

MCSD ONLY



Certificate Authority Project

MCSD Certification Practice Statement for MCSD General Signature Certificates

Document No: MCSD-PKI-CPS-GSC

MCSD ONLY



Document History

DOCUMENT DESCRIPTION	
TITLE	M.C.S.D. Certification Practice Statement for M.C.S.D. General Signature Certificates
REFERENCE	M.C.S.D.-PKI-CPS-GSC
AUTHOR	C. REMAN
VERSION	0.6
RELEASE DATE	19/07/2005
AUTHORISED BY	

DOCUMENT VERSION HISTORY			
VERSION	DATE	COMMENTS	AUTHOR
0.1	19/08/2005	First draft.	C. REMAN
0.2	05/09/2005	Modifications following remarks.	C. REMAN
0.3			
0.4			
0.5			
0.6	29/07/2007	Version for Approval: still remaining information to get from ITIDA	F. CAVENNE



Table of Contents

REFERENCES	10
1 INTRODUCTION	11
1.1 Overview	11
1.2 Document Name and Identification	11
1.3 PKI Participants	11
1.3.1 Policy Management Authority (PMA)	12
1.3.2 Certification Authority (CA)	12
1.3.3 Registration Authority (RA)	12
1.3.4 Local Registration Authority (LRA).....	13
1.3.5 Customer Support Officer	13
1.3.6 Verification Officer	14
1.3.7 Issue and Revocation Officer.....	14
1.3.8 Operators.....	15
1.3.9 Subscribers.....	15
1.3.10 Subjects.....	15
1.3.11 Relying Parties.....	16
1.3.12 Other participants	16
1.4 Certificate Usage	16
1.4.1 Appropriate Certificate Uses.....	16
1.4.2 Prohibited Certificate Uses	16
1.5 Policy Administration	16
1.5.1 Organization Administering the Document	16
1.5.2 Contact Person.....	16
1.5.3 Person Determining CPS Suitability for the Policy.....	17
1.5.4 CPS Approval Procedures	17
1.6 Definitions and Acronyms	17
1.6.1 Definitions.....	17
1.6.2 Acronyms.....	20
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES	22
2.1 Repositories	22
2.2 Publication of Certification Information	22
2.3 Time or Frequency of Publication	22
2.4 Access Controls on Repositories	23
3 IDENTIFICATION AND AUTHENTICATION	24



M.C.S.D. ONLY

- 3.1 Naming 24**
 - 3.1.1 Type of Names 24
 - 3.1.2 Need for Names to be Meaningful 24
 - 3.1.3 Anonymity or Pseudonymity of Subjects..... 25
 - 3.1.4 Rules for Interpreting Various Name Forms 25
 - 3.1.5 Uniqueness of Names 25
 - 3.1.6 Recognition, Authentication and Role of Trademarks 25

- 3.2 Initial Identity Validation 25**
 - 3.2.1 Method to Prove Possession of Private Key 25
 - 3.2.2 Authentication of Organization Identity 26
 - 3.2.3 Authentication of Individual Identity 27
 - 3.2.4 Non-Verified Subject Information 27
 - 3.2.5 Validation of Authority 28
 - 3.2.6 Criteria for Interoperation 28

- 3.3 Identification and Authentication for Re-Key Requests 28**
 - 3.3.1 Identification and Authentication for Routine Re-Key..... 28
 - 3.3.2 Identification and Authentication for Re-Key After Revocation 28

- 3.4 Identification and Authentication for Revocation Requests 28**

- 4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 30**

- 4.1 Certificate Application..... 30**
 - 4.1.1 Who Can Submit a Certificate Application 30
 - 4.1.2 Enrolment Process and Responsibilities..... 30

- 4.2 Certificate Application Processing 32**
 - 4.2.1 Performing Identification and Authentication Functions 32
 - 4.2.2 Approval or Rejection of Certificate Applications 32
 - 4.2.3 Time to Process Certificate Applications 32

- 4.3 Certificate Issuance 32**
 - 4.3.1 CA Actions During Certificate Issuance 32
 - 4.3.2 Notifications to Subject by the CA of Issuance of Certificate 32

- 4.4 Certificate Acceptance 32**
 - 4.4.1 Conduct Constituting Certificate Acceptance..... 32
 - 4.4.2 Publication of the Certificate by the CA 33
 - 4.4.3 Notification of Certificate Issuance by the CA to Other Entities 33

- 4.5 Key Pair and Certificate Usage..... 33**
 - 4.5.1 Subject Private Key and Certificate Usage 33
 - 4.5.2 Relying Party Public Key and Certificate Usage 33

- 4.6 Certificate Renewal 33**
 - 4.6.1 Circumstances for Certificate Renewal 33
 - 4.6.2 Who May Request Renewal 33
 - 4.6.3 Processing Certificate Renewal Requests 33
 - 4.6.4 Notification of New Certificate Issuance to Subject..... 33
 - 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 33
 - 4.6.6 Publication of the Renewal Certificate by the CA..... 34



M.C.S.D. ONLY

- 4.6.7 Notification of Certificate Issuance by the CA to Other Entities 34
- 4.7 Certificate Re-Key 34**
 - 4.7.1 Circumstances for Certificate Re-Key 34
 - 4.7.2 Who May Request Certificate of a New Public Key 34
 - 4.7.3 Processing Certificate Re-Keying Requests 34
 - 4.7.4 Notification of New Certificate Issuance to Subject 34
 - 4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate 34
 - 4.7.6 Publication of the Re-Keyed Certificate by the CA 34
 - 4.7.7 Notification of Certificate Issuance by the CA to Other Entities 34
- 4.8 Certificate Modification 34**
 - 4.8.1 Circumstances for Certificate Modification 35
 - 4.8.2 Who May Request Certificate Modification Requests 35
 - 4.8.3 Processing Certificate Modification Requests 35
 - 4.8.4 Notification of New Certificate Issuance to Subject 35
 - 4.8.5 Conduct Constituting Acceptance of Modified Certificate 35
 - 4.8.6 Publication of the Modified Certificate by the CA 35
 - 4.8.7 Notification of Certificate Issuance by the CA to Other Entities 35
- 4.9 Certificate Revocation and Suspension 35**
 - 4.9.1 Circumstances for Revocation 35
 - 4.9.2 Who Can Request Revocation 35
 - 4.9.3 Procedure for Revocation Request 36
 - 4.9.4 Revocation Request Grace Period 37
 - 4.9.5 Time Within Which CA Must Process the Revocation Request 37
 - 4.9.6 Revocation Checking Requirements for Relying Parties 37
 - 4.9.7 CRL Issuance Frequency 37
 - 4.9.8 Maximum Latency for CRLs 37
 - 4.9.9 On-Line Revocation/Status Checking Availability 37
 - 4.9.10 On-Line Revocation Checking Requirements 37
 - 4.9.11 Other Forms of Revocation Advertisements Available 37
 - 4.9.12 Special Requirements Related to Key Compromise 37
 - 4.9.13 Circumstances for Suspension 37
 - 4.9.14 Who Can Request Suspension 37
 - 4.9.15 Procedure for Suspension Request 38
 - 4.9.16 Limits on Suspension Period 38
- 4.10 Certificate Status Services 38**
 - 4.10.1 Operational Characteristics 38
 - 4.10.2 Service Availability 38
 - 4.10.3 Optional features 39
- 4.11 End of Subscription 39**
- 4.12 Key Escrow and Recovery 39**
 - 4.12.1 Key Escrow and Recovery Policy and Practices 39
 - 4.12.2 Session Key Encapsulation and Recovery Policy and Practices 39
- 5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS 40**
 - 5.1 Physical Controls 40**
 - 5.1.1 Site Location and Construction 40



M.C.S.D. ONLY

- 5.1.2 Physical Access 40
- 5.1.3 Power and Air Conditioning 40
- 5.1.4 Water Exposures 41
- 5.1.5 Fire Prevention and Protection 41
- 5.1.6 Media Storage 41
- 5.1.7 Waste Disposal..... 41
- 5.1.8 Off-Site Backup..... 41

- 5.2 Procedural Controls 41**
 - 5.2.1 Trusted Roles 41
 - 5.2.2 Number of Persons Required per Task 43
 - 5.2.3 Identification and Authentication for Each Role 44
 - 5.2.4 Roles Requiring Separation of Duties..... 44

- 5.3 Personnel Controls 45**
 - 5.3.1 Qualifications, Experience and Clearance Requirements 45
 - 5.3.2 Background Check Procedures 45
 - 5.3.3 Training Requirements 45
 - 5.3.4 Retraining Frequency and Requirements 45
 - 5.3.5 Job Rotation Frequency and Sequence..... 45
 - 5.3.6 Sanctions for Unauthorized Actions..... 45
 - 5.3.7 Independent Contractor Requirements..... 46
 - 5.3.8 Documentation Supplied to Personnel..... 46

- 5.4 Audit Logging Procedures..... 46**
 - 5.4.1 Types of Events Recorded 46
 - 5.4.2 Frequency of Processing Log 46
 - 5.4.3 Retention Period of Audit Log 46
 - 5.4.4 Protection of Audit Log 46
 - 5.4.5 Audit Log Backup Procedures 46
 - 5.4.6 Audit Collection system (Internal or External)..... 46
 - 5.4.7 Notification to Event-Causing Subject..... 47
 - 5.4.8 Vulnerability Assessments 47

- 5.5 Records Archival 47**
 - 5.5.1 Types of Records Archived..... 47
 - 5.5.2 Retention Period for Archive 48
 - 5.5.3 Protection of Archive..... 48
 - 5.5.4 Archive Backup Procedures 48
 - 5.5.5 Requirements for Time-Stamping of Records..... 48
 - 5.5.6 Archive Collection System (Internal or External) 48
 - 5.5.7 Procedure to Obtain and Verify Archive Information..... 49

- 5.6 Key Changeover 49**

- 5.7 Compromise and Disaster Recovery 49**
 - 5.7.1 Incident and Compromise Handling Procedures 49
 - 5.7.2 Computing Resources, Software and/or Data Are Corrupted 49
 - 5.7.3 Entity Private Key Compromise Procedures 50
 - 5.7.4 Business Continuity Capabilities After a Disaster 50

