STCS IDENTITY CA

CERTIFICATION PRACTICE STATEMENT

Document Classification : Public

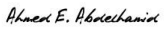
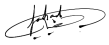
Version Number : 1.3

Issue Date: 23 December 2019

Copyright © 2019 Saudi Telecom Company Solutions. This document is intended for use only by STC Solutions and authorized participants. This document shall not be duplicated, used, or disclosed in whole or in part for any purposes without prior consent.

Document Reference

Item	Description
Document Title:	STCS Identity CA Certificate Practice Statement
Custodian Department:	STCS Cybersecurity
Owner:	STCS PA
Version Number:	1.3
Document Status:	Final

Author(s):	Katekani Hlabathi Security Consultant	 Signature/Date
Reviewer:	Ahmed E. Abdelhamid STCS Cybersecurity Advisory	 Signature/Date
Official Reviewer:	Mohamed A. Breik STCS Cybersecurity Advisory	Signed by: Mohamed A. Breik Signed at: 2019-12-23 18:29:06 Reason: Witnessing Mohamed A. Signature/Date
Approved by:	Fahad I. Aljutaily STCS Cybersecurity VP (STCS PKI Committee Chair)	Signed by: faljutaily Signed at: 2019-12-23 22:04:27 Reason: Witnessing faljutaily  Signature/Date

Document Revision History

Version	Date	Author(s)	Revision Notes
1.0	22/11/2019	Katekani Hlabathi	Initial standalone version
1.1	28/11/2019	Katekani Hlabathi	Final version after review
1.2	18/12/2019	Katekani Hlabathi	Final for approval and publishing
1.3	23/12/2019	Katekani Hlabathi	Added signatory. For approval and publishing

Document Control

This document shall be reviewed annually and an update by STCS may occur earlier if internal or external influences affect its validity.

Digitally Signed Copy of this document shall be stored at STCS Document Store.

Table of Contents

1 Introduction 10

1.1 Overview 10
1.1.1 Certificate Policy 11
1.1.2 Relationship between the CP and the CPS 11
1.1.3 Scope 11

1.2 Document Name and Identification 12

1.3 PKI Participants 12
1.3.1 STCS Public Key Infrastructure services (STCS PKI) 12
1.3.2 STCS Intermediary CA 13
1.3.3 STCS Identity CA (STCS IDCA) 13
1.3.4 Registration Authority (RA) 13
1.3.5 STCS Policy Authority (STCS PA) 14
1.3.6 STCS PKI Committee 14
1.3.7 Subscribers 14
1.3.8 Relying Parties 14
1.3.9 Online Certificate Status Protocol Responder 14

1.4 Certificate Usage 15
1.4.1 Appropriate Certificate Uses 15
1.4.2 Prohibited Certificate Uses 15

1.5 Policy Administration 16
1.5.1 Administration Organization 16
1.5.2 Contact Person 16
1.5.3 Person Determining CPS Suitability for the Policy 16
1.5.4 CPS Approval 16

1.6 Definitions and Acronyms 16

2 Publication and Repository Responsibilities 17

2.1 Repositories 17
2.1.1 Repository Obligations 17

2.2 Publication of Certification Information 17
2.2.1 Publication of Certificates and Certificate Status 17
2.2.2 Publication of CA Information 18

2.3 Time or Frequency of Publication 18

2.4 Access Controls on Repositories 18

3 Identification and Authentication 19

3.1 Naming 19
3.1.1 Types of Names 19
3.1.2 Need for Names to be Meaningful 19
3.1.3 Anonymity or Pseudonymity of Subscribers 19
3.1.4 Rules for Interpreting Various Name Forms 19
3.1.5 Uniqueness of Names 19
3.1.6 Recognition, Authentication and Role of Trademarks 20

3.2 Initial Identity Validation 20
3.2.1 Method to Prove Possession of Private Key 20
3.2.2 Identity-Proofing of organization Identity 20
3.2.3 Identity-Proofing of Individual Identity 21
3.2.4 Non-verified Subscriber Information 21

