5-54: Authority Information Access

Draft

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	Time							
2	UTCTime	m	m	m	c17			
3	GeneralizedTime	o	o	m	c18			
4	GeneralNames							
5	GeneralName	m	m	m	m			
6	otherName	o	o	o	o			
7	rfc822Name	o	o	m	c19			Note 26
8	dNSName	o	o	o	o			Note 26
9	x400Address	o	o	o	o			See ACP 123
10	directoryName	o	o	m	m			See ACP 133
11	ediPartyName	o	o	o	o			
12	nameAssigner	o	o	o	o			
13	partyName	o	o	o	m			
14	uniformResourceIdentifier	o	o	m	m			Note 26
15	iPAddress	o	o	o	o			Note 26
16	registeredID	o	o	o	o			
17	DistributionPointName							
18	fullName	m	m	m	m			See (4)
19	nameRelativeToCRLIssuer	m	m	m	m			See ACP 133
20	ReasonFlags							
21	unused	o	o	o	o			
22	keyCompromise	o	o	m	m			
23	cACompromise	o	o	m	m			
24	affiliationChange	o	o	m	o			
25	superseded	o	o	m	o			
26	cessationOfOperation	o	o	m	o			
27	certificateHold	o	o	m	o			

c17: If the date is before 2050 mr, else -.

c18: If the date is after 2049 mr, else -.

c19: If the e-mail address is included in the certificate then m, else o (see paragraph 4.1.2.6 of RFC 3280).

Note 26: See clause 4.2.1.7 of RFC 3280 for name formation rules.

Table 5-55: Common Fields

APPENDIX B TO CHAP 5

PICS PROFORMA FOR CERTIFICATE REVOCATION LISTS

CRL Introduction

B 1. This appendix provides the Profile for the Certificate Revocation List (CRL) for use in this environment. The structure for the CRL is defined in the 1997 version of ITU-T X.509 | ISO/IEC 9594-8.

B 2. The supplier of an implementation that claims to conform to ITU-T Rec. X.509 | ISO/IEC IS 9594-8 is required to complete a copy of the PICS Proforma provided in Sections B.1 through B.3 and is required to provide information necessary to identify both the supplier and the implementation.

Description of Tables

B 3. The “Item” and “Notes” columns are provided for cross-referencing. The numbers in the “Item” column are the row numbers. The numbers in the “Notes” column indicate the table numbers followed by the “item” number enclosed in parentheses. These two columns are used together to point to sub-elements. The “Notes” column also refers to additional information supplied in the last row of the table.

B 4. The “Protocol Elements” column refers to the name of ASN.1 fields taken from the X.500 recommendations.

B 5. In each table, the “Base” column reflects the level of support required for conformance to the base standard. The level of support refers to the support classification for the “Base” column. The “Base” column is broken into “Proc.” (i.e., processing) and “Gen.” (i.e., generation) columns. The “Proc.” column reflects the level of support required by compliant certificate processing and using entities who process CRLs. The “Gen.” column reflects the level of support required in compliant CRLs (i.e., the information that is included in the CRL). When the CA acts as an End Entity (e.g., when a CA receives a message), then the “Proc.” column applies.

B 6. The “Support” column is provided for completion by the supplier of the implementation as follows:

Y	the protocol element is fully supported (i.e., supporting the requirements of the m support classification)
N	the protocol element is not fully supported, further qualified to indicate the action taken on receipt of such an element as follows: ND - the element is discarded/ignored NR - the PDU is rejected
– or blank	the protocol element is not applicable

Support Classifications

B 7. Each of the protocol elements listed in section B.2 and B.3 are designated as having a support requirement of mandatory or optional. Where protocol elements are nested (i.e., the elements contain sub-elements), the requirement to support the nested element is relevant only when the immediately containing (parent) element is supported.

B 8. To specify the support level of the protocol elements, the following terminology is defined.

Static Capability

B 9. The following classifications are used to specify static conformance (i.e., capability).

B 10. **mandatory support (m)** : Implementations claiming to create certificates shall be able to generate the protocol element. Implementations claiming to process certificates shall be able to receive the protocol elements and perform all associated procedures (i.e., implying the ability to handle both the syntax and the semantics of the element) as relevant.

B 11. **optional (o)** : Implementations claiming to create certificates are not required to support generation of the protocol element. If support is claimed, the element shall be treated as if it were specified as mandatory support, and the sub-elements, if present, shall be supported as specified. Implementations claiming to perform processing of certificates shall ignore the protocol element and continue processing of the certificate.