- 5.8 CA or RA Termination 50**



6	TECHNICAL SECURITY CONTROLS.....	51
6.1	Key Pair Generation and Installation	51
6.1.1	Key Pair Generation	51
6.1.2	Private Key Delivery to CA component.....	51
6.1.3	Private Key Delivery to Subject.....	51
6.1.4	Public Key Delivery to Certificate Issuer	51
6.1.5	CA Public Key Delivery to Relying Parties	52
6.1.6	Key Sizes.....	52
6.1.7	Public Key Parameters Generation and Quality Checking.....	52
6.1.8	Key Usage Purposes (as per X.509 V3 Key Usage Field).....	52
6.2	Private Key Protection and Cryptographic Module Engineering Controls	52
6.2.1	Cryptographic Module Standards and Controls	52
6.2.2	Private Key (3 out of 5) Multi-Person Control	53
6.2.3	Private Key Escrow.....	53
6.2.4	Private Key Backup	53
6.2.5	Private Key Archival.....	53
6.2.6	Private Key Transfer Into or Form a Cryptographic Module.....	54
6.2.7	Private Key Storage on Cryptographic Module	54
6.2.8	Method of Activating Private Key	54
6.2.9	Method of Deactivating Private Key.....	54
6.2.10	Method of Destroying Private Key	55
6.2.11	Cryptographic Module Rating	55
6.3	Other Aspects of Key Pair Management.....	55
6.3.1	Public Key Archival	55
6.3.2	Certificate Operational Periods and Key Pair Usage Periods	55
6.4	Activation Data.....	55
6.4.1	Activation Data Generation and Installation	56
6.4.2	Activation Data Protection	56
6.4.3	Other Aspects of Activation Data	56
6.5	Computer Security Controls	56
6.5.1	Specific Computer Security Technical Requirements	56
6.5.2	Computer Security Rating.....	57
6.6	Life Cycle Technical Controls.....	57
6.6.1	System Development Controls	57
6.6.2	Security Management Controls.....	57
6.6.3	Life Cycle Security Controls.....	58
6.7	Network Security Controls.....	58
6.8	Time-Stamping	58
7	CERTIFICATE, CRL AND OCSP PROFILES.....	59
7.1	Certificate Profile	59
7.1.1	Version Number(s).....	59
7.1.2	Certificate Extensions	59
7.1.3	Algorithm Object Identifiers.....	59



M.C.S.D. ONLY

- 7.1.4 Name Forms59
- 7.1.5 Name Constraints59
- 7.1.6 Certificate Policy Object Identifier59
- 7.1.7 Usage of Policy Constraints Extension59
- 7.1.8 Policy Qualifiers Syntax and Semantics59
- 7.1.9 Processing Semantics for the Critical Certificate Policies Extension60
- 7.2 CRL Profile..... 60**
 - 7.2.1 Version Number(s).....60
 - 7.2.2 CRL and CRL Entry Extensions.....60
- 7.3 OCSP Profile..... 60**
 - 7.3.1 Version Number(s).....60
 - 7.3.2 OCSP Extensions60
- 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS 61**
 - 8.1 Frequency and Circumstances of Assessment 61**
 - 8.2 Identify/Qualifications of Assessor 61**
 - 8.3 Assessor’s Relationship to Assessed Entity 61**
 - 8.4 Topics Covered by Assessment 61**
 - 8.5 Actions Taken as a Result of Deficiency..... 61**
 - 8.6 Communications of Results 61**
- 9 OTHER BUSINESS AND LEGAL MATTERS 62**
 - 9.1 Fees 62**
 - 9.1.1 Certificate Issuance or Renewal Fees62
 - 9.1.2 Certificate Access Fees62
 - 9.1.3 Revocation or Status Information Access Fees62
 - 9.1.4 Fees for Other Services.....62
 - 9.1.5 Refund Policy.....62
 - 9.2 Financial Responsibility..... 62**
 - 9.2.1 Insurance Coverage62
 - 9.2.2 Other Assets62
 - 9.2.3 Insurance or Warranty Coverage for End-entities.....62
 - 9.3 Confidentiality of Business Information 62**
 - 9.3.1 Scope of Confidential Information.....62
 - 9.3.2 Information Not Within the Scope of Confidential Information63
 - 9.3.3 Responsibility to Protect Confidentiality Information63
 - 9.4 Privacy of Personal Information..... 63**
 - 9.4.1 Privacy Plan.....63
 - 9.4.2 Information Treated as Private.....63
 - 9.4.3 Information Not Deemed Private.....64
 - 9.4.4 Responsibility to Protect Private Information64



MCS D ONLY

9.4.5 Notice and Consent to Use Private Information 64

9.4.6 Disclosure Pursuant to Judicial or Administrative Process 64

9.4.7 Other Information Disclosure Circumstances 64

9.5 Intellectual Property Rights 64

9.6 Representations and Warranties 64

9.6.1 CA Representations and Warranties 64

9.6.2 RA/LRA Representations and Warranties 64

9.6.3 Subject Representations and Warranties 64

9.6.4 Subscriber Representations and Warranties 64

9.6.5 Relying Party Representations and Warranties 64

9.6.6 Representations and Warranties of Other Participants 64

9.7 Disclaimers of Warranties 64

9.8 Limitations of Liability 65

9.9 Indemnities 65

9.10 Term and Termination 65

9.10.1 Term 65

9.10.2 Termination 65

9.10.3 Effect of Termination and Survival 65

9.11 Individual Notices and Communications with Participants 65

9.12 Amendments 65

9.12.1 Procedure for Amendment 65

9.12.2 Notification Mechanism and Period 65

9.12.3 Circumstances Under Which OID Must be Changed 66

9.13 Dispute Resolution Provisions 66

9.14 Governing Law 66

9.15 Compliance with Applicable Law 66

9.16 Miscellaneous Provisions 66

9.16.1 Entire Agreement 66

9.16.2 Assignment 66

9.16.3 Severability 66

9.16.4 Enforcement (Attorney’s Fees and Waiver of Rights) 66

9.16.5 Force Majeure 66

9.17 Other Provisions 67

References

TITLE	REFERENCE
<i>M.C.S.D. Certificate Policy for M.C.S.D. Digital Signature Certificates</i>	[M.C.S.D._PC]
FIPS140-1 - <i>Security Requirements for Cryptographic Modules</i> , January 1994.	[FIPS140-1]
ISO/IEC 3166 – Codes for the representation of names of countries and their subdivisions – Part 1 : country codes	[ISO3166]
ISO/IEC 7816 - Identification Cards - Integrated Circuit Cards with Contacts	[ISO7816]
ISO/IEC 17799 – Information technology – Security techniques – Code of practice for information security management	[ISO17799]
ISO/IEC 9594-8 (2001) - <i>Information Technology – Open Systems Interconnection : The Directory : Authentication Framework</i> .	[ISO9594-8]
<i>Internet X.509 Public Key Infrastructure, Certificate and Certificate Revocation List (CRL) Profile</i> (April 2002) - Internet Engineering Task Force (IETF) - Network Working Group	[RFC3280]
<i>Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework</i> (November 2003) - Internet Engineering Task Force (IETF) - Network Working Group	[RFC3647]
<i>Internet X.509 Public Key Infrastructure, Qualified Certificates Profile</i> (March 2004) - Internet Engineering Task Force (IETF) - Network Working Group	[RFC3739]
ETSI TS 101 456 V1.2.1 – <i>Policy requirements for certification authorities issuing qualified certificates</i> , February 2004.	[ETSI TS 101 456]
BS 7799 Code of Practice for Information Security Management	[BS7799]
<i>Law n°15 Of The Year 2004 Regulating Electronic Signature (E-Signature) and Establishing The Information Technology (IT) Industry Development Authority</i>	[L-15]
<i>Ministry Of Communications And Information Technology – Decree n°109 For The Year 2005 Dated 15/5/2005 Issuing The Executive Regulations Of The Electronic Signature Law And Establishing The Information Technology (IT) Industry Development Authority</i>	[D-109]



1 Introduction

A Certification Practice Statement (CPS) is a statement of the practices which a Certification Authority employs when issuing certificates and managing the life-cycle of such certificates in accordance with the requirements of the associated Certificate Policy.

The CPS addresses the technical, procedural personnel policies and practices of the CA and security measures in all services and during the complete life cycle of certificates as issued the CA.

1.1 Overview

This document defines the Certification Practice Statement (CPS) for the issuance of MSCD General Signature Certificates by the M.C.S.D. Certification Authority as described in the Certificate Policy (CP) named "M.C.S.D. Certificate Policy for M.C.S.D. Digital Signature Certificates".

The MSCD General Signature Certificate is one of the two types of certificates the CA could issue.

The MSCD General Signature Certificate is for the management and use of certificates containing public keys used for authentication and data integrity and in support of non-repudiation. This certificate contains no transaction limits.

These certificates are suitable to be used for access control and digital signature and in particular to sign unlimited value transaction to be processed through the systems of MSCD.

The M.C.S.D. Certification Authority is a direct subordinate CA to the **ITIDA Root Certificate Authority. XXX Check the name of ITIDA CA XXX**

The information contained in this CPS is intended for personnel charged with the management and operation of certificates issued by the M.C.S.D. Certification Authority as well as for Subjects, Subscribers and other Relying Parties which have a relationship with MSCD Certificate Authority in respect to certificates issued by this CA.

The readers of this CPS shall also refer to the associated Certificate Policy in order to get all of the information about duties for each participant.

This CPS complies with the formal requirements of IETF RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework – with regard to format and content.

1.2 Document Name and Identification

This document is named : M.C.S.D. Certification Practice Statement for M.C.S.D. General Signature Certificates.

The document version number is : 0.2.

This Certification Practice Statement is also identified by an OID **XXX OID has to be requested, derived from the CP OID XXX.**

1.3 PKI Participants

The following sections introduce the PKI and community roles involved in issuing certificates and managing the certificate life cycle process.



1.3.1 Policy Management Authority (PMA)

The MCSD Policy Management Authority (PMA) is a body established by MCSD to :

- Oversee the creation and update of certificate policies, including evaluation of changes requested and plans for implementing any accepted changes.
- Review the Certification Practice Statements (CPS) to ensure that the practices of PKI components comply with the associated Certificate Policy.
- Oversee and audit the PKI.

The Policy Management Authority is the board of MCSD.

1.3.2 Certification Authority (CA)

The Certification Authority (CA) is the entity authorized by the PMA to create, sign and issue certificates.

The CA have a software and hardware infrastructure. The technology used for CA operations is Nexus Certificate Manager.

The CA is responsible for all aspects of the issuance and management of a certificate.

The CA shall ensure that the following functions are performed in accordance with the stipulations of the CP and this CPS :

- Certificate generation and revocation.
- Certificate and Certificate Revocation List (CRL) publication.

CA functions shall be performed by trained and vetted personnel knowing and applying procedures described in the CP and CPS.