3.2.5 Validation of Authority 21
3.2.6 Criteria of Interoperation 22

3.3 Identification and Authentication for Re-key Requests 22
3.3.1 Identification and Authentication for Routine Re-Key 22
3.3.2 Identification and Authentication for Re-key After Revocation 22

3.4 Identification and Authentication for Revocation Requests 22

4 Certificate Life-Cycle Operational Requirements 24

4.1 Certificate Application 24
4.1.1 Submission of Certificate Application 24
4.1.2 Enrollment Process and Responsibilities 24

4.2 Certificate Application Processing 25
4.2.1 Performing Identity-proofing Functions 25
4.2.2 Approval or Rejection of Certificate Applications 25
4.2.3 Time to Process Certificate Applications 25

4.3 Certificate Issuance 26
4.3.1 CA Actions During Certificate Issuance 26
4.3.2 Notification of Certificate Issuance 26

4.4 Certificate Acceptance 26
4.4.1 Conduct Constituting Certificate Acceptance 26
4.4.2 Publication of the Certificate by the CA 27
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 27

4.5 Key Pair and Certificate Usage 27
4.5.1 Subscriber Private Key and Certificate Usage 27
4.5.2 Relying Party Public Key and Certificate Usage 27

4.6 Certificate Renewal 28
4.6.1 Circumstances for Certificate Renewal 28
4.6.2 Who may request Certificate Renewal 28
4.6.3 Processing Certificate Renewal Requests 28
4.6.4 Notification of Renewed Certificate Issuance 28
4.6.5 Conduct constituting acceptance of a renewal certificate 28
4.6.6 Publication of a Renewal Certificate 28
4.6.7 Notification of Certificate Issuance by the CA to Other Entities 29

4.7 Certificate Re-Key 29
4.7.1 Circumstances for Certificate Re-key 29
4.7.2 Who can Request a Certificate Re-key 29
4.7.3 Processing Certificate Re-keying Requests 29
4.7.4 Notification of Re-Keyed Certificate Issuance to Subscriber 29
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 30
4.7.6 Publication of the Re-keyed Certificate by the CA 30
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 30

4.8 Certificate Modification 30

4.9 Certificate Revocation and Suspension 30
4.9.1 Circumstance for Revocation of a Certificate 30
4.9.2 Who Can Request Revocation of a Certificate 31
4.9.3 Procedure for Revocation Request 31
4.9.4 Revocation Request Grace Period 32
4.9.5 Time within which CA must Process the Revocation Request 32
4.9.6 Revocation Checking Requirements for Relying Parties 32
4.9.7 CRL Issuance Frequency 32

4.9.8 Maximum Latency of CRLs 32
4.9.9 Online Revocation Checking Availability 33
4.9.10 Online Revocation Checking Requirements 33
4.9.11 Other Forms of Revocation Advertisements Available 33
4.9.12 Special Requirements Related To Key Compromise 33
4.9.13 Circumstances for Certificate Suspension 33
4.9.14 Who Can Request Suspension 33
4.9.15 Procedure for Suspension Request 33
4.9.16 Limits on Suspension Period 34
4.9.17 Circumstances for Terminating Suspended Certificates 34
4.9.18 Procedure for Terminating the Suspension of a Certificate 34

4.10 Certificate Status Services 34

4.11 End of Subscription 34

4.12 Key Escrow and Recovery 35

5 Facility Management and Operational Controls 36

5.1 Physical Security Controls 36
5.1.1 Site Location and Construction 36
5.1.2 Physical Access 36
5.1.3 Power and Air Conditioning 36
5.1.4 Water Exposure 37
5.1.5 Fire Prevention and Protection 37
5.1.6 Media Storage 37
5.1.7 Waste Disposal 37
5.1.8 Off-Site Backup 37

