

UNCLASSIFIED

ACP 145(A)

**INTERIM IMPLEMENTATION GUIDE
FOR ACP 123/STANAG 4406
MESSAGING SERVICES BETWEEN
NATIONS**

ACP 145(A)



SEPTEMBER 2008

UNCLASSIFIED

Original

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(A), Interim Implementation Guide for ACP 123/STANAG 4406 Messaging Services Between Nations, is an UNCLASSIFIED CCEB publication.
3. The title of this document has been amended to harmonise with the NATO Military Messaging Strategy.
4. This publication contains Allied military information for official purposes only.
5. This ACP is to be maintained and amended in accordance with the provisions of the current version of ACP 198.

THE COMBINED COMMUNICATION-ELECTRONICS BOARD

LETTER OF PROMULGATION

FOR ACP 145(A)

1. The purpose of this Combined Communication Electronics Board (CCEB) Letter of Promulgation is to implement ACP 145(A) within the Armed Forces of the CCEB Nations. ACP 145(A), INTERIM IMPLEMENTATION GUIDE FOR ACP 123/STANAG 4406 MESSAGING SERVICES BETWEEN NATIONS, 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(A) is effective on receipt for CCEB Nations and when directed by NATO Military Committee (NAMILCOM) for NATO nations and Strategic Commands ACP 145(A) will supersede ACP 145, which shall be destroyed in accordance with national regulations. This ACP has been renamed from the original Gateway-to-Gateway Implementation Guide for ACP 123/STANAG 4406 Messaging Services.

EFFECTIVE STATUS

Publication	Effective for	Date	Authority
ACP 145(A)	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

JA STOTT
Lieutenant Commander, RN
CCEB Permanent Secretary

TABLE OF CONTENTS

TITLE PAGE

FOREWORD..... I

LETTER OF PROMULGATION..... II

RECORD OF MESSAGE CORRECTIONS III

TABLE OF CONTENTS IV

LIST OF FIGURES VIII

LIST OF TABLES VIII

CHAPTER 1 1-1

INTRODUCTION..... 1-1

 BACKGROUND 1-1

 PURPOSE OF THE DOCUMENT 1-1

 SCOPE OF THE DOCUMENT..... 1-1

CHAPTER 2..... 2-1

ARCHITECTURE 2-1

 GENERAL OVERVIEW..... 2-1

 GATEWAY 2-1

 NETWORK..... 2-2

 MESSAGING 2-2

 DIRECTORY..... 2-2

 SECURITY 2-2

CHAPTER 3..... 3-1

MESSAGING SERVICES 3-1

 MANAGEMENT SERVICES..... 3-1

 PROCEDURES..... 3-1

 NAMING AND ADDRESSING 3-1

 PRIORITY HANDLING 3-1

 NOTIFICATIONS 3-1

 P772 CONTENT..... 3-2

 AUDIT AND LOGGING 3-2

 ADDRESS LIST (AL) EXPANSION 3-3

 GATEWAY HANDLING POLICY 3-3

TRANSPORT ENVELOPE..... 3-3
APPROVED P772 CONTENT..... 3-3
ATTACHMENTS..... 3-3
ATTACHMENTS PROHIBITED..... 3-3
ATTACHMENTS ALLOWED - THE MINIMUM SET..... 3-4
QUALITY OF SERVICE..... 3-4

CHAPTER 4..... 4-1

DIRECTORY SERVICES..... 4-1

INTRODUCTION 4-1
DIRECTORY DATA STORAGE..... 4-1
TOP LEVEL DIRECTORY NAMING..... 4-2
DIRECTORY SCHEMA..... 4-2
DIRECTORY STRUCTURING DATA STORAGE REQUIREMENTS 4-2
MMHS DATA STORAGE REQUIREMENTS..... 4-2
PKI MANAGEMENT DATA STORAGE REQUIREMENTS..... 4-3
GATEWAY DATA STORAGE REQUIREMENTS 4-4
DIRECTORY DATA EXCHANGE..... 4-4
DIRECTORY MANAGEMENT..... 4-4
ADDITIONAL MANAGEMENT PROCEDURES..... 4-5
SECURITY MANAGEMENT 4-5
CONFIDENTIALITY..... 4-5
INTEGRITY 4-5
INFORMATION DOMAINS..... 4-5
OBJECT CLASSES AND ATTRIBUTES REQUIRED FOR ACP 145..... 4-5

CHAPTER 5..... 5-1

APPLICATION SECURITY SERVICES..... 5-1

SERVICES..... 5-1
COMPUTER NETWORK DEFENCE..... 5-1
PROTOCOLS 5-2
MESSAGING SECURITY PROTOCOLS 5-2
LABELLING..... 5-3
CERTIFICATE GENERATION 5-3
SECURITY LABEL 5-3
SECURITY POLICY IDENTIFIER..... 5-4
SECURITY CLASSIFICATION..... 5-4
PRIVACY MARK..... 5-4
SECURITY CATEGORIES 5-5
IMPLICIT TAGS..... 5-5
SECURITY LABEL VALUES 5-5

CHAPTER 6..... 6-1

PUBLIC KEY INFRASTRUCTURE 6-1

- CERTIFICATE MANAGEMENT 6-1
- CERTIFICATE GENERATION 6-1
- CERTIFICATE DISTRIBUTION..... 6-2
- ROOT CERTIFICATE DISTRIBUTION 6-2
- INTERMEDIATE CAA CERTIFICATE(S) DISTRIBUTION..... 6-2
- GATEWAY CERTIFICATE DISTRIBUTION..... 6-3
- LIFECYCLE..... 6-3
- ROOT CERTIFICATE PROVISIONING..... 6-3
- CA CERTIFICATE PROVISIONING 6-3
- GATEWAY CERTIFICATE PROVISIONING 6-4
- REVOCAION NOTIFICATION 6-4
- PUBLIC KEY CERTIFICATES 6-4
- PUBLIC KEY CERTIFICATE CHECKING..... 6-5
- CERTIFICATE REVOCATION LIST CHECKING..... 6-5
- CRYPTOGRAPHY 6-5
- COMPROMISED KEY LISTS 6-5

ANNEX A 6A-1

PICS PROFORMA FOR SIGNATURE CERTIFICATES..... 6A-1

(INFORMATIVE)..... 6A-1

- SIGNATURE CERTIFICATE INTRODUCTION 6A-1
- DESCRIPTION OF TABLES 6A-1
- SUPPORT CLASSIFICATIONS 6A-2
- DYNAMIC CAPABILITY..... 6A-3
- IDENTIFICATION OF THE IMPLEMENTATION..... 6A-3

ANNEX B.....6B-1

PICS PROFORMA FOR CERTIFICATE REVOCATION LISTS.....6B-1

(INFORMATIVE).....6B-1

- CRL INTRODUCTION.....6B-1
- DESCRIPTION OF TABLES6B-1
- SUPPORT CLASSIFICATIONS6B-2
- STATIC CAPABILITY.....6B-2
- DYNAMIC CAPABILITY.....6B-3
- IDENTIFICATION OF THE IMPLEMENTATION.....6B-4