MCSD CA shall be certified by the **ITIDA Root Certificate Authority. XXX Check the name of ITIDA CA XXX** allowing Relying Parties to have a trusted certification path for certificate interoperability.

The certificate registration function is a mandatory function of a PKI. The registration function is carried out by a component of the PKI separate from the CA which is bound to the CA or works with the CA.

The CA shall process and validate certification requests and revocation requests coming from Registration Authorities (RA).

1.3.3 Registration Authority (RA)

The Registration Authority is the entity that enters into an Agreement with the CA to collect and verify certificate applicants' identity and information, which is to be entered into certificates.

The RA have a software and hardware infrastructure.

The RA shall ensure that the following functions are performed in accordance with the stipulations of the CP and this CPS :

- Coordinate certification requests.



M.C.S.D. ONLY

- Verify the applicant's identity, information and applicant's right for performing such a request.
- Collect and process revocation requests through the CA.

RA functions shall be performed by trained and vetted personnel knowing and applying procedures described in the CP and CPS.

The RA could consist into one or several separate entities. Several structures could be allowed as long as the registration process is in accordance with the stipulations of this Policy. Therefore, the RA may delegate all or a part of its functions to local entities (LRA). In that case, the RA shall be responsible for the LRAs and shall supervise them.

1.3.4 Local Registration Authority (LRA)

A Local Registration Authority (LRA) is the entity that performs registration tasks on behalf of the RA.

A LRA is supervised by the RA. It may have a geographical or business connection and it operates within the framework of the M.C.S.D. PKI accredited procedures.

LRA shall ensure that the following functions are performed in accordance with the stipulations of the CP and this CPS :

- Verify the Subscriber's identity, register it and register the Trusted Signatories within the Subscriber organisation.
- Verify the Subject's identity and/or information and applicant's right for performing such a request.
- Manage and protect private data relating to Subscribers and Subjects.
- Deliver to the Subject the smartcard containing the public/private key pair and the associated certificate and smartcard's activation code.
- Collect and process certificate and revocation requests.

LRA functions shall be performed by trained and vetted personnel knowing and applying procedures described in the CP and CPS.

LRA functions are performed by several entities for separation of duties. Those entities are :

- Customer Support Officer
- Verification Officer
- Issue and Revocation Officer

1.3.5 Customer Support Officer

A Customer Support Officer is an entity that performs some functions of LRA tasks.

Customer Support Officers shall ensure that the following functions are performed in accordance with the stipulations of the CP and this CPS :

- Verify, in a face-to-face process with the Subscriber's representative, the Subscriber's identity, register it and register the Trusted Signatories within the Subscriber organisation.



MCS D ONLY

- Verify, in a face-to-face process, the Subject's identity and information before transmitting the certification request to the Verification Officer
- Deliver to the Subject the smartcard containing the public/private key pair and the associated certificate and smartcard's activation code.
- Collect Subject certificate acceptance forms.
- Collect revocation requests from Subscribers and/or Subjects.
- Provide technical support for Subjects.

Customer Support Officer functions shall be performed by trained and vetted personnel knowing and applying procedures described in the CP and CPS.

1.3.6 Verification Officer

A Verification Officer is an entity that performs some functions of LRA tasks.

Verification Officer shall ensure that the following functions are performed in accordance with the stipulations of the CP and this CPS :

- Collect certification requests and/or revocation requests from the Customer Support Officer.
- Verify identifying information and/or other data.
- Verify Subject's right for performing such a request.
- Create identity and/or revocation requests into the RA system.
- Submit issuance and/or revocation requirements to Issue and Revocation Officers.

Verification Officer functions shall be performed by trained and vetted personnel knowing and applying procedures described in the CP and CPS.

1.3.7 Issue and Revocation Officer

An Issue and Revocation Officer is an entity that performs some functions of LRA tasks.

Issue and Revocation Officers shall ensure that the following functions are performed in accordance with the stipulations of the CP and this CPS :

- Authorize certificate issuance and/or revocation
- Generate public/private keys and collect the issued certificate associated to those keys.
- Manage printing and personalization of smartcards.
- Verify the publication of CRL after certificate revocation.
- Authorize suspension and re-activation of certificates when required.
- Manage secure PIN production and dispatch.
- Deliver smartcards and activation data to Customer Support Officers.



MCSD ONLY

Issue and Revocation Officer functions shall be performed by trained and vetted personnel knowing and applying procedures described in the CP and CPS.

1.3.8 Operators

A Operator is the entity responsible for day-to-day technical operations and maintenances of the servers and infrastructure needed to support the MCSD CA and PKI components.

Operator functions shall be performed by trained and vetted personnel knowing and applying procedures described in the CP and CPS.

1.3.9 Subscribers

A Subscriber is the entity that contracts with the MCSD Certification Authority for the issuance of certificates on behalf of one or more Subjects.

The Subscriber bears ultimate responsibility for use of the private key associated with the public key certificate.

In the case of certificates issued to individual for their own use the Subscriber and Subject can be the same entity. In other cases, such as certificates issued to employees the Subscriber and Subject are different. The Subscriber would be, for instance, the employer and the Subject would be the employee.

Subscribers of MCSD include :

- Issuer companies,
- Brokerage firms / custodians,
- Individuals investors,
- Capital Market Authority,
- Stock Exchange,
- Clearing banks,
- Arabic Stock Exchange,
- Arabic Clearing and Settlement.

1.3.10 Subjects

A Subject is the entity whose name appears as the *Subject* in a certificate and who asserts that it uses its key and certificate in accordance with the CP and this CPS.

Subjects are individual persons that :

- Apply for a certificate.
- Are identified in a certificate.
- Hold the private key corresponding to the public key that is listed in a Subject certificate.

1.3.11 Relying Parties

A Relying Party is an entity including individuals and/or companies that rely on a certificate and/or a digital signature verifiable with reference to a public key listed in a Subject's certificate.

A Relying Party may, or may not also be a Subject or a Subscriber within the PKI.

The Relying Parties shall have access to directory services to obtain PKI related information such as the certificates and CRLs.

They shall also have access to a Web site to obtain related information such as the CP and this CPS.

1.3.12 Other participants

No stipulation

1.4 Certificate Usage

Certificates asserting a policy OID defined in this document shall only be used for transactions described in this CPS.

1.4.1 Appropriate Certificate Uses

MCSD General Signature Certificates shall be used with no transaction limit value for the following purposes :

- Digital signature of documents or data according to the Egyptian Law n°15 of 2004 and the Ministry of Communications and Information Technology Decree n°109 of 2005 (e.g. transactions to be processed through the systems of MCSD, CMA, CASE and other participants in the Egyptian capital markets).
- Access control to the MCSD Information System.

1.4.2 Prohibited Certificate Uses

Regulation of this is given in the associated CP.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The PMA is responsible for the review, approving and promulgation of this CPS.

The Policy Management Authority is the board of MCSD.

1.5.2 Contact Person

For issues related to this CPS, contact :

MCSD Policy Management Authority

70 El-Gomhoria Street



Cairo

EGYPT

Phone : +202 259 71 581

E-mail : XXX create a generic e-mail which isn't a named e-mail XXX

1.5.3 Person Determining CPS Suitability for the Policy

Regulation of this is given in the associated CP.

1.5.4 CPS Approval Procedures

Regulation of this is given in the associated CP.

1.6 Definitions and Acronyms

1.6.1 Definitions

Activation data	Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share).
Applicant	The Subject is sometimes also called an “applicant” after applying to a Certificate Authority for a certificate, but before the certificate issuance procedure is completed.
Archive	Long-term, physically separate storage.
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Backup	Copy of files and programs made to facilitate recovery if necessary.
Certificate Authority (CA)	An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.
Certificate	A digital representation of information which at least identifies the certification authority issuing it, names or identifies its Subject, contains the Subject’s public key, identifies its operational period, and is digitally signed by the Certification Authority issuing it.
Certificate Policy (CP)	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A CP addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates.
Certificate Revocation List (CRL)	A list maintained by a CA of the certificates which it has issued that were revoked prior to their stated expiration date.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).

**M.C.S.D. ONLY**

Certification path	An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.
Common Name	This is the X.500 commonName attribute, which contains a name of an object. If the object corresponds to a person, it is typically the person's full name.
Customer Support Officer	A Local registration Authority (LRA) that ensures some functions of LRA tasks, especially face-to-face with Subscribers and Subjects.
Cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.
Digital signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party who has the initial message can determine : (a) whether the transformation was created using the key that corresponds to the signer's key; and (b) whether the message has been altered since the transformation was made.
Distinguished Name (DN)	An ISO X.500 term defining a standard for unique identifiers for people, devices or other objects
Entity	Any autonomous element within the PKI. This may be a CA, a RA, an LRA or a Subject.
Key pair	Two mathematically related keys having the properties that one key can be used to encrypt a message that can only be decrypted using the other key, and even knowing one key, it is computationally infeasible to discover the other key.
Issue and Revocation Officer	A Local registration Authority (LRA) that ensures some functions of LRA tasks, especially certificate issuance and revocation authorization and smartcard personalization.
Local Registration Authority (LRA)	A Registration Authority with responsibility for a local community.
Nexus Certificate Manager	The software used for providing CA functions.
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.
Operator	Personnel responsible for the technical management of the PKI system and cryptographic services.
PKI	PKI is a set of policies, processes, server platforms, software, and workstations used to administer certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the



M.C.S.D. ONLY

PKI certificate policies.

Private key	The signing key pair used to create a digital signature or the key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public key	The signing key pair used to validate a digital signature or the key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Registration Authority (RA)	An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing Subject requests to revoke or suspend their certificates, and approving or rejecting requests by Subjects to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application.
Relying Party	A recipient of a certificate who acts in reliance on that certificate and/or any digital signatures verified using that certificate.
Relying Party Agreement	An Agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates. It may also be referred to as a directory.
Revoke (a certificate)	To prematurely end the operational period of a certificate effective at a specific date and time.
Root Certificate Authority (root CA)	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust certification paths) for a security domain.
SafeSign Management Server	The software used for providing RA and LRA functions.
Smartcard	A hardware token that contains a chip to implement among others cryptographic functions and that possesses some inherent resistance to tampering.
Subject	A Subject is an entity that is the subject named or identified in a certificate issued to that entity; holds a private key that corresponds to the public key listed in the certificate, and does not itself issue certificates to another party. A Subject may be a Subscriber acting on its own behalf.
Subject Agreement	An Agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subject.
Subscriber	A Subscriber is an entity subscribing with a CA on behalf of one or more Subjects.

