T/3501TL/2778/9

27 January 1997

Copy No.: ____

# CLOUD COVER
# CONFIDENTIALITY KEY INFRASTRUCTURE
# PART 4: SCHEMA FOR THE USE OF AN X.500 DIRECTORY IN SUPPORT OF THE CKI

**ISSUE 0.A**

This document and its content **shall** only be used for the purpose for which it was issued. The copyright of this document is reserved and is vested in the Crown

©1997 Crown Copyright.

# FOREWORD

This paper is issued by the Communications-Electronics Security Group (CESG) of Government Communications Headquarters as part of its responsibility to advise HMG on Electronic Information Systems Security (Infosec).

It suggests an architecture for a public key infrastructure (PKI) to support confidentiality between communicating systems. The paper forms part of a suite of documents which collectively provide advice on the implementation of a PKI, and the use of the services enabled by such an infrastructure (eg electronic mail). The architecture as described in the paper is an initial attempt at defining a PKI, and CESG will take into account any comments on its feasibility.

Technical correspondence in connection with this document should be addressed to:

Communications-Electronics Security Group (X27)
Government Communications Headquarters
PO Box 144
Cheltenham GL52 5UE
United Kingdom

| AMENDMENT RECORD | | |
|---|---|---|
| **Issue** | **Date** | **Description** |
| Initial draft | 6 December 1996 | |
| 0.A | 27 January 1997 | Reformat & release for internal review |

# CONTENTS

FOREWORD . . . . . ii
CONTENTS . . . . . iv
REFERENCES . . . . . v
DEFINITIONS . . . . . vi

**I. INTRODUCTION** . . . . . 1

**II. OVERVIEW** . . . . . 2

**III. ATTRIBUTE DEFINITIONS** . . . . . 3

**IV. OBJECT CLASS DEFINITIONS** . . . . . 4

Annex A ASN.1 Module . . . . . 5

# REFERENCES


[HMG] Securing Electronic Mail within HMG - Part I: Infrastructure and Protocol, Draft C, T/3113TL/2776/11 21 March 1996

[DH76] New Directions in Cryptography, IEEE Trans. In Information Theory IT-22 (1976) pages 644-655 W. Diffie and M. Hellman

[RHC] A proposed Architecture for Trusted Third Party Services, N. Jefferies, C. Mitchell, M. Walker, Information Security Group, Royal Holloway

[PKI-1] Internet Public Key Infrastructure Part I: X.509 Certificate and CRL Profile, June 1996, Internet Draft

[PKI-3] Internet Public Key Infrastructure Part III: Certificate Management Protocols, November 1996, Internet Draft

[RFC 822] "Standard for the format of ARPA Internet text messages", D. Crocker, 08/13/1982

[RFC 1521] "MIME (Multipurpose Internet Mail Extensions) Part One: Mechanisms for Specifying and Describing the Format of Internet Message Bodies", N. Borenstein, N. Freed, 09/23/1993

[RFC 793] "Transmission Control Protocol", J. Postel, 09/01/1981

[X.214] ITU-T X.214 (95) | ISO/IEC 8072:1996 Information technology - Open systems interconnection - Transport service definition

[X.420] ITU-T X.420 (to be published) | ISO 10021-7 Information technology - Message Handling Systems (MHS) - Interpersonal Messaging System

**Note:** this is equivalent to X.420 (92) plus implementor's guide version 8.

[X.500] ITU-T Recommendation X.500 to X.525 (1993) | ISO/IEC 9594:1994, Information technology – Open Systems Interconnection – The Directory

[X.509DAM] Final Text of Draft Amendments DAM 4 to ISO/IEC 9594-2, DAM 2 to ISO/IEC 9594-6, DAM 1 to ISO/IEC 9594-7, and DAM 1 to ISO/IEC 9594-8 on Certificate ExtensionsISO/IEC JTC 1/SC 21/WG 4 and ITU-T Q15/7 Collaborative Editing Meeting on the Directory, Geneva, April 1996 - Final draft 30th June 1996

[X.509TC] Technical Corrigenda to Rec. X.500 | ISO/IEC 9594 resulting from Defect Reports 9594/128