B 12. **conditional (c)** : Implementations shall support the protocol element under the conditions specified. If the conditions are met, the protocol element shall be treated as if it were specified as mandatory support. If these conditions are not met, the protocol element shall be treated as if it were specified as optional support (unless otherwise stated).

B 13. **not applicable (-)** : This element is not applicable in the particular context in which this classification is used.

Dynamic Capability

B 14. The following classifications are used to specify dynamic conformance (i.e., behaviour).

B 15. **required (r)** : The information for this protocol element must be populated upon certificate generation.

Identification of the implementation

Item	Question	Response
1	Date of statement (DD/MM/YYYY)	
2	PICS serial number	
3	System conformance statement cross reference	

Table 5-56: Identification of PICS

Item	Question	Response
1	Implementation name	
2	Implementation version	
3	Machine name	
4	Machine version	
5	Operating system name	
6	Operating system version	
7	Special configuration	
8	Other information	

Table 5-57: Identification of Implementation and/or system

Item	Question	Response
1	Organization name	
2	Contact name(s)	
3	Address	
4	Telephone number	
5	Telex number	
6	Fax number	
7	E-mail address	
8	Other information	

Table 5-58: Identification of system supplier and/or test laboratory client

Item	Question	Response
1	Title, reference number and date of publication of the standard	
2	CRL Version Number	

Table 5-59: Identification of the CRL

Item	Question	Response	Comments
1	Are all mandatory base standards requirements implemented?		Note 1
Note 1: Answering “No” to this section indicates non-conformance to the information object specification. Unsupported mandatory capabilities are to be identified in the IO-ICS, with an explanation of why the implementation is non-conformant. Such information shall be provided in A.8, “Other information”.			

Table 5-60: Global statement of conformance

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	signed	m	m	m	mr			
2	toBeSigned	m	m	m	mr			
3	version	o	o	m	mr			
4	signature	m	m	m	mr			See Table 5-62, Note 2
5	issuer	m	m	m	mr			See ACP 133
6	thisUpdate	m	m	m	mr			See Table 5-69 (1)
7	nextUpdate	o	o	m	mr			See Table 5-69 (1)
8	revokedCertificates	o	o	m	m			
9	userCertificates	m	m	m	mr			
10	revocationDate	m	m	m	mr			See Table 5-69 (1)
11	crEntryExtensions	o	o	m	m			See Table 5-67
12	crExtensions	o	o	m	mr			See Table 5-63
13	algorithmIdentifier	m	m	m	mr			See Table 5-62, Note 2
14	encrypted	m	m	m	mr			
Note 2: Population of the “parameter” sub-field is not recommended, as the values in this field will be ignored (see paragraph 2).								

Table 5-61: CRL

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	algorithm	m	m	m	mr			
2	parameters	m	m	m	m			

Table 5-62: Algorithm Identifier

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	extnID	m	m	m	mr			Note 3
2	critical	m	m	m	mr			d(false)
3	extnValue	m	m	m	mr			

Note 3: The CRL extensions are listed in B.2.2.1; and the CRL entry extensions are listed in B.2.2.2.

Table 5-63: Extensions

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	authorityKeyIdentifier	o	o	m	mr			See Table 5-65
2	issuerAltName	o	o	c1	c2			See Table 5-69 (4)
3	cRLNumber	o	o	m	mr			
4	issuingDistributionPoint	o	o	o	o			See Table 5-66, Note 4
5	deltaCRLIndicator	o	o	o	o			

c1: Support for processing this extension is determined on a bilateral basis.
c2: If the CRL's issuer is identified in a certificate with a cRLDistributionPoint extension's cRLIssuer field with a uniformResourceIdentifier name then support is mr, else o.
Note 4: This extension shall be indicated as critical.

Table 5-64: CRL Extensions

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	keyIdentifier	c3	c4	m	mr			
2	certIssuer	c4	c4	o	o			
3	certSerialNumber	c4	c4	o	o			

c3: If certIssuer or certSerialNumber is not supported then m, else o.
c4: If keyIdentifier field is not supported then m, else o.