**M.C.S.D. ONLY**

Subscriber Agreement	An Agreement used by a CA or RA setting forth the terms and conditions under which an individual or organization acts as a Subscriber.
Trusted Signatory	An employee of an organization nominated within the Subscriber Agreement who can authorize an employee of its organization to apply for a certificate.
Update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
Verification Officer	A Local registration Authority (LRA) that ensures some functions of LRA tasks, especially data verification and requests creation into the RA system.

1.6.2 Acronyms

CA	Certification Authority
CASE	Cairo and Alexandria Stock Exchanges
CMA	Capital Market Authority
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DMZ	DeMaterialized Zone
DN	Distinguish Name
FIPS	Federal Information Processing Standard
IETF	Internet Engineering Task Force
ISO	International Organization for standards
IT	Information Technology
LDAP	Lightweight directory Access Protocol
LMK	Local Master Key
LRA	Local Registration Authority
M.C.S.D.	Misr for Clearing, Settlement and Central Depository S.A.E
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RFC	Request For Comment
RSA	Rivest, Shamir, Adleman (encryption algorithm)



M.C.S.D. ONLY

SHA-1 Secure Hash Algorithm
URL Uniform Resource Locator

2 Publication and Repository Responsibilities

2.1 Repositories

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The unavailability of repositories should not exceed four (4) hours.

2.2 Publication of Certification Information

Regulation of this is given in the associated CP.

This CPS provides the following further information :

These information are related to :

- The ITIDA Root CA certificate to which the CA is subordinated.
- The CA certificate.
- Subjects' certificates.
- CRLs.

The CA CRL is accessed at the following online contact addresses :

XXX http full URL address of the CRL XXX (note : internal and external LDAP URL shall be the same to handle it on the intranet, we allocate the external URL to the internal directory IP)

The ITIDA Root CA certificate is available at the following address :

XXX http full URL address of the ITIDA Root CA certificate XXX

The MCS D CA certificate is available at the following addresses :

XXX maybe http full URL address of the MCS D CA certificate XXX

XXX ldap full URL address of MCS D CA Certificate XXX

Subject certificates are published in the LDAP directory server at XXX ldap URL address of the directory server XXX.

2.3 Time or Frequency of Publication

Regulation of this is given in the associated CP.



M.C.S.D. ONLY

This CPS provides the following further information :

Updates to this CPS or the associated CP are published within a period of seven (7) working days after final approval.

Updates to Subscriber Agreements, Subjects Agreements and Relying Party Agreements are published as necessary.

Certificates are published within a maximum period of four (4) hours after issuance.

The CRL is published every twenty-four (24) hours except if a certificate revocation occurs. In that case, a new CRL is published.

The publication time of the CRL should not exceed four (4) hours after issuance.

2.4 Access Controls on Repositories

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Information published in the repository portion of the web site is publicly-accessible information. Read-only access to such information is unrestricted.

By accessing certificates and/or CRL, persons implicitly agree to the Relying Party Agreement.

3 Identification and Authentication

3.1 Naming

3.1.1 Type of Names

Regulation of this is given in the associated CP.

3.1.2 Need for Names to be Meaningful

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The CA certificate contains names with commonly understood semantics permitting the determination of the identity of the CA that is in the *Subject* field of the certificate.

The CA Distinguished Name consists of the following components :

Attribute	Value
Country (C) =	"EG"
Organization (O) =	"MCDR MISR for Central Clearing, Depository and Registry"
Common Name (CN) =	"MCDR Certificate Authority NNN" where NNN is an empty character chain or a number

XXX Check the CA DN with ITIDA XXX

A number (e.g. year) could be added at the end of the CA Common Name for renewal purpose.

Subject certificates contain names with commonly understood semantics permitting the determination of the identity of the individual and the organization it belongs to that is in the *Subject* field of the certificate.

Subject Distinguished Names consist of the following components :

Attribute	Value	Type
Country (C) =	As defined in ISO 3166 e.g. "EG"	Mandatory
Organization (O) =	May contains one of the following : <ul style="list-style-type: none"> The legally registered name of the company for Subscriber acting on organization behalf. The established name of an individual for Subscriber acting on its own behalf. 	Mandatory
Organization Unit	May contains one of the following :	Optional



M.C.S.D. ONLY

(OU) =	<ul style="list-style-type: none"> The department or business unit name provided by the Subscriber within Subscriber acting on organization behalf. “Individual” for Subscriber acting on its own behalf. 	
Title (TITLE) =	<p>May contains one of the following :</p> <ul style="list-style-type: none"> The role played by the Subject for a Stock Exchange participant (e.g. “Broker”, “Custodian”, “Investor”, “Primary Dealer”, ...). “Employee” for M.C.S.D. employees. The role for which the Subscriber intends the certificate to be used (e.g. “Buyer”) for non-participants. 	Optional
Serial Number (serialNumber) =	<p>For M.C.S.D. Restricted Signature Certificate, this serial number is a alphanumerical combination of the Unique Participant Identifier and the national ID card Number of the subject.</p> <p>For M.C.S.D. General Signature Certificate, a alphanumeric string will be used to indicate the type of identification code to follow (e.g. “EgID:145431”)</p>	Mandatory
Common Name (CN) =	Indicates the established name of the Subject (first name, middle name(s) and surname), expressed in roman characters	Mandatory

3.1.3 Anonymity or Pseudonymity of Subjects

Regulation of this is given in the associated CP.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

Regulation of this is given in the associated CP.

3.1.6 Recognition, Authentication and Role of Trademarks

Regulation of this is given in the associated CP.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The method to prove possession of a private key shall be PKCS#10.

3.2.2 Authentication of Organization Identity

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The authentication of an organization Subscriber shall identify it in a unique and non ambiguous way and require the information specified below. The authentication is achieved through a face-to-face process with a Customer Support Officer.

The organization Subscriber provides the following information :

- The full registered name and address of the subscribing organization.
- The legal status of the subscribing organization and the number in the national commerce registry.
- The Stock Exchange registration number for CASE participants companies.
- The Subscriber Agreement duly signed by an independently verifiable Officer of the organization (e.g. listed board member).
- Full name and identification details of any Trusted Signatories and their handwriting sample signatures.
- Full name, identification details and a well-recognized form of government-issued photographic identification (such as a passport or a national identity card) of the person performing the face-to-face authentication.

Identification details for Trusted Signatories and the person performing the face-to-face include the following information :

- Full name and address.
- Date and place of birth.
- National identity number.
- Gender
- Passport style photograph

The following information may be optionally collected during the enrolment process:

- E-mail address,
- Contact telephone number,
- Unified participant code
- Unified Participant Code

All information provided by a Subscriber shall be verified by a Verification Officer.



3.2.3 Authentication of Individual Identity

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The authentication of a Subject shall identify it in a unique and non ambiguous way and require the information specified below. The authentication is achieved through a face-to-face process with a Customer Support Officer.

The Subject provides the following information :

- Full name and address.
- Date and place of birth.
- National Identity number.
-
- A well-recognized form of government-issued photographic identification, such as a passport or a national identity card.
- Limit value of transactions (this could be set to unlimited).
- Gender

The following information may be optionally collected during the enrolment process:

- E-mail address of the Subject,
- Contact telephone number,
- Unified Participant Code

If the Subject act as an employee of an organization, it shall also provide the information below :

- Role or department of the Subject within the organization Subscriber.

For issuing a Subject certificate the following information is also required :

- The Subject Agreement duly signed by the Subject and a Trusted Signatory of the organization Subscriber, if the Subject acts as an employee of an organization.
- The Subscriber Agreement and the Subject Agreement duly signed by the Subject, if the Subject acts on its own behalf.

All information provided by a Subscriber shall be verified by a Verification Officer.

3.2.4 Non-Verified Subject Information

Regulation of this is given in the associated CP.



3.2.5 Validation of Authority

Regulation of this is given in the associated CP.

This CPS provides the following further information :

For Subjects acting on behalf of an organization, Subject Agreements shall be signed by hand by a person from the Subscriber organization invested with appropriate signatory power, that is a Trusted Signatory.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-Key

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Any RA re-key request shall be initiated by the PMA in a face-to-face authentication of the requester with the CA.

3.3.2 Identification and Authentication for Re-Key After Revocation

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Any RA re-key request after revocation shall be initiated by the PMA in a face-to-face authentication of the requester with the CA.

3.4 Identification and Authentication for Revocation Requests

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Subject revocation requests can follow:

- Sending a revocation request with details of the authorization information and/or validation of identity in the form of a signed e-mail with a valid certificate to the Customer Support Officer.
- Sending a revocation request with details of the authorization information and/or validation of identity in the form of a document signed by the Subject or a Subscriber Trusted Signatory to the Customer Support Officer.
- A face-to-face authentication of the Subject requesting the revocation of its certificate with a Customer Support Officer as described in Section 3.2 without the need to provide signed Agreements.



MCS D ONLY

- For a revocation request with details of the authorization information and/or validation of identity in the form of a phone call to the Customer Support Officer.

All information provided for revocation requests shall be verified by a Verification Officer.

Subject revocation requests that cannot be verified prima facie as legitimate by the Customer Support Officer shall be confirmed by telephone by the Verification Officer with the person who signed the Subscriber Agreement or a Trusted Signatory within organization Subscriber.

For revocation requests that have not been fully authenticated, Subject certificates are suspended until the request is authenticated.

Any RA revocation request shall be initiated by the PMA in a face-to-face authentication of the requester with the CA.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Certificate application may be submitted by :

- Any individual who is the subject of the certificate.
- Any authorized representative of the RA.

4.1.2 Enrolment Process and Responsibilities

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Subjects undergo the following enrolment process :

- The Subject faces a Customer Support Officer.
- The Subject provides an application form and provides true and correct information to the Customer Support Officer (identifying information and Agreements).
 - If the subject does not act as an individual but for a subscribing organization this form should be signed by one of the trusted signatory in this organization and placed in a sealed envelope signed by this trusted signatory.
 - If the subject acts as an individual, he has to fill also the subscriber registration form.
- The Customer Support Officer checks and validates the given information (ID Card provided by the subject).
- The Customer Support Officer approves or rejects the certificate request.
- The Customer Support Officer transmits the Subject registration information to a Verification Officer.
- The Verification Officer checks and validates the Subject registration information and the appropriate Subscriber Agreement.
- The Verification Officer approves or rejects the certificate request.
- The Verification Officer authenticates himself to the RA.