[X.509] ITU-T X.509 (93) | ISO/IEC 9594-8: 1995 Information Technology – Open Systems Interconnection – The Directory: Authentication Framework

[X.511] ITU-T X.511 (93) | ISO/IEC 9594-3: 1995 Information Technology – Open Systems Interconnection – The Directory: Abstract Service Definition

[X.690] ITU-T X.690 (94) | ISO/IEC 8825-1:1995 Information Technology Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

# DEFINITIONS

## CKI Architecture Definitions

The following terms and associated concepts are described in the CKI Architecture and Concept of Operation (Part 1):

a. Certificate Management Authority (CMA)

b. CKI certificate

c. CKI User Agent (CKI UA)

d. CMA certificate

e. Domain

f. Domain certificate

g. Domain public / private key

h. External

i. Interoperability key

j. Local

k. Name constraints

l. Receive certificate

m. Receive public / private key

n. Recipient

o. Revoked user list

p. Seed key

q. Seed key identifier

r. Send certificate

s. Send public / private key

t. Sender

u. Shared secret key

v. Top Level Certificate Management Authority (TLCMA)

### X.509 Authentication Framework Definitions

The following terms are defined in the X.509 Authentication Framework [X.509]:

a. CA certificate

b. Certification Authority (CA)

c. Certificate

d. Certificate Revocation List (CRL)

### X.500 Directory Definitions

The following terms are defined in the Directory standard [X.500]:

a. Distinguished name

### Abbreviations

| | |
|---|---|
| AKI | Authentication Key Infrastructure |
| CA | Certification Authority |
| CKI | Confidentiality Key Infrastructure |
| CMA | Certificate Management Authority |
| CRL | Certificate Revocation List |
| PKI | Public Key Infrastructure |
| TLCMA | Top Level Certificate Management Authority |
| UA | User Agent |

# I. INTRODUCTION

1. This specification defines the sub-schema for use of an X.500 directory in support of a Confidentiality Key Infrastructure Key (CKI).

2. It is not essential to use an X.500 directory in support of the CKI. Thus, this schema is only required where an X.500 directory is used to distribute CKI certificates.

3. The CKI uses asymmetric cryptographic techniques in the generation of a shared symmetric key for confidentiality.

4. This specification is part 4 of a set of specifications for the CKI, which includes:

   Part 1: Architecture and concept of operation for the CKI;

   Part 2: CKI key management protocol;

   Part 3: Profile for the use of X.509 certificates in support of the CKI;

   Part 4: Schema for the use of an X.500 directory in support of the CKI;

   Part 5: Mapping of the CKI key management protocol onto communication and messaging protocols.

5. The use of X.500 directories is an optional part of the CKI.

6. The CKI is based on the Diffie-Hellman key agreement mechanism [DH76] with support of trusted third party services [RHC].

7. The CKI was initially developed to support secure electronic mail within and between UK government departments [HMG]. However, it is designed to be applicable to a range of application and communication services, and can be used to support confidentiality for governmental, commercial or any other type of organisation.

8. The CKI supports the management of confidentiality keys. It forms part of a public key infrastructure which can also incorporate an infrastructure for the management of authentication keys (called the Authentication Key Infrastructure - AKI). The AKI can be used to provide certified keys for signing CKI certificates and protecting protocol exchanges required for the CKI.

9. The design of the CKI takes account of the ongoing development of standards for public key infrastructures as they exist at the time this specification was developed (e.g. Internet PKI as defined in [PKI-1] and [PKI-3]).

## II. OVERVIEW

10. A Directory based on [X.500] can be used to distribute:

- send certificates,
- receive certificates,
- CRLs for CKI certificates,
- CRLs for CA Certificates including CMA certificates,
- domain certificates and
- CMA certificates.

11. This information is written into the directory when it is created and can be read by any CKI UA or peer CMA requiring the information.

12. The directory entry for the CMA holds:

- the CMA's domain certificate,
- the CMA certificate,
- CRLs for CKI certificates,
- CRLs for CA certificates.
- The directory entry for each user in a CMA's domain holds:
- the user's send certificate,
- the user's local receive certificate.