Table 5-65: Authority Key Identifier

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	distributionPoint	o	o	M	m			See Table 5-69 (17)
2	onlyContainsUserCerts	o	o	M	m			d(false)
3	onlyContainsCACerts	o	o	M	m			d(false)
4	onlySomeReasons	o	o	M	m			See Table 5-69 (20)
5	indirectCRL	o	o	M	m			d(false)

Table 5-66: Issuing Distribution Point

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	reasonCode	o	o	O	o			See Table 5-68
2	instructionCode	o	o	O	o			
3	invalidityDate	o	o	O	o			
4	certificateIssuer	o	o	O	o			See Table 5-69 (4), Note 5

Note 5: This extension shall be indicated as critical.

Table 5-67: CRL Entry Extensions

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	unspecified	o	o	M	m			
2	keyCompromise	o	o	M	m			
3	cACompromise	o	o	M	m			
4	affiliationChanged	o	o	M	m			
5	superseded	o	o	M	m			
6	cessationOfOperation	o	o	M	m			
7	certificateHold	o	o	M	o			
8	removeFromCRL	o	o	O	o			

Table 5-68: Reason Code

Item	Protocol Element	Base		Profile		Support		Notes
		Proc.	Gen.	Proc.	Gen.	Proc.	Gen.	
1	Time							
2	UTCTime	m	m	M	c5			
3	GeneralizedTime	o	o	M	c6			
4	GeneralNames							
5	GeneralName	m	m	M	m			
6	otherName	o	o	O	o			
7	rfc822Name	o	o	M	c7			Note 6
8	dNSName	o	o	O	o			Note 6
9	x400Address	o	o	O	o			See ACP 123
10	directoryName	o	o	M	m			See ACP 133
11	ediPartyName	o	o	O	o			
12	nameAssigner	o	o	O	o			
13	partyName	o	o	O	m			
14	uniformResourceIdentifier	o	o	M	m			Note 6
15	iPAddress	o	o	O	o			Note 6
16	registeredID	o	o	O	o			
17	DistributionPointName							
18	fullName	m	m	M	m			See (4)
19	nameRelativeToCRLIssuer	m	m	M	m			See ACP 133
20	ReasonFlags							
21	unused	o	o	O	o			
22	keyCompromise	o	o	M	m			
23	caCompromise	o	o	M	m			
24	affiliationChange	o	o	M	o			
25	superseded	o	o	M	o			
26	cessationOfOperation	o	o	M	o			
27	certificateHold	o	o	M	o			

c5: If the date is before 2050 m, else -.

c6: If the date is after 2049 m, else -.

c7: If the e-mail address is included in the certificate then m, else o (see paragraph 4.1.2.6 of RFC 3280).

Note 6: See clause 4.2.1.7 of RFC 3280 for name formation rules.

Table 5-69: Common Fields

ANNEX C TO CHAPTER FIVE

ASN.1 MODULE FOR SECURITY LABEL

```
NatoInformationSecurityLabelModule { joint-iso-ccitt (2) country (16) us (840) organization (1) u.s.
government (101) dod (2) infosec (1) modules (0) 20 }
```

```
DEFINITIONS IMPLICIT TAGS ::=
```

```
BEGIN
```

```
-- EXPORTS All; --
```

```
IMPORTS
```

```
-- Note: The definition of SecurityCategory and the SECURITY-CATEGORY macro are
-- formalized based on the note in RFC 2634. Productions of this macro are expressly for
-- use in the security-categories field of the ESSSecurityLabel.
```

```
SecurityCategory ::= SEQUENCE {
    type      [0] SECURITY-CATEGORY,
    value     [1] ANY DEFINED BY type }
```

```
SECURITY-CATEGORY MACRO ::=
```

```
BEGIN
```

```
    TYPE NOTATION ::= type | empty
```

```
    VALUE NOTATION ::= value (VALUE OBJECT IDENTIFIER)
```

```
END
```

```
-- Type 1 - restrictive attributes
```

```
restrictiveBitMap SECURITY-CATEGORY ::= {
    RestrictiveTag
    IDENTIFIED BY id-restrictiveAttributes }
```

```
RestrictiveTag ::= SEQUENCE {
    tagName      OBJECT IDENTIFIER,
    attributeFlags BIT STRING }
```

```
-- Type 2 - enumerated attributes
```

```
enumeratedAttributes SECURITY-CATEGORY ::= {
    EnumeratedTag
    IDENTIFIED BY id-enumeratedAttributes }
```

```
EnumeratedTag ::= SEQUENCE [
    tagName      OBJECT IDENTIFIER,
    attributeList SET OF SecurityAttribute }
```