M.C.S.D. ONLY

- The Verification Officer registers Subject registration information into the RA system.
- The Verification Officer transfer the Subject (and subscriber if applicable) registration information.
- The Issue and Revocation Officer authorizes or reject the certificate issuance.
- The Issue and Revocation Officer generates a public/private key pair in a smartcard for the Subject. The smartcard generates its own key pair.
- The Issue And Revocation Officer Archive the Forms (a scan copy is archived as well in another site than the paper form)
- A PKCS#10 certificate request is generated and is transmitted to the CA.
- The CA approves or rejects the certificate request.
- The CA issues the certificate.
- The CA publishes the issued certificate in the directory.
- The CA transmits the issued certificate to the RA.
- The Issue and Revocation Officer loads the certificate into the smartcard.
- The Issue and Revocation Officer prints the smartcard with the Subject's name and photograph, unique subject reference number and the name of the subscribing organization (for organization Subscriber).
- The Issue and Revocation Officer generates a new PIN code for the smartcard and monitors a secure PIN printing.
- The Issue and Revocation Officer sends the smartcard to the Customer Support Officer.
- The Customer Support Officer authenticates the Subject in a face-to-face process.
- The Customer Support Officer checks the Subject identifying information and that the Subject matches the photography on the smartcard.
- The Customer Support Officer delivers the smartcard and associated PIN code (PIN code is given to the Customer Support Officer by the Security Compliance Officer).
- The Subject signs the certificate acceptance form.
- The certificate acceptance form is archived (a scan copy is archived as well in another site than the paper form).

RA undergoes the following enrolment process :

- The RA generates a public/private key pair in the RA hardware cryptographic module and a PKCS#10 certificate request which is transmitted to the PMA (represented by one PMA member).
- The CA Operator authenticates the PMA in a face-to-face process.



MCS D ONLY

- The PMA provides true and correct information and the PKCS#10 certificate request.
- The CA Operator checks and validates the given information.
- The CA Operator approves or rejects the certificate request.
- The CA Operator authenticates itself to the CA.
- The PKCS#10 request is transmitted to the CA.
- The CA issues the certificate.
- The CA transmits the issued certificate to the PMA.
- The PMA transmits the certificate to the RA who installs the certificate in the RA system.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Regulation of this is given in the associated CP.

4.2.2 Approval or Rejection of Certificate Applications

Regulation of this is given in the associated CP.

4.2.3 Time to Process Certificate Applications

Regulation of this is given in the associated CP.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Regulation of this is given in the associated CP.

4.3.2 Notifications to Subject by the CA of Issuance of Certificate

Regulation of this is given in the associated CP.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The certificate acceptance for RA component is performed through the signature of a key ceremony document.



4.4.2 Publication of the Certificate by the CA

Regulation of this is given in the associated CP.

This CPS provides the following further information :

RA certificates may not be published to the directory.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

RA certificates shall not be used for any other functions except RA (such as signing certificate and/or revocation requests to the CA).

4.5.1 Subject Private Key and Certificate Usage

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Use of private key corresponding to the public key in the certificate shall only be permitted once Subject has agreed to the Subject Agreement and optionally the Subscriber Agreement and accepted the issued certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Regulation of this is given in the associated CP.

This CPS provides the following further information :

By accessing certificates and/or CRL, persons implicitly agree to the Relying Party Agreement.

4.6 Certificate Renewal

Regulation of this is given in the associated CP.

4.6.1 Circumstances for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subject

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.



4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.7 Certificate Re-Key

Regulation of this is given in the associated CP.

4.7.1 Circumstances for Certificate Re-Key

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Prior to the expiration of the RA certificate, it is necessary for the RA to re-key the certificate to maintain continuity of PKI services. The certificate may also be re-keyed after expiration.

4.7.2 Who May Request Certificate of a New Public Key

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Re-key requests may be submitted by :

- Any individual who is the subject of the certificate.
- Any authorized representative of the RA.

4.7.3 Processing Certificate Re-Keying Requests

Regulation of this is given in the associated CP.

4.7.4 Notification of New Certificate Issuance to Subject

See Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See Section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 Certificate Modification

Regulation of this is given in the associated CP.



4.8.1 Circumstances for Certificate Modification

Not applicable.

4.8.2 Who May Request Certificate Modification Requests

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subject

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

Regulation of this is given in the associated CP.

4.9.1 Circumstances for Revocation

Regulation of this is given in the associated CP.

4.9.2 Who Can Request Revocation

Regulation of this is given in the associated CP.

This CPS provides the following further information :

For Subjects, the revocation shall be requested by :

- The Subject holding the private key corresponding to the public key in the certificate.
- The Subscriber (or Subscriber Trusted Signatory) of the Subject certificate.
- M.C.S.D.
- The CA.
- The PMA.

For the RA, the revocation shall be requested by :

- The CA.



- The PMA.

4.9.3 Procedure for Revocation Request

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Subjects undergo the following revocation process :

- The revocation request is received by the Customer Support Officer as described in Section 3.4. The request shall contain information identifying the certificate to be revoked and the requester and the reason for revocation.
- The Verification Officer checks and validates the Subject revocation information. Subject revocation requests that cannot be verified prima facie as legitimate by the Customer Support Officer shall be confirmed by telephone by the Verification Officer with the person who signed the Subscriber Agreement or a Trusted Signatory within organization Subscriber.
- The Verification Officer approves or rejects the revocation request.
- The Verification Officer authenticates itself to the RA.
- The Verification Officer registers Subject revocation request into the RA system.
- The Verification Officer archives the Subject revocation information archived (a scan copy is archived as well in another site than the paper form).
- The Issue and Revocation Officer authorizes or rejects the revocation.
- The CA approves or rejects the revocation request.
- The CA revokes the certificate.
- The CA issue a new CRL and publishes this new CRL in the directory.

Subject revocation reasons are published.

RA undergoes the following revocation process :

- The CA Operator authenticates the PMA and the revocation information in a face-to-face process.
- The CA Operator checks and validates the given information.
- The CA Operator authenticates itself to the CA.
- The CA Operator approves or rejects the revocation request.
- The CA revokes the certificate.

It is recommended to remove the revoked keys from the hardware cryptographic module.



4.9.4 Revocation Request Grace Period

Regulation of this is given in the associated CP.

4.9.5 Time Within Which CA Must Process the Revocation Request

Regulation of this is given in the associated CP.

4.9.6 Revocation Checking Requirements for Relying Parties

Regulation of this is given in the associated CP.

4.9.7 CRL Issuance Frequency

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The CRL is published every twenty-four (24) hours except if a certificate revocation occurs. In that case, a new CRL is published immediately.

4.9.8 Maximum Latency for CRLs

Regulation of this is given in the associated CP.

4.9.9 On-Line Revocation/Status Checking Availability

Regulation of this is given in the associated CP.

4.9.10 On-Line Revocation Checking Requirements

Not applicable.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related to Key Compromise

Regulation of this is given in the associated CP.

4.9.13 Circumstances for Suspension

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Certificate suspension is not allowed for RA certificates.

4.9.14 Who Can Request Suspension

Regulation of this is given in the associated CP.

This CPS provides the following further information :

For Subjects, the suspension shall be requested by :

- The Subject holding the private key corresponding to the public key in the certificate.
- The Subscriber (or Subscriber Trusted Signatory) of the Subject certificate.



- M.C.S.D.
- The CA.
- The PMA.

4.9.15 Procedure for Suspension Request

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Subject certificates undergo the following suspension process :

- The Verification Officer determines that the suspension of a certificate is appropriate under Section 4.9.13 of the associated CP.
- The Verification Officer authenticates itself to the RA.
- The Verification Officer registers Subject suspension request into the RA system
- The Issue and Revocation Officer authorizes or reject the suspension
- The CA approves or rejects the suspension request.
- The CA suspends the certificate.
- The CA issue a new CRL and publishes this new CRL in the directory.

4.9.16 Limits on Suspension Period

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Subject certificates may be re-activated or revoked before end of suspension period.

Certificates that reach end of suspension period shall be revoked.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The status of certificates is available through LDAP directory specified in Section 2.2.

4.10.2 Service Availability

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The unavailability of repositories should not exceed four (4) hours.



MCS D ONLY

The revocation service is available from 9 am to 4 pm, Sunday to Thursday (except for public holidays). Outside of these opening hours, an answering machine will take information from the subjects allowing a CSO to call within operating hours.

PKI services availability is improved through the secure replication of CA and RA databases.

4.10.3 Optional features

No stipulation.

4.11 End of Subscription

Regulation of this is given in the associated CP.

4.12 Key Escrow and Recovery

Regulation of this is given in the associated CP.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.



5 Facility, Management and Operational Controls

5.1 Physical Controls

Regulation of this is given in the associated CP.

5.1.1 Site Location and Construction

Regulation of this is given in the associated CP.

This CPS provides the following further information :

5.1.2 Physical Access

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Access to the floor where the CA, RA and LRA are located is protected by access smartcard with printed photography and main working department of the working staff individual and is authorized to related jobs and watched by security individuals. In addition to this control, doors are protected by access control with a smartcard reader with recorded logs.

The CA equipment is located in a secure cage inside the datacenter. The door of the datacenter is protected by smartcard access control and is under video surveillance with recording operates twenty-four hours (24) a day, seven (7) days a week. The door of this secure cage is protected by smartcard and biometric access control under video surveillance with recording twenty-four hours (24) a day, seven (7) days a week. The secure cage is restricted to trusted personnel with a legitimate need to access core CA systems. Moreover, access to the Nexus CA system is authenticated through smartcard and sensitive operations require dual control.

The RA equipment and repository systems are located in the datacenter. The door of the datacenter is protected by smartcard access control and is under video surveillance. The datacenter is restricted to trusted vetted personnel engaged in CA or RA operations, systems and network maintenance and other datacenter operations.

LRA equipment for Verification Officers and Issue and Revocation Officers is located in a area protected by smartcard access control and under video surveillance. This area is restricted to trusted vetted personnel engaged in LRA operations, including Verification Officers and Issue and Revocation Officers, systems and network maintenance.

Any non-related personnel or visitors shall be identified, logged and accompanied by authorized staff. No photographic equipment is allowed in secure areas without top management's authorization.

5.1.3 Power and Air Conditioning

Regulation of this is given in the associated CP.

This CPS provides the following further information :



M.C.S.D. ONLY

Heat and humidity sensors are connected to information system. They trigger alarms at critical thresholds and send SMS mobile messages to dedicated personnel.

5.1.4 Water Exposures

Regulation of this is given in the associated CP.