13. For each user in an external domain, for which a receive certificate has been created, the CMA creates an alternative entry for that user within the CMA's own directory management domain which holds:

- the user's external receive certificate,
- "see also" reference to the user's main entry.

**Note:** This alternative entry is required as the CMA, and its users, may not have the required access rights to the external user's home directory management domain.

14. To assist in locating the alternative entry of an external user the CMA holds a subtree mapping table which identifies an external naming subtree and its local alternative.

## III. ATTRIBUTE DEFINITIONS

15. The CKI certificates are held in the following attributes:

```
sendCertificate ATTRIBUTE ::= {
    SUBTYPE OF      userCertificate -- defined in [X.509]
    WITH SYNTAX     Certificate
    ID          id-cki-at-sendCertificate }

receiveCertificate ATTRIBUTE ::= {
    SUBTYPE OF      userCertificate
    WITH SYNTAX     Certificate
    ID          id-cki-at-receiveCertificate }

domainCertificate ATTRIBUTE ::= {
    SUBTYPE OF      userCertificate
    WITH SYNTAX     Certificate
    ID          id-cki-at-domainCertificate }
```

16. A CRL for CKI certificates is held in attribute **`certificateRevocationList`** and a CRL for CA certificates is held in attribute as defined in [X.509].

17. The following attribute specifies the mapping from a subtree for users in an external domain to a subtree in the CMA's directory management domain.

```
externalUserSubtreeMapping ATTRIBUTE ::= {
    WITH SYNTAX     UserSubtreeMapping
    ID          id-cki-at-externalUserSubtreeMapping }
UserSubtreeMapping ::= SEQUENCE OF SEQUENCE {
    externalBase    GeneralName, -- defined in [X.509DAM]
    localBase       GeneralName             }
```

18. The procedure for using the **`externalUserSubtreeMapping`** attribute is as follows:

    a. The **`externalBase`** value which matches all or part of the external user's distinguished name (from the root down) is found. If two or more **`externalBase`** values match then the one with the most complete match should be selected.

    b. If a match is found for the part of the user name, the **`externalBase`** is replaced by the **`localBase`** to find the alternative entry for the user (i.e. the one holding the receive certificate).

    **Note:** Names that match this mapping table are not necessarily members of the external domain û see Part 1, ºVI.C on name constraints.

## IV. OBJECT CLASS DEFINITIONS

19. The CKI user auxiliary object class is for objects which use the CKI:

```
ckiUser OBJECT-CLASS ::= {
    SUBCLASS OF     {top}
    KIND            auxiliary
    MAY CONTAIN     {sendCertificate |
                     receiveCertificate }
    ID          id-cki-oc-ckiUser }
```

20. The Certificate Management Authority auxiliary object class is for objects which act as a CMA. This object inherits the attributes of a certification authority (CA certificate, revocation lists etc.).

```
certificateManagementAuthority ::= {
    SUBCLASS OF     {certificationAuthority-V2}
-- This inherits mandatory attributes: caCertificate,
-- certificateRevocationList and authorityRevocationList
    KIND            auxiliary
    MAY CONTAIN     {domainCertificate |
externalUserSubtreeMapping }
    ID          id-cki-oc-certificateManagementAuthority }
```

21. The **externalCKIuser** auxiliary object class is for the alternative entry of external users. This is used as an auxiliary with the same structural object class as for the main user entry.

```
externalCkiUser OBJECT-CLASS ::= {
    SUBCLASS OF     {top}
    KIND            auxiliary
    MAY CONTAIN     {receiveCertificate |
                     seeAlso}
    ID          id-cki-oc-externalCkiUser }
```