-- Type 6 - release attributes

```
permissivebitMap SECURITY-CATEGORY ::= {
    PermissiveTag
    IDENTIFIED BY id-permissiveAttributes }
```

```
PermissiveTag ::= SEQUENCE
    tagName      OBJECT IDENTIFIER,
    attributeFlags BIT STRING }
```

```
SecurityAttribute ::= INTEGER (0..MAX)
```

-- Type 7 - informative attributes

```
informativeAttributes SECURITY-CATEGORY ::= {
    InformativeTag
    IDENTIFIED BY id-informativeAttributes }
```

```
FreeFormField ::= SEQUENCE {
    tagName      OBJECT IDENTIFIER,
    field        FreeFormField }
```

```
FreeFormField ::= CHOICE {
    bitSetAttributes BIT STRING,
    securityAttributes SET OF SecurityAttribute }
```

-- Object identifier assignment

```
id-infosec ID ::= { joint-iso-ccitt (2) country (2) us (840) organization (1) u.s. government (101) dod (2) 1 }
```

```
id-security-categories ID ::= { id-infosec 8 }
```

```
id-commonSecurityCategoriesSyntaxes ID ::= { id-security-categories 3 }
```

```
id-restrictiveAttributes ID ::= { id-commonSecurityCategoriesSyntaxes 0 }
```

```
id-enumeratedAttributes ID ::= { id-commonSecurityCategoriesSyntaxes 1 }
```

```
id-permissiveAttributes ID ::= { id-commonSecurityCategoriesSyntaxes 2 }
```

```
id-informativeAttributes ID ::= { id-commonSecurityCategoriesSyntaxes 3 }
```

END

C 1. In the following discussion, a *tag* is a data structure that contains some information preceded by some identifying parameters, such as type and length. A tag's *type* indicates how the data in the tag is to be processed or interpreted, e.g., whether or not an information control decision should be based on the data.

C 2. National security category values will consist of one or more of the four tag types defined above. The tag name identifies a registry entry where the tag and its associated semantics are defined. The security tags carry security attributes of the data being exchanged. These tag types are described in the following sections.

C 3. The *Restrictive Tag* is composed of a bit string. The bit string is used to convey a set of non-hierarchical attributes that apply to the labelled information. A bit is assigned to every security policy-defined restrictive attribute. Bits corresponding to restrictive attributes that apply will be set to 1. All other bits are set to 0. Security compartments are examples of markings that are appropriate for restrictive security attributes.

C 4. The *Enumerated Tag* is composed of one or more non-negative integers. Each non-negative integer represents a non-hierarchical attribute that applies to the labelled information. Use of the integer representation is intended to minimize label length in cases where only a few attributes out of a large set of attributes apply to the labelled information. Attributes enumerated by tags of this type could be restrictive (e.g., compartments) or permissive (e.g., release permissions).

C 5. The *Permissive Tag* is composed of a bit string. The bit string is used to convey a set of non-hierarchical attributes that apply to the labelled information. A bit is assigned to every security policy-defined permissive attribute. Bits corresponding to types or groups of entities that are granted access to the information are set to 1. All other bits are set to 0. Release markings and caveats are examples of markings appropriate for permissive security attributes.

C 6. The *Informative Tag* may be composed of either a bit string or a set of non-negative integers. Either form may be used to convey security attributes that are informative only, and are not considered for the purposes of access control. When the *Informative Tag* is composed of a bit string, the bit string is used to convey a set of non-hierarchical attributes that apply to the labelled information. A bit is assigned to every security policy-defined free-form attribute. Bits corresponding to free-form attributes that apply will be set to 1. All other bits are set to 0. When the *Informative Tag* is composed of non-negative integers, each non-negative integer represents a non-hierarchical attribute that applies to the labelled information. Use of the integer representation is intended to minimize label length in cases where only a few attributes out of a large set of attributes apply to the labelled information.

CHAPTER 6

IMPLEMENTATION TESTING

Overview

601. This chapter defines the high-level test strategy and planning requirements for G2G interoperability testing. The chapter will define the test levels, the expected outcomes and the national test schedules.

602. The chapter will not explicitly identify tests; instead it will set a benchmark for testing by identifying the types of tests and the expected outcomes for each test level. Test procedures and detailed test plans will be the multilateral responsibility of the nations participating in the test exercises. This chapter:

- describes the scope and objectives of the Messaging G2G testing;
- identifies the functional requirements and the features to be tested.