ANNEX C 6C-1

ASN.1 MODULE FOR SECURITY LABEL..... 6C-1

(NORMATIVE)..... 6C-1

ANNEX D 6D-1

**CCEB-SPECIFIC REQUIREMENTS FOR INTERIM IMPLEMENTATION OF ACP 123
MESSAGING SERVICES BETWEEN NATIONS..... 6D-1**

(NORMATIVE)..... 6D-1

 SCOPE 6D-1

 MESSAGE SIGNATURE CRYPTOGRAPHIC REQUIREMENTS 6D-1

 PKI CRYPTOGRAPIC REQUIREMENTS 6D-1

STANDARDS AND REFERENCESS&R-1

GLOSSARY OF TERMS..... GLOSSARY-1

LIST OF FIGURES

Figure 2-1: Gateway Concept 2-1

Figure 6-1: Illustrative National Gateway PKI Architecture 6-2

LIST OF TABLES

Table 6-1: Identification of PICS 6A-3

Table 6-2: Identification of Implementation and/or System 6A-4

Table 6-3: Identification of System Supplier and/or Test Laboratory Client 6A-4

Table 6-4: Identification of the CRL 6A-4

Table 6-5: Global Statement of Conformance 6A-5

Table 6-6: Self-Signed CA Signature Certificate 6A-5

Table 6-7: Algorithm Identifier 6A-6

Table 6-8: Extensions 6A-6

Table 6-9: Standard Extensions 6A-7

Table 6-10: Authority Key Identifier 6A-8

Table 6-11: Key Usage 6A-8

Table 6-12: Private Key Usage Period 6A-8

Table 6-13: Certificate Policies 6A-9

Table 6-14: Policy Mappings 6A-9

Table 6-15: Basic Constraints 6A-9

Table 6-16: Name Constraints 6A-9

Table 6-17: General Subtrees 6A-9

Table 6-18: Policy Constraints 6A-10

Table 6-19: CRL Distribution Points 6A-10

Table 6-20: Authority Information Access 6A-10

Table 6-21: CA Signature Certificate 6A-11

Table 6-22: Algorithm Identifier 6A-11

Table 6-23: Extensions 6A-12

Table 6-24: Standard Extensions 6A-12

Table 6-25: Authority Key Identifier 6A-13

Table 6-26: Key Usage 6A-13

Table 6-27: Private Key Usage Period 6A-13

Table 6-28: Certificate Policies 6A-14

Table 6-29: Policy Mappings 6A-14

Table 6-30: Basic Constraints 6A-14

Table 6-31: Name Constraints 6A-14

Table 6-32: General Subtrees 6A-14

Table 6-33: Policy Constraints 6A-15

Table 6-34: CRL Distribution Points 6A-15

Table 6-35: Authority Information Access 6A-15

Table 6-36: Gateway Signature Certificate 6A-16

Table 6-37: Algorithm Identifier 6A-16
Table 6-38: Extensions 6A-17
Table 6-39: Standard Extensions 6A-17
Table 6-40: Authority Key Identifier 6A-18
Table 6-41: Key Usage 6A-18
Table 6-42: Private Key Usage Period 6A-18
Table 6-43: Certificate Policies 6A-19
Table 6-44: Policy Mappings 6A-19
Table 6-45: Basic Constraints 6A-19
Table 6-46: Name Constraints 6A-19
Table 6-47: General Subtrees 6A-19
Table 6-48: Policy Constraints 6A-20
Table 6-49: CRL Distribution Points 6A-20
Table 6-50: Authority Information Access 6A-20
Table 6-51: Common Fields 6A-21
Table 6-52: Identification of PICS for CRLs 6B-4
Table 6-53: Identification of Implementation and/or System 6B-4
Table 6-54: Identification of System Supplier and/or Test Laboratory Client 6B-4
Table 6-55: Identification of the CRL 6B-5
Table 6-56: Global Statement of Conformance 6B-5
Table 6-57: CRL 6B-6
Table 6-58: Algorithm Identifier 6B-6
Table 6-59: Extensions 6B-7
Table 6-60: CRL Extensions 6B-7
Table 6-61: Authority Key Identifier 6B-7
Table 6-62: Issuing Distribution Point 6B-8
Table 6-63: CRL Entry Extensions 6B-8
Table 6-64: Reason Code 6B-8
Table 6-65: Common Fields 6B-9

CHAPTER 1

INTRODUCTION

BACKGROUND

101. Military Messaging (MM) services are an essential component of a modern Defence Force Command and Control infrastructure. MM allows commanders at all levels to execute effectively 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 MM 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 including cross certification, messaging between Nations will use gateway services with security services provided using Secure Multipurpose Internet Mail Extensions (S/MIME) Version 3 (V3) with its Enhanced Security Services (ESS) using a simplified security model. When all national implementations have implemented (interoperable) PKI, Message Security and, agree to cross certification, the interim solution contained within this document may become obsolete.

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 architecture between Nations. All implementation must adhere to the specifications in this document. How this is achieved within a nation is beyond the scope of this document (e.g., gateway – gateway, gateway – desktop, etc).

SCOPE OF THE DOCUMENT

104. This document details the requirements for the implementation of requirements for a common set of data structures and profiles for use between National ACP 123/STANAG 4406 based Military Message Handling Systems (MMHS). 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 MM interoperability between Nations will be achieved directly in the end system or using 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 ESS defined in this ACP. The concept is illustrated at Figure 2-1.

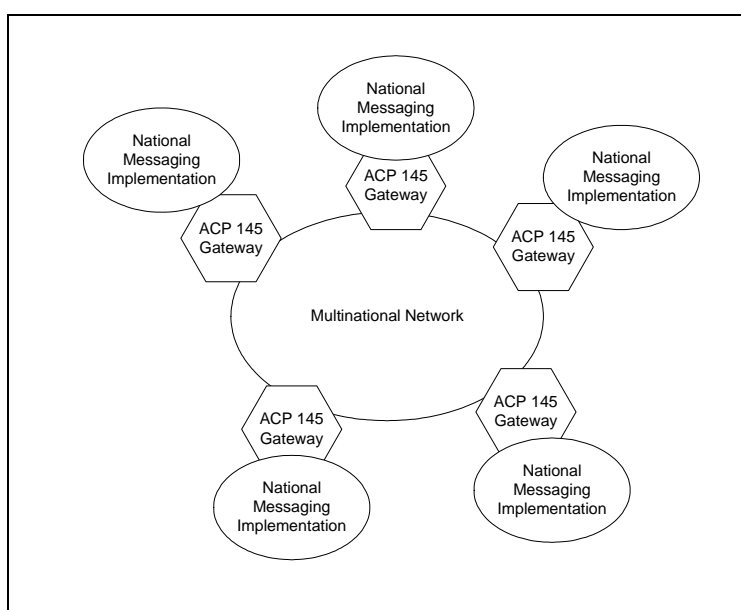


Figure 2-1: Gateway Concept

GATEWAY

202. The use of a 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:

- a. P772 (as per ACP 123/STANAG 4406);
- b. S/MIME signature with ESS label (as per chapter 5);

- c. P1 (as per ACP 123/STANAG 4406); and
- d. Directory services (as per chapter 4).

NETWORK

203. Any secure Transmission Control Protocol/Internet Protocol (TCP/IP) network can be used to provide network services to support MM between National gateway infrastructures. The network will allow Information Domains to be established in support of multinational and bilateral operations between the nations.

MESSAGING

204. 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

205. Directory services will provide a repository of information for use by MM systems and users. The primary role of the directory in support of MM is to provide Organisational Name mapping to X.400 OR Addresses and security information. The directory service is provided and managed at national borders for access by CCEB nations and coalition partners. The directory section of this document identifies the directory architecture for supporting the messaging domain structure and gives details of the schema requirements.

SECURITY

206. Applications layer messaging security services between national environments are provided by S/MIME V3 with ESS. Security services can support the Origin Authentication, Integrity and Security labelling services defined by S/MIME V3 ESS between trusted interfaces. Digital signatures are implemented using one or more trusted certificate per nation.