5.1.5 Fire Prevention and Protection

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Fire prevention and protection measures against other damaging exposure to flame or smoke have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The following media storage carriers shall be used :

- Paper
- CD-ROMs/DVD-ROMs
- Data backup magnetic tapes
- Hardware tokens (e.g. smartcards)
- Hard disk drives

Media storage carriers shall be stored in locked cupboards in secure areas. Media carriers storing sensitive data shall be stored in a safe.

5.1.7 Waste Disposal

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Data stored on paper shall be destroyed by a document shredder. Electronic media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroized in accordance with the manufacturer's guidance prior to disposal.

5.1.8 Off-Site Backup

Regulation of this is given in the associated CP.

5.2 Procedural Controls

5.2.1 Trusted Roles

Regulation of this is given in the associated CP.



M.C.S.D. ONLY

This CPS provides the following further information :

The table below defines roles involved in the certification process. Each role is assigned particular functions. Each role also specifies the degree of knowledge (either whole or split) allowed in relation to PINs and passwords together access authorization to certain parts of the operational infrastructure (security areas, safes, secure operations rooms).

A member of staff can embody more than one role. However, it should be noted that there are roles requiring separation of duties (as described in Section 5.2.4). It is also permissible for the duties of a certain role to be distributed among a number of staff members.

Role	Function	Code
Policy Management Authority	Creation and updates of Certificate Policies. Review Certificate Practice statements and results of CA audits.	PMA
CA Manager	Overall responsibility for CA, RA and LRA operations	CAM
Customer Support Officer	Performs face-to-face process with Subscribers and Subjects. Receives applications for certificates and revocation. Identification and authentication of Subscribers and Subjects. Verification of documentation. Instruction and guidance of Subscribers and Subjects. Delivery of smartcards and PIN codes to Subjects.	CSO
Verification Officer	Verification of the completeness and accuracy of certificate and revocation applications. Verification of Subscriber and/or subject authorization. Documentation storage if applicable. Captures Subscribers and Subjects information and requests into the RA system	VO
Issue and Revocation Officer	Approval of certificate and revocation applications Managing of electrical and graphical personalization of smartcards for Subjects. Managing of secure PIN production and dispatch.	IRO
CA Operator	Access of all certification functions into the CA system. Responsible for the usage and storage of electronic data carriers on which the CA's private keys are stored.	CAO
RA Operator	Access of administration functions into the RA system. Creation of RA users (e.g. Verification Officer)	RAO
Server Officer	Installation, configuration and administration of hardware and software deployed for the PKI without access and special knowledge of the cryptographic keys and their passwords used in the certification management. Performs system and data backup. Administration of database.	SO
Network Officer	Installation, configuration and administration of network systems.	NO



M.C.S.D. ONLY

Security Compliance Officer	Definition and ensuring compliance with the data security regulations. Manages physical security and access to the PKI system and issues authorization. Monitor audit logs and provides security audit reports. Supervise key ceremony.	SCO
LMK holder	Holder of a part of the secret of the hardware cryptographic module.	LMKH

5.2.2 Number of Persons Required per Task

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Task	Required roles	Comments
Installation of PKI hardware and software	SO	NO may also be needed.
Initialization of the hardware cryptographic module of the CA or RA	PMA, LMKH (5), SCO	
Generation/renew/revocation of CA keys and certificate	PMA, CAO (2), SCO	Dual control for CAO.
Initialization of CA processes for issuance of certificates and CRL	CAO (2)	Dual control for CAO.
Generation/renew/revocation of RA keys and certificate	PMA, CAO, RAO, SCO	
Reconstruction of the LMK of the CA or RA	PMA, LMKH (3), SCO, CAM	
Data backup	SO	
Restoration of backup data of the CA or RA	SO, SCO, CAO, RAO	CAO allows for CA restoration. RAO allows for RA restoration.
Restoration of backup data for other systems	SO, SCO	
Archive of CA or RA data	SO, SCO	
Audit	SCO	
Issuance of physical authorizations	SCO, CAM	
Technical issuance of authorizations	SO, SCO, CAM	Monitor by ISO.
Development of operational/security principles	SCO	
Initiation and termination of processes (e.g. server, backup)	SO	



M.C.S.D. ONLY

Verification of registration data of the CA or RA	PMA	CAO allows for CA restoration. RAO allows for RA restoration.
Verification of registration/revocation data of Subscribers and Subjects	CSO, VO	
Storage of Subscriber and Subject documents	VO	May be transmitted to ISO for archive.
Capture of Subscriber and Subject information into the RA system	VO	
Generation of keys, certificate and PIN code for Subjects	IRO	
Delivery of Smart Card to subjects	CSO	
Revocation of Subject certificates	IRO	

5.2.3 Identification and Authentication for Each Role

Regulation of this is given in the associated CP.

This CPS provides the following further information :

A smartcard and the associated PIN code is delivered to authorized personnel who may perform CA, RA or LRA operations. The smartcard allows to be identified and authenticated into the CA or RA system.

User account and password may be also provided if required.

5.2.4 Roles Requiring Separation of Duties

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The following table shows roles requiring separation of duties :

Roles	Incompatible with
PMA – Policy Management authority	CSO, VO, IRO, CAO, RAO, SO, NO, CAM, SCO
CAM – CA Manager	CSO, VO, IRO, CAO, RAO, SO, NO, PMA, SCO
CSO – Customer Support Officer	PMA, VO, IRO, CAO, RAO, SO, NO, SCO, CAM
VO – Verification Officer	PMA, CSO, IRO, CAO, RAO, SCO, CAM
IRO – Issue and Revocation Officer	PMA, CSO, SCO, CAO, RAO, SO, NO, VO, CAM



M.C.S.D. ONLY

CAO – CA Operator	PMA, SCO, CSO, VO, IRO, CAM Because of dual control CAOs shall be at least two different individuals.
RAO – RA Operator	PMA, SCO, CSO, VO, IRO, CAM
SO – Server Officer	PMA, SCO, CSO, VO, IRO, CAM
NO – Network Officer	PMA, SCO, CSO, VO, IRO, CAM
SCO – Security Compliance Officer	SO, NO, CAO, RAO, VO, IRO, CSO, PMA, CAM
LMKH – LMK Holder	

5.3 Personnel Controls

5.3.1 Qualifications, Experience and Clearance Requirements

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Depending on the role they fulfill, personnel have knowledge of the following fields :

- IT security technology, cryptography, electronic signatures, PKI,
- TCP/IP networks, relational databases, operating systems,
- General security, ISO17799, BS7799-2,
- National and international laws, responsibilities of different parties described in Agreements.

5.3.2 Background Check Procedures

Regulation of this is given in the associated CP.

5.3.3 Training Requirements

Regulation of this is given in the associated CP.

5.3.4 Retraining Frequency and Requirements

Regulation of this is given in the associated CP.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Regulation of this is given in the associated CP.

This CPS provides the following further information :

In matters of criminal liability the proper authorities shall be notified.

5.3.7 Independent Contractor Requirements

Not applicable.

5.3.8 Documentation Supplied to Personnel

Regulation of this is given in the associated CP.

5.4 Audit Logging Procedures

Regulation of this is given in the associated CP.

5.4.1 Types of Events Recorded

Regulation of this is given in the associated CP.

This CPS provides the following further information :

If events could not be recorded directly through the information system, these events are recorded in a paper form. This is the case, for instance, for hardware maintenance.

The systems requiring such record of events are CA and RA systems, not LRA systems.

5.4.2 Frequency of Processing Log

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Any exceptional events may receive special monitoring.

5.4.3 Retention Period of Audit Log

Regulation of this is given in the associated CP.

5.4.4 Protection of Audit Log

Regulation of this is given in the associated CP.

This CPS provides the following further information :

On computers, electronic audit logs are protected by the system that has generated them. When outside computers, paper document and electronic media are stored in locked cupboards or safe in secure areas with access control.

5.4.5 Audit Log Backup Procedures

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Incremental audit logs are backup daily and full backups are performed weekly.

A copy of the full backup shall be performed.

5.4.6 Audit Collection system (Internal or External)

Regulation of this is given in the associated CP.



5.4.7 Notification to Event-Causing Subject

Regulation of this is given in the associated CP.

5.4.8 Vulnerability Assessments

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Audit log analysis is the responsibility of the Information Security Compliance Officer (SCO). This analysis allows to underline :

- The relationship between an anomaly and its cause/author. This could lead to either re-training or sanctions of the concerned personnel.
- The relationship between an anomaly and the type of action that leads to the anomaly or between an anomaly and its time of occurrence. This could end to either updates of processes or updates of protection measures.

If an anomaly is noticed in any audit logs, it is recommended to perform a comparison between CA and RA audit logs, operating system audit logs and manual audit logs in order to verify the concordance between dependant events.

Critical anomalies, that could lead to an interruption of PKI services or the revocation of the CA certificate, shall be noticed to the PMA.

5.5 Records Archival

5.5.1 Types of Records Archived

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The following type of recorded are archived :

- CA and RA system equipment configuration files.
- The CP.
- The full CPS.
- Any contractual Agreements to which the CA is bound duly signed (Subscriber, Subject, Relying Parties Agreements, ITIDA Root CA) (paper form and scanned version).
- Any mail duly signed by the PMA requesting for CA certificate and/or revocation application.
- Key ceremony documents duly signed (paper form and scanned version).
- Audit logs (electronic media and paper).
- All issued or published certificates.



- CRLs.
- Subject and Subscriber identification and authentication information.
- Certificate and revocation requests.
- Requests to obtain and verify archived information.

5.5.2 Retention Period for Archive

Regulation of this is given in the associated CP.

This CPS provides the following further information :

All archives described above are archived for a minimum period of 5 years except for CA and RA equipment configuration files which are archived as long as the version of the files are valid and running on the CA/RA system.

5.5.3 Protection of Archive

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Paper documents and electronic media are archived in locked cupboards or safe in secure areas with access control. Scanned copies of paper documents are stored in another site.

The media holding the archive data and the applications required to process the archive data shall be maintained to ensure that the archive data can be accessed for the time period set forth in this CPS.

Protection of the integrity of media is performed by the use of suitable media with regard to retention period requirements.

5.5.4 Archive Backup Procedures

Regulation of this is given in the associated CP.

5.5.5 Requirements for Time-Stamping of Records

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Date and time on CA and RA systems is synchronised to a time server.

Date and time written on paper document are evidence.

After archive, date and time are protected by the use of non-rewritable media.

5.5.6 Archive Collection System (Internal or External)

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Archive collection systems are internal.