## Annex A ASN.1 Module

```
CKIDirectorySchema {iso(1) member-body(2) uk(826) disc(0) cesg(1145)
       infosec(1) cki(4) module(1) directorySchema (2) }
DEFINITIONS ::=
BEGIN

IMPORTS
-- Note: The object identifier reference for the following modules
-- may change with the final publication of the 1997 edition of X.500

    Certificate
        FROM AuthenticationFramework {joint-iso-ccitt ds(5) module(1)
                    authenticationFramework(7) 2}

    NameConstraintsSyntax, GeneralName
        FROM CertificateExtensions {joint-iso-ccitt ds(5) module(1)
                    certificateExtensions(26) 0}

    OBJECT-CLASS, ATTRIBUTE, top, auxiliary
        FROM InformationFramework {joint-iso-ccitt ds(5) module(1)
                    informationFramework(1) 2}

    certificationAuthority-V2
        FROM SelectedObjectClasses {joint-iso-ccitt ds(5) module(1)
                        selectedObjectClasses(6) 2}
    userCertificate, seeAlso
        FROM SelectedAttributeTypes {joint-iso-ccitt ds(5) module(1)
                    selectedAttributeTypes(5) 2};


-- Attribute Definitions

sendCertificate ATTRIBUTE ::= {
    SUBTYPE OF      userCertificate -- defined in [X.509]
    WITH SYNTAX     Certificate
    ID          id-cki-at-sendCertificate }

receiveCertificate ATTRIBUTE ::= {
    SUBTYPE OF      userCertificate
    WITH SYNTAX     Certificate
    ID          id-cki-at-receiveCertificate }

domainCertificate ATTRIBUTE ::= {
    SUBTYPE OF      userCertificate
    WITH SYNTAX     Certificate
    ID          id-cki-at-domainCertificate }

externalUserSubtreeMapping ATTRIBUTE ::= {
    WITH SYNTAX     UserSubtreeMapping
    ID          id-cki-at-externalUserSubtreeMapping }

UserSubtreeMapping ::= SEQUENCE OF SEQUENCE {
    externalBase    GeneralName, -- defined in [X.509DAM]
    localBase       GeneralName             }
```

```
-- Object Class Definitions

ckiUser OBJECT-CLASS ::= {
    SUBCLASS OF     {top}
    KIND            auxiliary
    MAY CONTAIN     {sendCertificate |
receiveCertificate }
    ID          id-cki-oc-ckiUser }

certificateManagementAuthority ::= {
    SUBCLASS OF     {certificationAuthority-V2}
-- This inherits mandatory attributes: caCertificate,
-- certificateRevocationList and authorityRevocationList
    KIND            auxiliary
    MAY CONTAIN     {domainCertificate |
externalUserSubtreeMapping }
    ID          id-cki-oc-certificateManagementAuthority }

externalCkiUser OBJECT-CLASS ::= {
    SUBCLASS OF     {top}
    KIND            auxiliary
    MAY CONTAIN     {receiveCertificate |
                     seeAlso}
    ID          id-cki-oc-externalCkiUser }


-- Object Identifier Assignments

id-cki          OBJECT IDENTIFIER   ::= {iso(1) member-body(2)
       uk(826) disc(0) cesg(1145) infosec(1) cki(4)}

id-cki-module       OBJECT IDENTIFIER   ::= {id-cki 1}
id-cki-at           OBJECT IDENTIFIER   ::= {id-cki 2}
id-cki-oc           OBJECT IDENTIFIER   ::= {id-cki 3}


-- Attributes

id-cki-at-sendCertificate   OBJECT IDENTIFIER   ::= {id-cki-at 1}
id-cki-at-receiveCertificate OBJECT IDENTIFIER  ::= {id-cki-at 2}
id-cki-at-domainCertificate OBJECT IDENTIFIER   ::= {id-cki-at 3}
id-cki-at-domainNameConstraints
                    OBJECT IDENTIFIER   ::= {id-cki-at 4}
id-cki-at-externalUserSubtreeMapping
                    OBJECT IDENTIFIER   ::= {id-cki-at 5}


-- Object classes

id-cki-oc-ckiUser       OBJECT IDENTIFIER   ::= {id-cki-oc 1}
id-cki-oc-certificateManagementAuthority
                    OBJECT IDENTIFIER   ::= {id-cki-oc 2}
id-cki-oc-externalCkiUser   OBJECT IDENTIFIER   ::= {id-cki-oc 3}

END
```