207. 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.

208. Application layer messaging security services are defined in Chapter 5 of this document.

209. 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.

CHAPTER 3

MESSAGING SERVICES

MANAGEMENT SERVICES

301. To achieve interoperability, nations agree to implement the required management services described by ACP 123 and STANAG 4406. Additional gateway management services may result from bilateral or multilateral 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 the sending 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/STANAG 4406 Annex A para B109).

NAMING AND ADDRESSING

304. Messages exchanged between national gateways shall comply with the naming and addressing requirements of ACP 123/STANAG 4406. In addition, the directory-name field shall be provided for each originator and recipient of the message in the formal-name field in the O/R descriptor. The value of each directory-name provided shall consist of the X.500 distinguished name corresponding to those users in the ACP 145 directory. DDA fields must not be altered or lost in transit.

PRIORITY HANDLING

305. Nations agree to implement technical or procedural mechanisms to handle inbound and outbound ACP 123/STANAG 4406 messages in accordance with the message precedence defined in ACP 123 clause 413 or the equivalent STANAG 4406 reference.

NOTIFICATIONS

306. For the most part, it is expected that nations will not implement identical ACP 123/STANAG 4406 solutions however, most nations will likely choose to implement most or all of the ACP 123/STANAG 4406 notifications/reports Elements of Service (EoS). Between nations, these national solutions will result in varied Message Transfer System (MTS) and thus,

there will be a need for a simple solution to military notifications. Nations have agreed to support the following EoS:

- a. Delivery Report (DR) and NDR (See ACP 123 clause 302 or the equivalent STANAG 4406 reference); and
- b. Receipt Notification (RN) (see ACP 123 clause 202.ag or the equivalent STANAG 4406 reference).

307. Nations agree to use best effort to deliver a message received by a recipient gateway and if a message cannot be delivered, an NDR will be generated to the originating gateway. Nations agree that an NDR could be generated by the recipient national GW or beyond. One of the criteria for the origination of an NDR is time out. Nations agree to generate an 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 or the equivalent STANAG 4406 reference. Notwithstanding, this proposed limitation on the exchange of notifications between national systems, 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).

308. ACP 145 Gateways must distinguish standard X.400 Reports and Notifications from MMs. Originating systems should not attempt to wrap, sign or provide ESS security labels for Notifications. Receiving gateways must accept and onward route standard, unwrapped X.400 Reports and Notifications.

309. For security reasons users need to be aware that, reports and notifications do not contain a security label therefore the subject line should be unclassified. Return of content in NDRs shall not be allowed.

P772 CONTENT

310. Except as otherwise stated, EoS present in the message shall be preserved by the recipient national system.

AUDIT AND LOGGING

311. ACP 123 clauses 305 and 311 and the equivalent STANAG 4406 reference define the audit and logging requirements for MM.

ADDRESS LIST (AL) EXPANSION

312. ALs will only be expanded within the source nation. Due to the residual risk that source nation 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 with an external domain OR address) to prevent secondary AL expansion to another nation.

313. AL Policy, established by the owner of the AL, will determine whether notifications are returned in response to an Originator request. Requesting of RN/Non-Receipt Notification (NRN) for AL containing a large number of members is discouraged.

GATEWAY HANDLING POLICY

314. Nations agree to only pass formal ACP 123 messages across their boundary including X.400 DR/NDR and Receipt Notifications. ACP 127 or JANAP 128 formatted messages will not be passed through the gateway except as text in an ACP 123 message.

TRANSPORT ENVELOPE

315. The transport envelope is defined in ACP 123/STANAG 4406 and the use of this transport mechanism with S/MIME is further defined in STANAG 4631. Nations agree to use the security services defined in Chapter 5 to transport the content type defined in ACP 123/STANAG 4406 across national boundaries.

APPROVED P772 CONTENT

316. Military Message content is exchanged as P772 as defined in ACP 123/STANAG 4406.

ATTACHMENTS

ATTACHMENTS PROHIBITED

317. Each nation has an obligation to take measures to protect its networks and avoid contamination of allied networks that may be connected to it. The Boundary Protection Services (BPS) implemented by national systems will determine the type of attachments acceptable to a nation. BPS should be provided at national borders for detecting and eliminating the transmission and reception of:

- a. Attachments with executable content;
- b. Malicious code;
- c. Offensive material; and

- d. Viruses.

The reception of a MM containing an attachment as described above, should result in the generation of an NDR with an appropriate error code.

ATTACHMENTS ALLOWED - THE MINIMUM SET

318. Attachments derived from the following applications form the minimum agreed set. It is essential that national systems are able to accept these attachments.

- a. **Office Applications:**

- (1) Word processing files with file extensions: .doc, .rtf, .txt,
- (2) Presentation files with file extensions: .ppt, and
- (3) Spreadsheet files with file extension: .xls;

- b. Graphic files with file extension: .gif; and;

- c. Portable document formats with file extension: .pdf.

QUALITY OF SERVICE

319. Nations accept that circumstances may arise where message delivery times might exceed that required by its precedence as defined in ACP 123/STANAG 4406, however, there is no information to determine how or when. This should be managed using normal engineering development for network sizing.

CHAPTER 4

DIRECTORY SERVICES

INTRODUCTION

401. The directory stores information (including MMHS, email and general contact information for organizations, organizational roles and organizational persons as well as certificates and certificate revocation lists for the gateway or system) and exchanges this information with other Nations through replication services, whilst protecting the integrity and confidentiality of the directory data.

402. The DS consists of a number of national Directory System Agents (DSAs) that collectively hold the multinational Directory Information Tree (DIT) for each information domain. These DSAs, which belong to the individual nation or organizations, cooperate to make the whole DIT available to international and national users. The distribution of information between these DSAs and internal systems is a local responsibility, as is the amount of information provided by an organization or a nation.

403. It is anticipated that directory support for military messaging systems will include a minimal set of information that must be shared. Supplementary information may also be shared on a bilateral basis.

404. Access to the DS data will be based on the following assumptions:

- a. User access to Directory information will only be performed at, or behind each nation's or organization's DSA, and the method of access is defined locally;
- b. Everyone with access to the network will be granted read-only access to shared information;
- c. Only authorized directory managers (persons or applications) will be given access to add, delete and change their own directory entries; and
- d. Nations receiving Directory information may modify it if necessary to make it usable on their national systems.

DIRECTORY DATA STORAGE

405. Storage of information within the national DSAs and effective sharing of this information internationally is dependent upon data storage rules which include:

- a. Top-level naming;
- b. Use of a common subset of the standard Directory Schema when exchanging directory data between nations or organizations; and

- c. Support for different functional components (such as MMHS, PKI etc.).

TOP LEVEL DIRECTORY NAMING

406. Directory naming will be based on the country-naming context. Nations are ultimately responsible for their individual DIT structures. Adherence to this high level DIT will ensure interoperability and replication of directory data. Lower level DITs will reflect national implementation and may differ.

DIRECTORY SCHEMA

407. Directory support requires the storage and retrieval of information to facilitate messaging to organizational units, organizational roles, and to formal message address lists. In addition, the directory will be used to publish Public Key information required.

408. ACP 133(C) classes A and B schema are required to support ACP 145.

409. Four distinct uses of the directory have been identified to support ACP 145. These uses are addressed in later subsections:

- a. Directory structuring support;
- b. MMHS support;
- c. PKI management support; and
- d. Gateway support.

DIRECTORY STRUCTURING DATA STORAGE REQUIREMENTS

410. Directory Structuring requirements include the ability to create directory hierarchies for both national use and to support Coalition Joint Task Force structures. Entries which may be suitable for Directory Structuring include **OrganizationalUnits**, **AliasCommonName** and **AliasOrganizationalUnit** entries.