5.5.7 Procedure to Obtain and Verify Archive Information

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The Security Compliance Officer (CSO) is invested with the authority for downloading and verification of archived data.

The request to obtain and verify archive information shall also be archived and include the identity of the requester, the description of data to be recovered, the reason and date of the request, the identity of the person performing the data recovery and the date of delivery of recovered data. This request shall be signed by the requester and the person performing the data recovery.

5.6 Key Changeover

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The CA's private signing keys are changed periodically. The overlap time of the keys is at least the validity period of a Subject certificate. Three (3) months prior to this overlap time the CA shall generate a new key pair and request a certificate for it through a key ceremony.

RA certificates are renewed at the same time as CA certificates.

The changeover of the CA keys doesn't affect Subjects. Overlapping mechanisms are implemented in order that the changeover of the CA keys doesn't imply Subject certificate revocation.

If the changeover of the CA keys is due to compromise, Subjects shall not use their certificates after notification and should obtain new certificates as soon as the PKI system will run with new certificates.

The CA shall not issue certificates that extend beyond the expiration date of its own certificate

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Procedures for handling breaches of security and the compromising of CA's private keys are given in the Business Continuity Policy. Basic elements of the procedures are given in the following sections.

5.7.2 Computing Resources, Software and/or Data Are Corrupted

Regulation of this is given in the associated CP.

This CPS provides the following further information :



MCS D ONLY

Computing equipment of the CA and RA system are equipped with higher availability hardware such as RAID hard disk drives or redundant hardware cryptographic module.

The Information Security Officer (ISO) shall verify that software and data backup procedures are correctly done.

Hardware equipment allows quick change of malfunctioning hardware.

Should the existence of malfunctioning or manipulated computing resources, software, and/or data be ascertained within the CA or RA, recovery is done using redundant hardware, software backup and/or data backup.

If required, additional protective measures will also be put in place to prevent the occurrence of similar incidents in the future. Should corrupted data be found in any certificate, the certificate Subject will be immediately notified and the certificate immediately revoked.

5.7.3 Entity Private Key Compromise Procedures

Regulation of this is given in the associated CP.

5.7.4 Business Continuity Capabilities After a Disaster

Regulation of this is given in the associated CP.

This CPS provides the following further information :

MCDR has developed a Business Continuity Policy and associated procedures to handle various forms of disasters.

5.8 CA or RA Termination

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Upon receipt of CA termination notification, subjects shall not use anymore their certificates.



6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Regulation of this is given in the associated CP.

This CPS provides the following further information :

CA generates their own key pairs with the hardware cryptographic module Thales SafeSign Crypto Module. The signing key pair of the CA is a RSA key pair. Other CA key pairs may be generated for internal CA uses such as signing audit log.

RA generates their own key pairs with the hardware cryptographic module Thales SafeSign Crypto Module and requests a certificate to the CA. The key pair of the RA is a RSA key pair.

Key pairs of CA, RA are RSA key pairs and are generated by the smartcard.

Subject smartcards generate their own key pairs.

6.1.2 Private Key Delivery to CA component

Not applicable.

6.1.3 Private Key Delivery to Subject

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Private key is delivered to Subject through the delivery of the smartcard storing the key pair and certificate in a face-to-face process with the Customer Support Officer. Prior to the delivery, the Subject is identified and authenticated.

6.1.4 Public Key Delivery to Certificate Issuer

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The public key is delivered through the delivery of a certificate request signed with the private key corresponding to the public key. The certificate request is PKCS#10 package.

RA PKCS#10 request is transferred to the CA through the network or a media that can contain electronic data such as a floppy disk, a CD-ROM or an USB key.

Subject PKCS#10 requests are extracted from the smartcard and send to the CA through the network.



6.1.5 CA Public Key Delivery to Relying Parties

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The root CA and CA public key are available to Relying Party using an X.509 certificate in a PKCS#7 package. They can also be downloaded from the LDAP directory. The CA certificate is also available in the LDAP directory.

The CA certificate is delivered to Subject on the Subject smartcard.

6.1.6 Key Sizes

Regulation of this is given in the associated CP.

6.1.7 Public Key Parameters Generation and Quality Checking

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The hardware cryptographic module shall check the quality of key pairs it generates.

6.1.8 Key Usage Purposes (as per X.509 V3 Key Usage Field)

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The signing key of the CA is the only key permitted for signing certificates and CRLs and has keyCertSign and CRLSign key usage bits set.

Any other key of the CA used for internal purposes such as signing audit logs shall have only Digital Signature and Non-Repudiation key usage bits set.

Subject keys may be used for authentication, non-repudiation and digital signature and have Digital Signature and Non-Repudiation key usage bits set.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The cryptographic module Thales SafeSign Crypto Module used by CA and RA components uses RSA and SHA-1 algorithms in accordance with their standardization :

- RSA : ANSI X 9-31 and PKCS#1 v2.1 standards
- SHA-1 : FIPS PUB 180-1 and ANSI X9.30 (part 2) standards

MCSD ONLY

Smartcards used by Subjects shall use RSA and SHA-1 algorithms in accordance with their standardization :

- RSA : ANSI X 9-31 and PKCS#1 v2.1 standards
- SHA-1 : FIPS PUB 180-1 and ANSI X9.30 (part 2) standards

6.2.2 Private Key (3 out of 5) Multi-Person Control

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The PMA and the Information Security Officer (ISO) shall be present for private key control of CA or RA component.

Private keys in the cryptographic module Thales SafeSign Crypto Module are protected in confidentiality with a local master key (LMK). The LMK shall be present in the cryptographic module to generate or recover private keys.

On first generation, the LMK is generated inside the cryptographic module Thales SafeSign Crypto Module and is split on five (5) smartcards. The LMK is shared by five (5) secret holders.

To prevent loss, each smartcard containing a part of the LMK is backed up.

The LMK shall only be restored under control of three shareholders, each owning a smartcard containing a part of the LMK.

Upon generation or recovery of the LMK, CA or RA private keys can be generated or recovered inside the cryptographic module Thales SafeSign Crypto Module.

In the Nexus CA software, sensitive operations related to CA keys such as creation, modification, removal of CA keys, require dual CA Operator control.

6.2.3 Private Key Escrow

Regulation of this is given in the associated CP.

6.2.4 Private Key Backup

Regulation of this is given in the associated CP.

This CPS provides the following further information :

CA and RA private keys stored inside the cryptographic module Thales SafeSign Crypto Module are exported from the cryptographic module encrypted by the LMK. These encrypted keys are stored on a non-rewritable media such as CD-ROM in duplicate. Each media storing the encrypted keys is protected in integrity by organisational measures and is stored in a safe on site and off-site.

Subject private keys are not backed-up.

6.2.5 Private Key Archival

See Section 6.2.3.

No CA and/or RA private keys are archived beyond the end of validity of the associated certificate.

Subject private keys are not archived.

6.2.6 Private Key Transfer Into or Form a Cryptographic Module

Regulation of this is given in the associated CP.

This CPS provides the following further information :

RA private keys shall be transferred into a cryptographic module for the same reasons and following the same process as for CA private keys.

In the event that a private key shall be transported from one cryptographic module Thales SafeSign Crypto Module to another, the private key shall be encrypted by the LMK during transport and require the use of three (3) smartcards containing a part of the LMK out of five (5) and so the presence of three (3) key shareholders out of five (5). Prior to the transfer into a cryptographic module Thales SafeSign Crypto Module of the encrypted private key, the LMK is introduced into the cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

Regulation of this is given in the associated CP.

This CPS provides the following further information :

CA and RA private keys held on the cryptographic module Thales SafeSign Crypto Module are stored encrypted by the LMK.

6.2.8 Method of Activating Private Key

Regulation of this is given in the associated CP.

This CPS provides the following further information :

CA and RA private keys held on the cryptographic module Thales SafeSign Crypto Module are activated when they are generated or when they are introduced into the cryptographic module with the LMK that encrypted the private keys.

CA private keys need also to be activated under dual CA Operator control through Nexus CA software.

Subject private keys are activated with PIN codes.

6.2.9 Method of Deactivating Private Key

Regulation of this is given in the associated CP.

This CPS provides the following further information :

CA and RA private keys held on the cryptographic module Thales SafeSign Crypto Module are deactivated when the cryptographic module power is cut or when keys are deleted from the cryptographic module. The reasons for deletion are :

- On request from the cryptographic module Operator.
- On intrusion detection.
- On temperature change indicating a possible attack.
- On abnormal removal of the cryptographic module.



M.C.S.D. ONLY

CA private keys could be deactivated under dual CA Operator control through Nexus CA software.

Subject private key are deactivated when the smartcard is removed from the smartcard reader and blocked after three (3) wrong PIN code attempts.

6.2.10 Method of Destroying Private Key

Regulation of this is given in the associated CP.

This CPS provides the following further information :

CA and RA private keys held on the cryptographic module Thales SafeSign Crypto Module are destroyed when private keys are erased from the module or when the module is reset and all media storing a backup of private keys are destroyed.

If CA private keys are destroyed through Nexus CA software under dual CA Operator control, all media storing a backup of private keys shall be destroyed.

Subject private key are destroyed when the key is erased from the smartcard or when the chip of the smartcard is cut in two.

6.2.11 Cryptographic Module Rating

Regulation of this is given in the associated CP.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Regulation of this is given in the associated CP.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Key usage periods for keying material is as follow :

- The CA public key is valid **6 years**.
- The CA private key is valid **6 years**.
- The RA public key is valid **3 years**.
- The RA private key is valid **3 years**.
- Subject public key is valid **3 years**.
- Subject private key is valid **3 years**.

6.4 Activation Data



6.4.1 Activation Data Generation and Installation

Regulation of this is given in the associated CP.

This CPS provides the following further information :

During the initialization of the CA and/or RA cryptographic module Thales SafeSign Crypto Module, smartcards used to stored a part of the LMK are protected with a six (6) digits PIN code. This PIN code is chosen by the future holder of the smartcard. The CA and/or RA cryptographic module Thales SafeSign is also configured so that access to its administration functions require strong authentication through a Crypto Officer smartcard protected with a six (6) digits PIN code. An organisational process requests dual operator to perform administration functions : one of the operator hold the smart card and the other one the PIN number.

Subject smartcard are protected with a PIN code. The PIN code is generated during smartcard personalization in a random way and write down in a sealed envelope. The sealed envelope is delivered to the Subject in a face-to-face process at the same time the smartcard is delivered.

6.4.2 Activation Data Protection

Regulation of this is given in the associated CP.