Objectives of G2G Testing

Test Items

603. The test strategy defines three functional test levels ranging from basic message interoperability testing to full multinational messaging. These test levels have been defined to allow testing to commence prior to the development and deployment of a G2G CMI architecture and directory service capabilities.

Core functionality

604. The test levels outlined in this chapter are based on the CCEB Interoperability model dated Mar 02. Existing national legacy ACP 127/128 and e-mail systems meet all agreed functionality up to and including level 2 of the model.

605. This document defines a series of tests that are associated with each of the agreed levels of the Interoperability test model within the context of ACP 145 that cover the G2G interoperability. The G2G test sets associated with each level of the interoperability model will confirm a gateway system's conformance to that level's defined functionality. The levels are defined as follows:

- Level 2 –Basic messaging (COTS e-Mail Services and Legacy Text Based Messaging Services)
- Level 3a – Military Messaging Services with Directory Services

- Level 3b – Military Messaging Services with Certificate Management Infrastructure¹⁰
- Level 4 – Integrity & Non-Repudiation Security Services - Full G2G messaging with Directory Services and Certificate Management Infrastructure

606. Level 2 testing will confirm that the ACP 123 G2G capability meets the existing messaging capabilities. Level 3a enhances level 2 testing with the inclusion of CMI but no directory (assumes that a working directory system may not be available). Similarly Level 3b enhances level 2 testing with directory services by no CMI (assumes that a CMI model may not be available at the time of testing). Level 4 testing will confirm that the ACP 123 gateway solutions meet all defined G2G requirements up to and including level 4 of the Interoperability Model.

607. For a detailed definition of the testing levels refer to Table XXX.

Operational Scenario

608. Operational test scenarios have not been defined. If and when operational scenarios are defined, test cases that exercise these scenarios will be defined. These test cases will be mapped into the test structure defined by the document.

Test Structure

Approach

609. The test levels defined in **Table xxx**? level of testing. For instance level 2 basic message testing calls a test procedure called “receiving a message”, which is a generic test. The test conditions that apply to this procedure require this test be repeated for messages containing various elements of service, various faults, and addressing conditions. This approach was selected for simplicity of presentation; this reduces the duplication of simple test procedures, while articulating the test requirements for a particular test level.

610. There is no expectation that this format need be reflected in other lower level testing documentation.

611. The test regime is structured to validate messaging interpretability between national ACP 145 messaging gateways. Each test level details the message traffic that will be passed between the gateways to confirm compliance with ACP 145 guidelines.

612. It is recommended that a nation undertaking gateway interoperability testing utilise a client/server system, that is indicative of the nations own message handling

¹⁰ Level 3A testing assumes that each nation has a working gateway system, but the allied directory architecture is not in place. It is assumed that the testers will manually install the other certificates into each nations gateway product. This testing does not preclude the nation using its own national directory system to support the gateway.

system, to send and receive messages to/from its border ACP 145 gateway. Validation of a gateway system is problematic if it is not tested in a situation that models the actual deployment scenario.

613. The test procedures are based on the assumption that the test messages are generated by an internal national client (could be a mailer) and sent to the national ACP 145 gateway for transportation into the ACP 145 environment. Similarly it is assumed that the ACP 145 will receive messages from the ACP 145 environment and route the message to internal mail client (could be an MTA).

Test INDEX

614. The Test Index is based on the functional requirements identifying individual test levels. The test levels are:

- Level 2 –Basic messaging (COTS e-Mail Services and Legacy Text Based Messaging Services)
- Level 3 B – Military Messaging Services with Certificate Management Infrastructure¹¹
- Level 3 A – Military Messaging Services with Directory Services
- Level 4 – Integrity & Non-Repudiation Security Services - Full G2G messaging with Directory Services and Certificate Management Infrastructure

Level 2 – Basic Messaging – Send/Receive ACP 123 messages	Reference
<p>Test conditions</p> <p>a) ACP 123 compliant messages, including</p> <ul style="list-style-type: none"> i. Valid CCEB formatted ACP 123, and ii. Invalid message format. <p>b) With and without attachments, including</p> <ul style="list-style-type: none"> i. Valid file types, ii. Invalid file types, iii. Virus infected files, iv. Size restrictions <p>c) Single and multiple addressees, including</p> <ul style="list-style-type: none"> i. Valid addresses, ii. Some/all invalid addresses, iii. Blind copy recipients, and iv. Mixed internal and external addresses. 	