MMHS DATA STORAGE REQUIREMENTS

411. Support is required in the Directory Service to support the onwards conversion and routing of military messages to a legacy ACP 127 address within a Nation. In order to allow a Plain Language Address (PLA) for the originator to be added, nations must provide the appropriate PLA for each directory entry corresponding to a potential Originator of a military message. The **plaACP127** attribute is defined in subset C of ACP 133(C).

412. The following ACP 133(C) defined schema objects types have been identified to support MM:

- a. **Organizational Unit entries** – ACP 123 messages will be addressed to national organizations. ACP 133 has defined an **aCPOrganizationalUnit** object class for this purpose. When using this object class the entry must contain a descriptive **organizationalUnitName** attribute, a PLA (if required), **alternatePLAName** (if required), and an X.400 O/R Address;
- b. **Organizational Role entries** – ACP 123 messaging may also be addressed to role-based entries within an organization. ACP 133 has defined an **aCPOrganizationalRole** object class for this purpose. When using this object class the entry must contain a descriptive **commonName** naming attribute and an X.400 O/R Address; and
- c. **ACPI23 Messaging ALs** – In accordance to ACP 100, a nation may be responsible for establishing and sharing formal message ALs. The Directory Service will be used to publish these lists amongst the nations. ACP 133 has defined an **addressList** object class 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 **commonName** naming attribute, the Distinguished Names of Action members of the AL in the **member** attribute, and the Distinguished Names of Information members of the AL in the **copyMember** attribute, the information plain language addressees of the collective in the **infoAddressee** attribute, and the action plain language addressees of the collective in the **actionAddressee** attribute. The Owner of the AL will need to assure that valid entries exist for members contained in the ALs being published by the nation.

PKI MANAGEMENT DATA STORAGE REQUIREMENTS

413. The Directory Service will support the use of PKI(s) between trustpoints 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.

414. **Root CA entry** – This object must be based on a 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, its **cACertificate** attribute must not be populated in the directory.

415. **Intermediate CA entry** – If required, this object must be based on a structural object class which can incorporate the **pkiCA** auxiliary object class. This entry is used to store the certificate and CRL.

GATEWAY DATA STORAGE REQUIREMENTS

416. Where ACP 145 functionality is provided by means of a Gateway, there may be additional requirements on this directory. 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. It is anticipated that most future requirements for ACP 145 gateway directory support will be of national interest and not for replication to other nations.

DIRECTORY DATA EXCHANGE

417. There is a requirement to replicate directory information between nations or organizations. The implementation of this could be dependent on a number of factors including support for multiple information domains, network topology and security requirements.

418. The Directory Service will be based on a replication service suitable for the target environment. Some possible mechanisms include:

- a. Use of messaging services to transport Directory information as message attachments (e.g., LDIF files);
- b. A meta-directory based Lightweight Directory Access Protocol (LDAP) access;
or
- c. The X.500 Directory Information Shadowing Protocol (DISP).

DIRECTORY MANAGEMENT

419. Management of the multinational Directory Service nodes is a National responsibility.

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

- a. Multinational Schema;
- b. High level DIT structure;
- c. Multinational data dictionary;
- d. Replication mechanisms; and
- e. Data integrity of shared data.

421. These issues must be detailed in the national and appropriate mutually agreed international ConOps for the networks to which the ACP 145 service are to be connected.

ADDITIONAL MANAGEMENT PROCEDURES

422. **Mastering of Non-National Directory Subtrees:** Certain data held in the directory is not specific to, nor logically owned by, a single Nation or organization, but still need to be managed, maintained and made accessible to all directory users. An example of this 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) will master this data.

SECURITY MANAGEMENT

CONFIDENTIALITY

423. Confidentiality of Directory information will be ensured by the underlying network on which the ACP 145 gateway is connected.

INTEGRITY

424. Integrity and synchronization of data must be ensured as directory information is transferred between nations.

INFORMATION DOMAINS

425. If a need for multiple information domains is identified, nations or organizations will be responsible for sharing only the subset of information releasable to a particular information domain (e.g., US/UK, 5-eyes CCEB, NATO).

OBJECT CLASSES AND ATTRIBUTES REQUIRED FOR ACP 145

426. Object classes and attribute support requirements shall be in accordance with ACP 133(C) unless otherwise agreed (e.g., bilaterally, multi-laterally). Any implementation-specific definitions of scheme elements that are required must be defined separately.

CHAPTER 5**APPLICATION SECURITY SERVICES****SERVICES**

501. This document requires three application layer message security services. They are:

- a. Authentication of Origin;
- b. Message Integrity; and
- c. 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 is the application layer directory security services;

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

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 should be 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:

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

- e. Network health;
- f. Infrastructure inventory; and
- g. Standard Operating Procedures to identify, report, manage, investigate and remedy security related incidents/intrusions.

PROTOCOLS

MESSAGING SECURITY PROTOCOLS

506. The NATO Profile for the use of S/MIME CMS and ESS (STANAG 4631), 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:

- a. 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 PKI rules specified in Chapter 6 of this;
- b. Clause 3.3.3.1 specifies the required signed attributes:
 - (1) Note that **signingTime**, **sMIMECapabilities**, and **sMIMEEncryptionKeyPreference** 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, and
 - (2) Implementations in the G2G architecture MAY support **mlExpansionHistory**, vice MUST;
- c. In clause 4.3.1, directions for populating the fields in the **essSecurityLabel** attribute are specified paragraphs 507 through 519 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); and
- d. The certificate field MUST be supported. The **extendedCertificate**, **v1AttrCert**, **v2AttrCert**, and other forms of the S/MIME **CertificateChoices** SHOULD NOT be used.

LABELLING**CERTIFICATE GENERATION**

507. Labelling is based on the NATO AC/322-D(2004) 0021 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.

508. There is no requirement to use the label for routing. This does not stop nations using the label for routing should they wish.

509. The P772 header security label will only be supported on a bilateral basis.

510. National Gateways will generate a message security label and place it into the S/MIME V3 ESS Security Label attribute as described in the following paragraphs.

511. The receiving national system must correctly interpret the security label from the originating nation. Nations need to consider also conveying and preserving the original label as a measure against label creep and as a mechanism to identify the original policy used to label the message. 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 LABEL¹

512. 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 }
```

¹ 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.

SECURITY POLICY IDENTIFIER

513. The **security-policy-identifier** is an 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.

SecurityPolicyIdentifier:= OBJECT IDENTIFIER.

SECURITY CLASSIFICATION

514. 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 will be agreed on a bilateral basis. The named values below will be used for the classifications defined in ACP 123 clause 247.

```
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

515. 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

516. 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. Annex C defines the abstract syntax of the security categories to be used by CCEB Nations.

IMPLICIT TAGS

517. Refer to Annex C.

SECURITY LABEL VALUES

518. Values exchanged in the G2G architecture for the security policy identifier, privacy mark, classification and security categories shall be defined according to originating domain's policies. The range of values exchanged and their treatment by the receiving domain may be subject to supplemental agreements.

CHAPTER 6**PUBLIC KEY INFRASTRUCTURE**

601. NATO Policy is covered in NATO PKI documentation for ACP 145 Gateways.

CERTIFICATE MANAGEMENT

602. Each Nation is progressing towards a PKI to support internal national Public Key (PK) enabled applications. However, the evolving nature of National PKIs and the technically divergent National PKIs is leading many Nations to adopt a PKI that supports the G2G Architecture with Certificate Authorities (CAs) that may not be subscribers of their National PKI. In order to minimize the risk associated with the use of evolving national PKIs, it is advised that nations may be required to deploy PKIs that will be independent from their national PKIs to support their Gateway. Alternatively, they may subscribe to another Nation's Gateway PKI or acquire a suitable commercially sourced PKI certificate.