5.2 Procedural Controls 37
5.2.1 Trusted Roles 37
5.2.2 Number of Persons Required per Task 38
5.2.3 Identification and Authentication for Each Role 38
5.2.4 Separation of Roles 38

5.3 Personnel Controls 38
5.3.1 Background, Qualifications and Experience Requirements 38
5.3.2 Background Check and Clearance Procedures 38
5.3.3 Training Requirements 39
5.3.4 Retraining Frequency and Requirements 39
5.3.5 Job Rotation Frequency and Sequence 39
5.3.6 Sanctions for Unauthorized Actions 39
5.3.7 Contracting Personnel Requirements 39
5.3.8 Documentation Supplied to Personnel 39

5.4 Audit Logging Procedures 40
5.4.1 Types of Events Recorded 40
5.4.2 Frequency of Processing Data 41
5.4.3 Retention Period for Audit Log 41
5.4.4 Protection of Audit Log 41
5.4.5 Audit Log Backup Procedures 41
5.4.6 Audit Collection System (Internal or External) 41
5.4.7 Notification to Event-Causing Subject 41
5.4.8 Vulnerability Assessments 42

5.5 Records Archival 42
5.5.1 Types of Events Archived 42
5.5.2 Retention Period for Archive 42
5.5.3 Protection of Archive 42

5.5.4 Archive Backup Procedures 43
5.5.5 Requirements for Time-Stamping of Records 43
5.5.6 Archive Collection System (Internal or External) 43
5.5.7 Procedures to Obtain and Verify Archive Information 43
5.6 Key Changeover 43
5.7 Compromise and Disaster Recovery 43
5.7.1 Incident and Compromise Handling Procedures 43
5.7.2 Computing Resources, Software, and/or Data Are Corrupted 44
5.7.3 CA Private Key Compromise Recovery Procedures 44
5.7.4 Business Continuity Capabilities after a Disaster 44
5.8 CA OR RA Termination 45
5.8.1 CA Termination 45
5.8.2 RA Termination 45
6 Technical Security Controls 46
6.1 Key Pair Generation and Installation 46
6.1.1 Key Pair Generation 46
6.1.2 Private Key Delivery to Subscribers 46
6.1.3 Public Key Delivery to Certificate Issuer 46
6.1.4 CA Public Key Delivery to Relying Parties 47
6.1.5 Key Sizes 47
6.1.6 Public Key Parameters Generation and Quality Checking 47
6.1.7 Key Usage Purposes 47
6.2 Private Key Protection and Crypto-Module Engineering Controls 48
6.2.1 Cryptographic Module Standards and Controls 48
6.2.2 Subscriber Private Key Multi-Person Control 48
6.2.3 Private Key Escrow 48
6.2.4 Private Key Backup 48
6.2.5 Private Key Archival 48
6.2.6 Private Key Transfer Into or From a Cryptographic Module 48
6.2.7 Private Key Storage on Cryptographic Module 48
6.2.8 Method of Activating Private Keys 48
6.2.9 Methods of Deactivating Private Keys 48
6.2.10 Methods of Destroying Private Keys 49
6.2.11 Cryptographic Module Rating 49
6.3 Other Aspects of Key Pair Management 49
6.3.1 Public Key Archive 49
6.3.2 Certificate Operational Periods and Key Usage Periods 49
6.4 Activation Data 49
6.4.1 Activation Data Generation and Installation 49
6.4.2 Activation Data Protection 49
6.4.3 Other Aspects of Activation Data 49
6.5 Computer Security Controls 49
6.5.1 Specific Computer Security Technical Requirements 49
6.5.2 Computer Security Rating 50
6.6 Life-Cycle Security Controls 50
6.6.1 System Development Controls 50
6.6.2 Security Management Controls 50
6.6.3 Life Cycle Security Ratings 51
6.7 Network Security Controls 51