¹¹ Level 3A testing assumes that each nation has a working gateway system, but the allied directory architecture is not in place. It is assumed that the testers will manually install the other certificates into each nations gateway product. This testing does not preclude the nation using its own national directory system to support the gateway.

<ul style="list-style-type: none"> d) Various precedences, <ul style="list-style-type: none"> i. Same/ different for primary and copy recipients, ii. Precedence time out. e) Notification, including <ul style="list-style-type: none"> i. No notifications, ii. Non- Delivery notifications, and iii. Delivery notifications. f) With and without distribution codes, and g) Alternative recipient. 	
L2-001	Send a message to from an Internal message client to an Allied message client.
L2-002	Receive a message to from an Allied message client.
L2-003	Replying to a message received from an Allied message client.
L2-004	Forwarding a message received from an Allied message client.
<insert new L2 test>	

Table 6-1: Level 2 Testing

Draft

Level 3A – Messaging with Certificate Management Infrastructure – Sending and Receiving an ACP 123 message		Reference
Test conditions (in addition to test cases defined in level 2 testing)		
a) ACP 123 compliant messages, including <ul style="list-style-type: none"> i. Signed and Non signed messages with valid and invalid signatures, ii. Various key lengths, and iii. Various algorithms. b) With and without attachments, including <ul style="list-style-type: none"> i. Various classifications using SMIME cryptographic labels, <ul style="list-style-type: none"> i. Correctly labelled for destination network, ii. Incorrectly labelled for destination network, and iii. With an invalid label. c) Various categories/caveats using SMIME v3 ESS cryptographic labels, <ul style="list-style-type: none"> f) Notification, including <ul style="list-style-type: none"> i. Signed receipts. 		
L3A-001	Send a message to from an Internal message client to an Allied message client.	
L3A-002	Receive a message to from an Allied message client.	
L3A-003	Replying to a message received from an Allied message client.	
L3A-004	Forwarding a message received from an Allied message client.	
<insert new L2A test>		

Table 6-2: Level 3A Testing

Level 3B – Messaging with Directory Services		Reference
Test conditions (in addition to test cases defined in level 2 testing)		
a. Mail lists, including (This test condition may not be relevant, depends on final implementation within ACP 145) <ul style="list-style-type: none"> i. Valid addresses, ii. Invalid addresses, iii. Exempted addressing iv. Mixed internal and external addresses, v. Mail list loops across national boundaries, vi. Mail list administration (add, modify and delete), b. Directory user interface, including <ul style="list-style-type: none"> i. Addressing using directory lookup, ii. Functional address searching. 		
L3B-001	Send a message to from an Internal message client to an Allied message client.	
L3B-002	Receive a message to from an Allied message client.	
L3B-003	Replying to a message received from an Allied message client.	
L3B-004	Forwarding a message received from an Allied message client.	
L3B-005	Directory searching and browsing for addresses.	
<insert new L3B test>		

Table 6-3: Level 3B Testing

Level 4 – Messaging with Certificate Management Infrastructure and Directory Services		Reference
Test conditions (in addition to test cases defined in level 2 , 3A and 3B testing)		
c. CRL distribution using the directory, including		
i. Single CRL, and		
ii. Multiple CRLs.		
d. Certificate distribution using the directory.		
L4-001	Send a message to from an Internal message client to an Allied message client.	
L4-002	Receive a message to from an Allied message client.	
L4-003	Replying to a message received from an Allied message client.	
L4-004	Forwarding a message received from an Allied message client.	
L4-005	Directory searching and browsing for addresses.	
L4-006	Publishing of national CMI certificates and configuration information into the in boarder Directory.	
<insert new L4 test>		

Table 6-4: Level 4 Testing

Accreditation:

615. This will reference the agreed process as specified in the WAN Security documentation. The WAN System security policy will be enhanced to cover additional issues associated with formal messaging G2G architecture.

Guards

616.

Intruder Detection

617.

Virus Protection

618.

Protocols

619.

Certificate Management

620.

Cryptography

621.

Labelling

622.

Authentication

623.

Draft

CHAPTER 8

STANDARDS AND REFERENCES

Reference	Title
ACP 123	
ACP 133	
X.400	
X.500	
X.841	

Draft

CHAPTER 9

LIST OF EFFECTIVE PAGES

Chapter 1
Chapter 2
Chapter 3
Chapter 4
Chapter 5
Chapter 6
Chapter 7
Chapter 8
Chapter 9

Draft