603. Another option is to stand up a National Gateway PKI which should be designed to minimize the amount of information that would need to be published to other nations. It would be recommended that this Gateway PKI should only consist of a root (self-signing entity), subordinate CA and the Relying Party (RP), i.e., the National Gateway(s) (see Figure 6-1).

604. In this model, 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. Only the Gateway PKI Root CA certificate is needed in the trust file because the Gateway that performed the signature includes the CA's certificate who issued their certificate in the message (see below).

CERTIFICATE GENERATION

605. The specific requirements for the Root CA certificate, Intermediate CA's certificate(s), and Gateway's certificate are not specified by this document. A collective Protocol Implementation Conformance Statement (PICS) Proforma for signature certificates is provided in Annex A. The processing requirements for Relying Parties (RPs) can be found in Section 5 of RFC 3280.

606. 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

607. Distribution of the National Gateway PKI Certificate is performed via out of band procedures (e.g., exchange of a floppy disk, CD, or some other bilaterally agreed mechanism) that contain the DER encoded public key certificate of the Nation's Gateway Certificate.

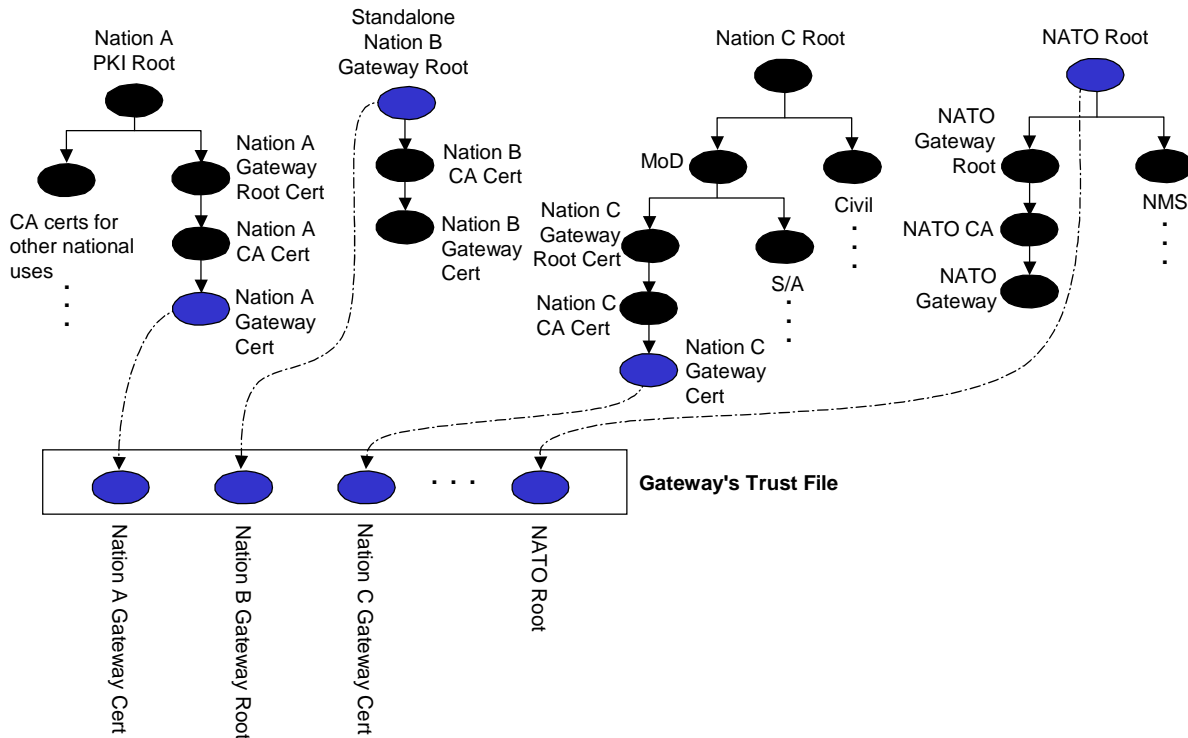


Figure 6-1: Illustrative National Gateway PKI Architecture

INTERMEDIATE CAA CERTIFICATE(S) DISTRIBUTION

608. Sending gateways should include Intermediate Gateway CAs certificate in the **SigningCertificate** attribute within the signed S/MIME V3 generated by the Gateway, and in the **pkiCA X.500** directory attribute.

GATEWAY CERTIFICATE DISTRIBUTION

609. Sending gateways should include the Gateway's Public Key Certificate in the **SigningCertificate** attribute within the signed S/MIME V3 generated by the Gateway.

LIFECYCLE

610. All subscribers of the PKI will, at one time or another, require new certificates. Root CAs, Intermediate CAs, and Gateways will need new certificates to continue subscribing to the PKI after the validity date in their certificate passes, to re-subscribe 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 "certificate provisioning" to mean any of these operations. Further, the procedures defined herein imply that the certificate provisioning process will result in a name being bound to a 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 PROVISIONING

611. To support Nation's Gateway Root Certificate expiration (i.e., current date is past the validity date in the certificate), a new root certificate needs to be generated and distributed to the other nations via the procedure defined in paragraph 607. 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).

612. Procedures for recovering from compromise of a national root should be disclosed according to respective national policies.

CA CERTIFICATE PROVISIONING

613. In order to ensure uninterrupted service, the new certificate should be distributed two weeks 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).

614. Procedures for recovering from compromise of an intermediate CA should be disclosed according to respective national policies.

GATEWAY CERTIFICATE PROVISIONING

615. 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.

616. Procedures for recovering from compromise of a gateway certificate should be disclosed according to respective national policies.

REVOCACTION NOTIFICATION

617. 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.

618. Revocation or compromise of intermediate or gateway certificates should be handled by an agreed revocation mechanism. Possible revocation mechanisms include:

- a. CRLs exchanged via the directory; and
- b. On-line status checking via OCSP.

619. If CRLs are used as the agreed revocation mechanism, CRL Issuance will generally happen every 24 hours unless operational constraints dictate otherwise. If there are no revoked certificates, the CAs are required to publish an empty CRL (i.e., a CRL with no revoked certificates).

PUBLIC KEY CERTIFICATES

620. This section specifies the V3 X.509 certificates as described in Recommendation X.509 (1997). Root, intermediate CA, gateway certificates, and CRLs should comply with national certificate profiles and policy. The specific national profiles should be disclosed to ensure mutual support. A minimum set of requirements shall be satisfied to ensure interoperability between national interface points. These requirements include the following:

- a. SHOULD NOT include private extensions that are marked critical;
- b. Certificates MUST include the public key of the subject;
- c. Certificates MUST include the DN of the issuer; and

- d. Certificate MUST include a validity period.

PUBLIC KEY CERTIFICATE CHECKING

621. 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 LIST CHECKING

622. 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

623. This section intentionally does not specify detailed algorithm information. National implementation under this policy must use algorithms that are consistent and interoperable between the National Gateways. Policies regarding appropriate cryptographic algorithms are expected to necessarily change over time. Therefore, gateway implementations are encouraged to be flexible and modular in their support of cryptographic algorithms.

624. The sending gateway should employ cryptography consistent with the sending nation's policy. Receiving gateways should be prepared to accept and validate certificates and CRLs that employ algorithms that are not consistent with their own policies.

