T/3500TL/2778/9

27 January 1997

Copy No.: ____

CLOUD COVER
CONFIDENTIALITY KEY INFRASTRUCTURE
PART 3: X.509 CERTIFICATE PROFILE

ISSUE 0.A

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

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 document profiles the use of public key certificates, and certificate revocation lists, for a confidential key infrastructure (CKI).

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

3. This specification is part 3 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.

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

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

6. 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.

7. 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.

8. 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. GENERAL

9. The certificates used for the CKI are as defined in [X.509] with the extensibility defined in [X.509TC] using the certificate extension fields defined in [X.509DAM].

10. Other requirements on the use of certificate (and CRL) extension fields which are in common to the Authentication Key Infrastructure are to be specified separately.

III. SEND / RECEIVE CERTIFICATE PROFILE

11. The X.509 certificate fields, including extension fields, for the send and receive certificates are used as follows:

Field Name	Usage
`version`	v3
`serialNumber`	as per standard
`signature`	as per standard - this carries the same algorithm identifier as used in the certificate signature.
`issuer`	as per standard - this carries the issuing CMA's distinguished name
`validity`	as per standard - the date part of **`notBefore`** and **`notAfter`** are also used as the Datestamp value in generating of the subject public key. The universal time representation (ending in "Z") of GeneralizedTime shall be used. Note: A draft technical corrigendum is being issued to enable use of GeneralizedTime in validity.
`subject`	as per standard - this carries the distinguished name of the sender or recipient.
`subjectPublicKeyInfo` `algorithm`	Object identifier for key agreement algorithm as used in this CKI

`parameters`	Both send and receive certificate: the seed key identifier, as used in generating the public key
	Send certificate: Base and modulus
	The syntax to be used for this field is:
	`SEQUENCE {`
	`seedKeyId   KeyIdentifier,`
	`baseModulus BaseModInfo OPTIONAL`
	`}`

`subjectPublicKey`	as per standard - this carries the send or receive public key
`issuerUniqueIdentifier`	not required
`subjectUniqueIdentifier`	not required

`authorityKeyIdentifier`
(extension)
`Key Identifier`
	this contains an identifier for the CMA's public key which is used to verify the certificate.
	Note:In the case of the CMA's public key being revoked the subject's key is also revoked.
	Non-CriticalNote: In the case of this field not being recognised, if an CMA public key is revoked then all certificates issued by that CMA are revoked independent of which public key is used.

`keyUsage` (extension)	**`keyAgreement`** bit always set if send certificate: **`decipherOnly`** bit (bit 7) is set if receive certificate: **`encipherOnly`** bit (bit 8) is set Critical Note: A draft technical corrigendum is being issued to add these key usage bits to those defined in [X.509DAM].
`basicConstraints` (extension)	**`cA`** is FALSE Critical

IV. DOMAIN CERTIFICATE PROFILE

12. The X.509 certificate fields, including extension fields, for the domain certificates are used as follows:

Field Name	**Usage**
`version`	v3
`serialNumber`	as per standard
`signature`	as per standard - this carries the same algorithm identifier as used in the certificate signature.
`issuer`	as per standard - this carries the issuing CA’s distinguished name. Note: This may be the CMA or some other CA.
`validity`	as per standard The universal time representation (ending in “Z”) of `GeneralizedTime` shall be used. Note: A draft technical corrigendum is being issued to enable use of `GeneralizedTime` in validity.
`subject`	as per standard - this carries the distinguished name of the CMA.
`subjectPublicKeyInfo` `algorithm`	Object identifier for key agreement algorithm as used to establish interchange keys from domain public / private keys.
`parameters`	Base and modulus carried in `BaseModInfo` (as defined in Part 2)
`subjectPublicKey`	as per standard - this carries the domain public key.
`issuerUniqueIdentifier`	not required
`subjectUniqueIdentifier`	not required
`keyUsage` (extension)	`keyAgreement` bit set
`basicConstraints` (extension)	cA is `FALSE` Critical

V. CMA CERTIFICATE PROFILE

13. The X.509 certificate fields, including extension fields, for the CMA certificates are used as follows:

Field Name	Usage
version	v3
serialNumber	as per standard
signature	as per standard - this carries the same algorithm identifier as used in the certificate signature.
issuer	as per standard - this carries the issuing CA's distinguished name
validity	as per standard The universal time representation (ending in "Z") of **GeneralizedTime** shall be used. Note: A draft technical corrigendum is being issued to enable use of GeneralizedTime in validity.
subject	as per standard - this carries the distinguished name of the CMA.
subjectPublicKeyInfo **algorithm**	Object identifier for key agreement algorithm as used to sign certificates.
parameters	No parameters required
subjectPublicKey	as per standard - this carries domain public key.
issuerUniqueIdentifier	not required
subjectUniqueIdentifier	not required
subjectKeyIdentifier (extension)	this contains an identifier for the CMA's public key. This identifier shall be unique across the domains where the CMA certificate is used (e.g. created using a hash of certificate serial number and CMA certificate issuer name.) Non-critical. Note: In the case of this field not being recognised, if an CMA public key is revoked then all certificates issued by that CMA are revoked independent of which public key is used.
basicConstraints (extension)	cA is **TRUE** **pathLenConstraint** = 0 Critical

`nameConstraints` (extension)	The name constraints for users in the CMAs domain Critical

VI. CRL PROFILE

14. The certificate revocation list (CRL) used for the CKI is as defined in [X.509] with the extensibility defined in [X.509TC] using the certificate extension fields defined in [X.509DAM].

15. The fields, including extension fields, of the CRL are used as follows:

Field Name	**Usage**
`version`	v2
`signature`	as per standard - this carries the same algorithm identifier as used in the certificate signature
`issuer`	as per standard
`thisUpdate`	as per standard
`nextUpdate`	not required
`revokedCertificates` `userCertificate`	Serial number of revoked certificate
`revocation date`	It is recommended that this field be used for audit purposes.