This CPS provides the following further information :

CA and RA activation data shall never be disclosed and may only be made know to members of personnel who required them for the execution of their duties. A record in writing is permissible for backup purposes and is store in a safe in a secure area with access control at the entrance. The use of such stored activation data shall be the subject of a request to the Information Security Officer (ISO).

6.4.3 Other Aspects of Activation Data

Regulation of this is given in the associated CP.

This CPS provides the following further information :

PIN codes of smartcards used to stored a part of the LMK are composed of at least six (6) digits. cryptographic module Thales SafeSign Crypto Module smartcards are locked after three (3) wrong PIN code attempts.

Subject PIN codes are composed of at least four (4) alphanumeric characters. Subject smartcards are locked after three (3) wrong PIN code attempts.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Security technical requirements on PKI equipments are described in M.C.S.D. PKI Security Policy document.

LRA equipments do not require key pairs for running. LRA are authenticated by the RA through certificates of their Operators



M.C.S.D. ONLY

Access to the operating system of PKI equipments require the use of non-privileged accounts except when administrator privileges are required. Each Operator owns a specific user account with sufficient privileges to perform its PKI duties.

Access control of Operators for each PKI component is done through an authentication to the operating system and, in addition, a smartcard strong authentication to the software.

Operating system right access is managed through a user account name and a password. Password shall be composed in accordance with M.C.S.D. Security Charter

A certificate is delivered on a smartcard to PKI trusted personnel in order to be identified and authenticated into the PKI system for the duties they need to perform.

Operators are registered in a face-to-face process in order to be properly identified and authenticated.

Operator keys may be used for authentication, non-repudiation and digital signature and have Digital Signature and Non-Repudiation key usage bits set.

Operators shall periodically obtains new keys and re-establishes their identity. Operators certificates shall not be used for any other functions except authentication to the PKI system

Operator keys could be generated for backup purposes. In that case, Operator smartcards and the associated PIN codes shall be stored in a safe in a secure area with access control at the entrance. The use of such smartcards shall be the subject of a request to the PMA.

There are at least two (2) CA Operators. CA Operator key pair are valid 5 years.

There is at least one (1) RA Operators. RA Operator key pair are valid 5 years.

There are at least two (2) LRA Operators: one Verification Officer and one Issue and Revocation Officer. LRA Operator key pair are valid 5 years.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Activity of PKI components is monitored in order to anticipate required updates such as increased storage capacity.

6.6.2 Security Management Controls

Regulation of this is given in the associated CP.

This CPS provides the following further information :



M.C.S.D. ONLY

Security management controls include internal and external audits, regular inspection and upgrades of the security system and software, checking security measures during on-going operations.

CA equipment is dedicated to CA functions. PKI equipment changes or upgrades are performed by trusted personnel.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Network security controls are in accordance with the M.C.S.D. PKI Security Policy document.

The network of the PKI system is divided into various security zones which are all separated from one another by firewalls. Firewalls are configured to allow network traffic only on an authorized communication matrix restricted to required protocols. Backbone network traffic is monitored in real-time when required for detection of unauthorized activities, intrusion attempts and compromised equipment.

The CA is located in a dedicated subnet protected with firewall which is not accessible from outside world. The CA can only transfer or receive data to or from the RA. The CA can also transfer data to the repository through two firewalls.

The RA is located in a subnet, different from the CA one, protected with firewall which is not accessible from outside world.

The external repository is located in a DMZ, isolated from M.C.S.D. network through strict filtering components.

6.8 Time-Stamping

Regulation of this is given in the associated CP.

7 Certificate, CRL and OCSP Profiles

7.1 Certificate Profile

Regulation of this is given in the associated CP.

This CPS provides the following further information :

For certificate extension QcStatement, there is no limit value.

For certificate extension CertificatePolicies, the PolicyIdentifier field is the OID of this CPS.

7.1.1 Version Number(s)

Regulation of this is given in the associated CP.

7.1.2 Certificate Extensions

Regulation of this is given in the associated CP.

7.1.3 Algorithm Object Identifiers

Regulation of this is given in the associated CP.

7.1.4 Name Forms

Regulation of this is given in the associated CP.

This CPS provides the following further information :

DN are in accordance with Section 3.1.2.

7.1.5 Name Constraints

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Name constraints are in accordance with Section 3.1

7.1.6 Certificate Policy Object Identifier

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The certificate Policy OID is specified in Section 1.2.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

Regulation of this is given in the associated CP.



M.C.S.D. ONLY

This CPS provides the following further information :

The URL of the CPS is specified in Section 2.2.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Regulation of this is given in the associated CP.

7.2 CRL Profile

Regulation of this is given in the associated CP.

7.2.1 Version Number(s)

Regulation of this is given in the associated CP.

7.2.2 CRL and CRL Entry Extensions

Regulation of this is given in the associated CP.

7.3 OCSP Profile

7.3.1 Version Number(s)

Not applicable.

7.3.2 OCSP Extensions

Not applicable.



8 Compliance Audit and Other Assessments

8.1 Frequency and Circumstances of Assessment

Regulation of this is given in the associated CP.

8.2 Identify/Qualifications of Assessor

Regulation of this is given in the associated CP.

8.3 Assessor's Relationship to Assessed Entity

Regulation of this is given in the associated CP.

8.4 Topics Covered by Assessment

Regulation of this is given in the associated CP.

This CPS provides the following further information :

The topics of a compliance audit include technical and organizational processes and trusted personnel involved in PKI operations and management of PKI equipments. They include CA, RA and LRA equipments, Nexus CA and SafeSign Management software.

8.5 Actions Taken as a Result of Deficiency

Regulation of this is given in the associated CP.

8.6 Communications of Results

Regulation of this is given in the associated CP.



9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Regulation of this is given in the associated CP.

9.1.2 Certificate Access Fees

Regulation of this is given in the associated CP.

9.1.3 Revocation or Status Information Access Fees

Regulation of this is given in the associated CP.

9.1.4 Fees for Other Services

Regulation of this is given in the associated CP.

9.1.5 Refund Policy

Regulation of this is given in the associated CP.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Regulation of this is given in the associated CP.

9.2.2 Other Assets

Regulation of this is given in the associated CP.

9.2.3 Insurance or Warranty Coverage for End-entities

Regulation of this is given in the associated CP.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Regulation of this is given in the associated CP.

This CPS provides the following further information :



M.C.S.D. ONLY

The following information are considered confidential :

- Identifying information of Subscribers and Subjects except that which is bound into the certificate.
- Identifying information of PKI components except that which is bound into the certificate.
- Private keys of PKI components and Subjects.
- Activation data of PKI components and Subjects.
- PKI components' audit logs and reports.
- Disaster recovery plans.
- Sensitive information of this CPS.
- CA and RA data backups.
- Spare system hard drive containing replication of operational data.

A list of the personnel or type of personnel that could access such information should be specified by the PMA or Security Compliance Officer (ISO). It is specified in M.C.S.D. Access Control Policy.

9.3.2 Information Not Within the Scope of Confidential Information

Regulation of this is given in the associated CP.

This CPS provides the following further information :

Information which are not considered confidential are :

- Certificates.
- CRL.
- Revocation status information.
- Information contained within repositories.
- Spare system hard drive containing only the operating system and basic software.

9.3.3 Responsibility to Protect Confidentiality Information

No stipulation.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Regulation of this is given in the associated CP.

9.4.2 Information Treated as Private

Regulation of this is given in the associated CP.



9.4.3 Information Not Deemed Private

Regulation of this is given in the associated CP.

9.4.4 Responsibility to Protect Private Information

Regulation of this is given in the associated CP.

9.4.5 Notice and Consent to Use Private Information

Regulation of this is given in the associated CP.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Regulation of this is given in the associated CP.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

Regulation of this is given in the associated CP.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Regulation of this is given in the associated CP.

9.6.2 RA/LRA Representations and Warranties

Regulation of this is given in the associated CP.

9.6.3 Subject Representations and Warranties

Regulation of this is given in the associated CP.

9.6.4 Subscriber Representations and Warranties

Regulation of this is given in the associated CP.

9.6.5 Relying Party Representations and Warranties

Regulation of this is given in the associated CP.

9.6.6 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

Regulation of this is given in the associated CP.



9.8 Limitations of Liability

Regulation of this is given in the associated CP.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This CPS shall remain in effect until either a new CPS is approved by the PMA and published in the repository or the PKI is terminated.

9.10.2 Termination

This CPS shall survive any termination of the CA. The requirements of this CPS shall remain in effect through the end of the archive period.

9.10.3 Effect of Termination and Survival

The responsibilities for protecting confidential and private information and M.C.S.D.'s intellectual property rights shall survive the termination of this CPS.

9.11 Individual Notices and Communications with Participants

Regulation of this is given in the associated CP.

9.12 Amendments

9.12.1 Procedure for Amendment

Errors, updates or suggested changes to this CPS shall be communicated to the contact in Section 1.5.2. Such communication shall include a description of the change, a change justification and contact information for the person requesting the change.

Minor changes to this CPS that do not materially affect the assurance level of this CPS are indicated by version number that contains a decimal number e.g. version 1.2 for a version with minor changes as opposed to version 2.0 that addresses major issues.

All versions of this CPS shall be reviewed and approved by the PMA.

Revised versions shall be published on a web site and be disseminated to interested parties (PKI components, Subscribers and Subjects, ...).

9.12.2 Notification Mechanism and Period

The PMA reserve the right to amend this CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and change to contact information. The PMA shall designate whether amendments are material or non-material.



MCS D ONLY

The PMA may request the CA to notify its PKI components, Subscribers and Subjects of material amendments to this CPS. The notification shall contain a statement of proposed changes, the comment period and the proposed effective date of change. Proposed amendments shall be published on a web site.

Except as otherwise stated, the comment period for any material amendments to this CPS shall be thirty (30) days.

Written and signed comments on proposed changes shall be directed to the PMA. Decisions with respect to the proposed changes are at the sole discretion of the PMA.

The PMA shall accept, accept with modification or reject the proposed change after completion of the review period. The PMA will determine the period for final change notice.

9.12.3 Circumstances Under Which OID Must be Changed

The PMA shall determine whether changes to the CPS require a change in the CPS OID.

9.13 Dispute Resolution Provisions

Regulation of this is given in the associated CP.

9.14 Governing Law

The laws of Egypt shall govern this CPS.

9.15 Compliance with Applicable Law

Regulation of this is given in the associated CP.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If a section of this CPS is determined incorrect or invalid by a court of law or other tribunal having authority, the other sections of this CPS shall remain valid until the policy is updated.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.



9.17 Other Provisions

No stipulation.