COMPROMISED KEY LISTS

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

ANNEX A

**PICS PROFORMA FOR SIGNATURE CERTIFICATES
(INFORMATIVE)**

SIGNATURE CERTIFICATE INTRODUCTION

A 1. This Annex provides the Protocol Implementation Conformance Statement (PICS) 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 Rec. 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 the Tables in this Annex 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 standard². 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.³

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

- a. Y - the protocol element is fully supported (i.e., supporting the requirements of the m support classification);
- b. 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; and
- c. – or blank - the protocol element is not applicable.

SUPPORT CLASSIFICATIONS

A 7. Each of the protocol elements listed in the tables below is 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.

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

- a. **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;

² 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 –.

³ “Proc.” columns in the PAA, PCA, CA, External Domain, and EE certificate tables are identical.

- b. **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 was 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;
- c. **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); and
- d. **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):

- a. **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 6-1: 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 6-2: 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 6-3: 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 6-4: 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 the Identification of Implementation and/or System Table in this Annex in the row labelled “Other information”.			

Table 6-5: Global Statement of Conformance

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	signed	m	m			
2	toBeSigned	m	m			
3	version	m	m			
4	serialNumber	m	m			
5	signature	m	m			See Table 6-7; See Note 2
6	issuer	m	m			See ACP 133
7	validity	m	m			
8	notBefore	m	m			See Table 6-50 (1)
9	notAfter	m	m			See Table 6-50 (1)
10	subject	m	m			See ACP 133
11	subjectPublicKeyInfo	m	m			
12	algorithm	m	m			See Table 6-7
13	subjectPublicKey	m	m			
14	issuerUniqueIdentifier	o	o			
15	subjectUniqueIdentifier	o	o			
16	extensions	o	o			See Table 6-8
17	algorithmIdentifier	m	m			See Note 2
18	encrypted	m	m			

Note 2: Population of the “parameter” sub-field is not recommended, as the values in this field will be ignored.

Table 6-6: Self-Signed CA Signature Certificate

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

Note 3: The parameters p, q and g shall be present in the self-signed CA certificate.

Table 6-7: Algorithm Identifier

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

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

Table 6-8: Extensions

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	authorityKeyIdentifier	o	o			See Table 6-10
2	subjectKeyIdentifier	o	o			
3	keyUsage	o	o			See Table 6-11
4	extKeyUsage	o	o			
5	privateKeyUsagePeriod	o	o			See Table 6-12
6	certificatePolicies	o	o			See Table 6-13
7	policyMappings	o	o			See Table 6-14
8	subjectAltName	o	o			See Table 6-51 (1), Note 5
9	issuerAltName	o	o			See Table 6-51 (1), Note 5
10	subjectDirectoryAttributes	o	o			
11	basicConstraints	o	o			See Table 6-15; Note 6
12	nameConstraints	o	o			See Table 6-16
13	policyConstraints	o	o			See Table 6-18
14	cRLDistributionPoints	o	o			See Table 6-19 Note 5
15	authorityInfoAccess	o	o			See Table 6-20
16	inhibitAnyPolicy	o	o			
17	subjectInfoAccess	o	o			
18	freshestCRL	o	o			
<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 6-9: Standard Extensions

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	keyIdentifier	c2	c2			Note 7
2	certIssuer	c3	c3			
3	certSerialNumber	c3	c3			
<p>c2: If certIssuer or certSerialNumber is not supported then m, else o.</p> <p>c3: If keyIdentifier field is not supported then m, else o.</p> <p>Note 7: The authorityKeyIdentifier shall carry the KMID in keyIdentifier.</p>						

Table 6-10: Authority Key Identifier

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	digitalSignature	o	o			Note 8
2	nonRepudiation	o	o			Note 8
3	keyEncipherment	o	o			
4	dataEncipherment	o	o			
5	keyAgreement	o	o			
6	keyCertSign	o	o			
7	cRLSign	o	o			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 6-11: Key Usage

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	notBefore	m	C4			
2	notAfter	m	C4			
c4: Support for at least one of the components is m.						

Table 6-12: Private Key Usage Period

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

Table 6-13: Certificate Policies

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

Table 6-14: Policy Mappings

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

Table 6-15: Basic Constraints

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	permittedSubtrees	m	o			See Table 6-17
2	excludedSubtrees	m	o			See Table 6-17

Table 6-16: Name Constraints

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	base	m	m			See Table 6-51 (5)
2	minimum	m	m			d(0)
3	maximum	m	o			

Table 6-17: General Subtrees

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

Table 6-18: Policy Constraints

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	distributionPoint	o	o			See Table 6-49 (17)
2	reasons	o	o			See Table 6-49 (20)
3	cRLIssuer	o	o			See Table 6-49 (4)

Table 6-19: CRL Distribution Points

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

Note 9: See Clause 4.2.2.1 of RFC 3280 for support requirements for id-ad-caIssuers.

Table 6-20: Authority Information Access

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	signed	m	m			
2	toBeSigned	m	m			
3	Version	m	m			
4	serialNumber	m	m			
5	signature	m	m			See Table 6-22
6	issuer	m	m			See ACP 133
7	validity	m	m			
8	notBefore	m	m			See Table 6-51 (1)
9	notAfter	m	m			See Table 6-51 (1)
10	subject	m	m			See ACP 133
11	subjectPublicKeyInfo	m	m			
12	algorithm	m	m			See Table 6-22
13	subjectPublicKey	m	m			
14	issuerUniqueIdentifier	o	o			
15	subjectUniqueIdentifier	o	o			
16	extensions	o	o			See Table 6-23
17	algorithmIdentifier	m	m			See Table 6-22 Note 10
18	encrypted	m	m			

Note 10: Population of the “parameter” sub-field is not recommended, as the values in this field will be ignored.

Table 6-21: CA Signature Certificate

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

Note 11: The parameters p, q and g should be present in the CA certificates.

Table 6-22: Algorithm Identifier

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

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

Table 6-23: Extensions

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	authorityKeyIdentifier	o	o			See Table 6-25
2	subjectKeyIdentifier	o	o			
3	keyUsage	o	o			See Table 6-26
4	extKeyUsage	o	o			
5	privateKeyUsagePeriod	o	o			See Table 6-27
6	certificatePolicies	o	o			See Table 6-28
7	policyMappings	o	o			See Table 6-29
8	subjectAltName	o	o			See Table 6-51 (1)
9	issuerAltName	o	o			See Table 6-51(1)
10	subjectDirectoryAttributes	o	o			See Table 6-30
11	basicConstraints	o	o			See Table 6-30
12	nameConstraints	o	o			See Table 6-31
13	policyConstraints	o	o			See Table 6-33
14	cRLDistributionPoints	o	o			See Table 6-34
15	authorityInfoAccess	o	o			See Table 6-35
16	inhibitAnyPolicy	o	o			
17	subjectInfoAccess	o	o			
18	freshestCRL	o	o			See Table 6-34

Table 6-24: Standard Extensions

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	keyIdentifier	c7	c7			Note 15
2	certIssuer	c8	c8			
3	certSerialNumber	c8	c8			

c7: If certIssuer or certSerialNumber is not supported then m, else o.
c8: If keyIdentifier field is not supported then m, else o.
Note 15: The authorityKeyIdentifier shall carry the KMID in keyIdentifier.

Table 6-25: Authority Key Identifier

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	digitalSignature	o	o			Note 16
2	nonRepudiation	o	o			Note 16
3	keyEncipherment	o	o			
4	dataEncipherment	o	o			
5	keyAgreement	o	o			
6	keyCertSign	o	o			
7	cRLSign	o	o			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 6-26: Key Usage

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	notBefore	m	c9			
2	notAfter	m	c9			

c9: Support for at least one of the components is m.

Table 6-27: Private Key Usage Period

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

Table 6-28: Certificate Policies

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

Table 6-29: Policy Mappings

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

Table 6-30: Basic Constraints

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	permittedSubtrees	m	o			See Table 6-32
2	excludedSubtrees	m	o			See Table 6-32

Table 6-31: Name Constraints

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	base	m	m			See Table 6-51(5)
2	minimum	m	m			d(0)
3	maximum	m	o			

Table 6-32: General Subtrees

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

Table 6-33: Policy Constraints

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	distributionPoint	o	o			See Table 6-51 (17)
2	reasons	o	o			See Table 6-51 (20)
3	cRLIssuer	o	o			See Table 6-51 (4)

Table 6-34: CRL Distribution Points

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

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

Table 6-35: Authority Information Access

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	signed	m	m			
2	toBeSigned	m	m			
3	version	m	m			
4	serialNumber	m	m			
5	signature	m	m			See Table 6-37
6	issuer	m	m			See ACP 133
7	validity	m	m			
8	notBefore	m	m			See Table 6-51 (1)
9	notAfter	m	m			See Table 6-51 (1)
10	subject	m	m			See ACP 133
11	subjectPublicKeyInfo	m	m			
12	algorithm	m	m			See Table 6-37
13	subjectPublicKey	m	m			
14	issuerUniqueIdentifier	o	o			
15	subjectUniqueIdentifier	o	o			
16	extensions	o	o			See Table 6-38
17	algorithmIdentifier	m	m			See Table 6-37
18	encrypted	m	m			
Note 18: Population of the “parameter” sub-field is not recommended, as the values in this field will be ignored.						

Table 6-36: Gateway Signature Certificate

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	algorithm	m	m			
2	parameters	m	m			Note 19
Note 19: The parameters p, q and g should be present in the Gateway certificates.						

Table 6-37: Algorithm Identifier

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

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

Table 6-38: Extensions

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	authorityKeyIdentifier	o	o			See Table 6-40
2	subjectKeyIdentifier	o	o			
3	keyUsage	o	o			See Table 6-41
4	extKeyUsage	o	o			
5	privateKeyUsagePeriod	o	o			See Table 6-42
6	certificatePolicies	o	o			See Table 6-43
7	policyMappings	o	o			See Table 6-44
8	subjectAltName	o	o			See Table 6-51 (1), Note 22
9	issuerAltName	o	o			See Table 6-51 (1), Note 22
10	subjectDirectoryAttributes	o	o			
11	basicConstraints	o	o			See Table 6-45
12	nameConstraints	o	o			See Table 6-46
13	policyConstraints	o	o			See Table 6-48
14	cRLDistributionPoints	o	o			See Table 6-49, Note 21
15	authorityInfoAccess	o	o			See Table 6-50
16	inhibitAnyPolicy	o	o			
17	subjectInfoAccess	o	o			
18	freshestCRL	o	o			See Table 6-49

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 6-39: Standard Extensions

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	keyIdentifier	c11	c11			Note 23
2	certIssuer	c12	c12			
3	certSerialNumber	c12	c12			
<p>c11: If certIssuer or certSerialNumber is not supported then m, else o.</p> <p>c12: If keyIdentifier field is not supported then m, else o.</p> <p>Note 23: The authorityKeyIdentifier shall carry the KMID in keyIdentifier.</p>						

Table 6-40: Authority Key Identifier

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	digitalSignature	o	o			Note 24
2	nonRepudiation	o	o			Note 24
3	keyEncipherment	o	o			
4	dataEncipherment	o	o			
5	keyAgreement	o	o			
6	keyCertSign	o	o			
7	cRLSign	o	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 6-41: Key Usage

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	notBefore	m	c13			
2	notAfter	m	c13			
c13: Support for at least one of the components is m.						

Table 6-42: Private Key Usage Period

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

Table 6-43: Certificate Policies

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

Table 6-44: Policy Mappings

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

Table 6-45: Basic Constraints

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	permittedSubtrees	m	o			See Table 6-47
2	excludedSubtrees	m	o			See Table 6-47

Table 6-46: Name Constraints

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	base	m	m			See Table 6-51 (5)
2	minimum	m	m			d(0)
3	maximum	m	o			

Table 6-47: General Subtrees

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

Table 6-48: Policy Constraints

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	distributionPoint	o	o			See Table 6-65 (17)
2	reasons	o	o			See Table 6-65 (20)
3	cRLIssuer	o	o			See Table 6-65 (4)

Table 6-49: CRL Distribution Points

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

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

Table 6-50: Authority Information Access

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	time					
2	UTCTime	m	m			
3	generalizedTime	o	o			
4	generalNames					
5	generalName	m	m			
6	otherName	o	o			
7	rfc822Name	o	o			Note 26
8	DNSName	o	o			Note 26
9	x400Address	o	o			See ACP 123
10	directoryName	o	o			See ACP 133
11	ediPartyName	o	o			
12	nameAssigner	o	o			
13	partyName	o	o			
14	uniformResourceIdentifier	o	o			Note 26
15	IPAddress	o	o			Note 26
16	registeredID	o	o			
17	distributionPointName					
18	fullName	m	m			See (4)
19	nameRelativeToCRLIssuer	m	m			See ACP 133
20	reasonFlags					
21	unused	o	o			
22	keyCompromise	o	o			
23	CACompromise	o	o			
24	affiliationChange	o	o			
25	superseded	o	o			
26	cessationOfOperation	o	o			
27	certificateHold	o	o			

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

Table 6-51: Common Fields

ANNEX B

**PICS PROFORMA FOR CERTIFICATE REVOCATION LISTS
(INFORMATIVE)**

CRL INTRODUCTION

B 1. This Annex provides the Protocol Implementation Conformance Statement (PICS) for the CRL for use in this environment. The structure for the CRL is defined in the 1997 version of ITU-T Rec. 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 the tables in this Annex 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 the tables below is 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:** The information for this protocol element must be populated upon certificate generation.

IDENTIFICATION OF THE IMPLEMENTATION

B 16. The tables below should be used to provide details on the 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 6-52: Identification of PICS for CRLs

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 6-53: 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 6-54: 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 6-55: 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 the Identification of Implementation and/or System Table in this Annex in the row labelled “Other information”.</p>			

Table 6-56: Global Statement of Conformance

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	signed	m	m			
2	toBeSigned	m	m			
3	version	o	o			
4	signature	m	m			See Table 6-58, Note 2
5	issuer	m	m			See ACP 133
6	thisUpdate	m	m			See Table 6-65 (1)
7	nextUpdate	o	o			See Table 6-65 (1)
8	revokedCertificates	o	o			
9	userCertificates	m	m			
10	revocationDate	m	m			See Table 6-65 (1)
11	crlEntryExtensions	o	o			See Table 6-63
12	crlExtensions	o	o			See Table 6-60
13	algorithmIdentifier	m	m			See Table 6-58, Note 2
14	encrypted	m	m			

Note 2: Population of the “parameter” sub-field is not recommended, as the values in this field will be ignored.

Table 6-57: CRL

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

Table 6-58: Algorithm Identifier

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

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 6-59: Extensions

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	authorityKeyIdentifier	o	o			See Table 6-61
2	issuerAltName	o	o			See Table 6-65 (4)
3	cRLNumber	o	o			
4	issuingDistributionPoint	o	o			See Table 6-62, Note 4
5	deltaCRLIndicator	o	o			

Note 4: This extension shall be indicated as critical.

Table 6-60: CRL Extensions

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

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

Table 6-61: Authority Key Identifier

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	distributionPoint	o	o			See Table 6-65 (17)
2	onlyContainsUserCerts	o	o			d(false)
3	onlyContainsCACerts	o	o			d(false)
4	onlySomeReasons	o	o			See Table 6-65 (20)
5	indirectCRL	o	o			d(false)

Table 6-62: Issuing Distribution Point

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	reasonCode	o	o			See Table 6-64
2	instructionCode	o	o			
3	invalidityDate	o	o			
4	certificateIssuer	o	o			See Table 6-65 (4), Note 5

Note 5: This extension shall be indicated as critical.

Table 6-63: CRL Entry Extensions

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

Table 6-64: Reason Code

Item	Protocol Element	Base		Support		Notes
		Proc.	Gen.	Proc.	Gen.	
1	time					
2	UTCTime	m	m			
3	generalizedTime	o	o			
4	generalNames					
5	generalName	m	m			
6	otherName	o	o			
7	rfc822Name	o	o			Note 6
8	dNSName	o	o			Note 6
9	x400Address	o	o			See ACP 123
10	directoryName	o	o			See ACP 133
11	ediPartyName	o	o			
12	nameAssigner	o	o			
13	partyName	o	o			
14	uniformResourceIdentifier	o	o			Note 6
15	iPAddress	o	o			Note 6
16	registeredID	o	o			
17	distributionPointName					
18	fullName	m	m			See (4)
19	nameRelativeToCRLIssuer	m	m			See ACP 133
20	reasonFlags					
21	unused	o	o			
22	keyCompromise	o	o			
23	caCompromise	o	o			
24	affiliationChange	o	o			
25	superseded	o	o			
26	cessationOfOperation	o	o			
27	certificateHold	o	o			

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

Table 6-65: Common Fields

ANNEX C

ASN.1 MODULE FOR SECURITY LABEL

(NORMATIVE)

```
informationSecurityLabelModule { joint-iso-ccitt (2) country (16) u.s. (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 permissive attributes

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

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

-- Type 3 - enumerated restrictive attributes

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

-- 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 }
```

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

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

-- Object identifier assignment

ID ::= OBJECT IDENTIFIER

id-infosec ID ::= { joint-iso-ccitt (2) country (16) u.s. (840) organization (1) gov (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-enumeratedPermissiveAttributes ID ::= { id-commonSecurityCategoriesSyntaxes 1 }

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

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

id-enumeratedRestrictiveAttributes ID ::= { id-commonSecurityCategoriesSyntaxes 4 }

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 five 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 Permissive 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. All attributes enumerated by tags of this type are of the permissive type (e.g., release permissions).

C 5. The Enumerated Restrictive 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. All attributes enumerated by tags of this type are of the restrictive type (e.g., compartments).

C 6. 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 7. 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.

ANNEX D

**CCEB-SPECIFIC REQUIREMENTS FOR
INTERIM IMPLEMENTATION OF ACP 123
MESSAGING SERVICES BETWEEN NATIONS**

(NORMATIVE)

SCOPE

D 1. This annex encapsulates additional requirements for CCEB Nations that implement ACP 145(A). This annex is normative for CCEB Nations, but can be considered as informative for other users of ACP 145(A).

MESSAGE SIGNATURE CRYPTOGRAPHIC REQUIREMENTS

D 2. The Secure Hash Algorithm (SHA-1) is the approved hashing algorithm for use in message signatures.

D 3. Implementations are required to support generating message signatures using at least one of the Digital Signature Algorithm (DSA) or the Rivest, Shamir, Adelman (RSA) algorithm. Implementations are required to support validating message signatures using both algorithms. These requirements are identical to those of the cited commercial S/MIME standards. Note that there are two versions of the RSA Algorithm commonly referred to as the X9 version and PKCS #1 v1.5. The version cited herein is the PKCS #1 v1.5 algorithm.

PKI CRYPTOGRAPIC REQUIREMENTS

D 4. SHA-1 is the approved hashing algorithm for certificate and CRL signatures.

D 5. RSA (PKCS #1 v1.5) is the approved signature algorithm for certificate and CRL signatures.

STANDARDS AND REFERENCES

Reference	Title
AC/322-D (2004) 0021	INFOSEC Technical and implementation guidance for electronic labelling of NATO information
ACP 100	Allied Callsigns and Address Group Systems – Instructions and Assignments
ACP 123	Common Messaging Strategy and Procedures
ACP 127	Communications Instructions – Tape Relay Procedures
ACP 128	Allied Telecommunications Record System (ALTERS) Operating Procedures
ACP 133	Common Directory Services and Procedures
DSA	FIPS PUB 186-2, Digital Signature Standard, 27 January 2000
DSA CN1	FIPS PUB 186-2 Change Notice 1, 5 October 2001
RFC 2634	Enhanced Security Services for S/MIME
RFC 3280	Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
RFC 3855	Transporting Secure/Multipurpose Internet mail Extensions (S/MIME) Objects in X.400
RSA	PKCS #1: RSA Encryption Standard, v1.5, 1 November 1993
SHA-1	FIPS PUB 180-1, Secure Hash Standard, 17 April 1995
STANAG 4406	Military Message Handling System
STANAG 4631	Profile for the use of the Cryptographic Message Syntax (CMS) and the Enhanced Security Services (ESS) for S/MIME
X.400	ITU-T Series of Recommendations on Message Handling Systems
X.500	ITU-T Series of Recommendations on Directory Services

GLOSSARY OF TERMS

Abbreviation	Definition
ACP	Allied Communications Publication
AL	Address List
ASN	Abstract Syntax Notation
BPS	Boundary Protection Services
CA	Certificate Authority
CCEB	Combined Communications Electronics Board
CCITT	Consultative Committee International Telegraph & Telephone
CMDE	Common Messaging and Directory Environment
CMI	Certificate Management Infrastructure
CMS	Cryptographic Message Syntax
CND	Computer Network Defence
CNOC	Combined Network Operations Centre
CRL	Certificate Revocation List
DER	Distinguished Encoding Rules
DISA	Defense Information System Agency
DISN	Defense Information System Network
DISP	Directory Information Shadowing Protocol
DIT	Directory Information Tree
DN	Directory Name
DR	Delivery Report
DS	Directory Services
DSA	Directory System Agent or Digital Signature Algorithm
EE	End Entity
EoS	Elements of Service
ESS	Enhanced Security Services
G2G	Gateway-to-Gateway
GMT	Greenwich Mean Time
GW	Gateway
IPKI	Internet Public Key Infrastructure
ITU-T	International Telecommunications Union - Telecommunication

Abbreviation	Definition
KMID	Key Material Identifier
LDAP	Lightweight Directory Access Protocol
LDIF	Lightweight Directory Access Protocol Data Interchange Format
MM	Military Messaging
MMHS	Military Message Handling System
MTA	Message Transfer Agent
MTS	Message Traffic System
NATO	North Atlantic Treaty Organisation
NNOC	National Network Operations Centre
NDR	Non-Delivery Report
NRN	Non-Receipt Notification
O/R	Originator / Recipient
OID	Object Identifier
PK	Public Key
PKCS	Public Key Cryptosystem
PKI	Public Key Infrastructure
POC	Point Of Contact
RN	Receipt Notification
RP	Relaying Party
RSA	Rivest Shamir Adelman
S/MIME	Secure Multipurpose Internet Mail Extensions
SHA-1	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
UTCTime	Universal Time
V2	Version 2
V3	Version 3