6.8 Time Stamping 51

7 Certificate, CRL and OCSP Profiles 52

7.1 Certificate Profile 52
7.1.1 Version Numbers 52
7.1.2 Certificate Extensions 52
7.1.3 Algorithm Object Identifiers 52
7.1.4 Name Forms 52
7.1.5 Name Constraints 52
7.1.6 Certificate Policy Object Identifier 53
7.1.7 Usage of Policy Constraints Extension 53
7.1.8 Policy Qualifiers Syntax and Semantics 53
7.1.9 Processing Semantics for the Critical Certificate Policy Extension 53

7.2 CRL Profile 53
7.2.1 STCS Identity CA CRL Profile 53
7.2.2 Version Numbers 53
7.2.3 CRL and CRL Entry Extensions 53

7.3 OCSP Profile 54
7.3.1 Version Number 54
7.3.2 OCSP Extensions 54

8 Compliance Audit and Other Assessments 55

8.1 Frequency of Audit or Assessments 55

8.2 Identity and Qualifications of Assessor 55

8.3 Assessor's Relationship to Assessed Entity 55

8.4 Topics Covered By Assessment 55

8.5 Actions Taken As A Result of Deficiency 56

8.6 Communication of Results 56

9 Other Business and Legal Matters 57

9.1 Fees 57
9.1.1 Certificate Issuance/Renewal Fee 57
9.1.2 Certificate Access Fees 57
9.1.3 Revocation or Status Information Access Fee 57
9.1.4 Fees for Other Services 57
9.1.5 Refund Policy 57

9.2 Financial Responsibility 57
9.2.1 Insurance Coverage 57
9.2.2 Other Assets 57
9.2.3 Insurance/warranty Coverage for End-Entities 57

9.3 Confidentiality of Business Information 58
9.3.1 Scope of Confidential Information 58
9.3.2 Information not within the Scope of Confidential Information 58
9.3.3 Responsibility to Protect Confidential Information 59

9.4 Privacy of Personal Information 59
9.4.1 Privacy Plan 59
9.4.2 Information Treated as Private 59
9.4.3 Information not Deemed Private 59
9.4.4 Responsibility to Protect Private Information 59
9.4.5 Notice and Consent to Use Private Information 59

9.4.6 Disclosure Pursuant to Judicial/Administrative Process 59
9.4.7 Other Information Disclosure Circumstances 60
9.5 Intellectual Property Rights 60
9.6 Representations and Warranties 60
9.6.1 STCS INDENTITY CA Representations and Warranties 60
9.6.2 RA Representations and Warranties 61
9.6.3 Relying Parties Representations and Warranties 61
9.6.4 Subscriber Representations and Warranties 61
9.7 Disclaimers of Warranties 62
9.8 Limitations of Liability 62
9.9 Indemnities 63
9.10 Term and Termination 63
9.10.1 Term 63
9.10.2 Termination 63
9.10.3 Effect of Termination and Survival 63
9.11 Individual Notices and Communications with Participants 64
9.12 Amendments 64
9.12.1 Procedure for Amendment 64
9.12.2 Notification Mechanism and Period 64
9.12.3 Circumstances under which OID must be changed 64
9.13 Dispute Resolution Procedures 64
9.14 Governing Law 64
9.15 Compliance with Applicable Law 65
9.16 Miscellaneous Provisions 65
9.16.1 Entire Agreement 65
9.16.2 Assignment 65
9.16.3 Severability 65
9.16.4 Enforcement (Attorney Fees/Waiver of Rights) 65
9.16.5 Force Majeure 65
9.17 Other Provisions 65
9.17.1 Fiduciary Relationships 65
9.17.2 Administrative Processes 66
Appendix-A: Certificate Types 67
A.1 Certificate types supported 67
A1.1 Digital Identity Certificate Service (IDS) 67
A.1.2 RA Identity Certificate (RA Certificate) 72
A.1.3 Online Certificate Status Protocol Certificate (OCSP Certificate) 73

1 INTRODUCTION

This Certification Practice Statement (CPS) establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by the STCS Identity Certification Authority. In particular, this CPS establishes the processes and procedures the STCS Identity CA follows to:

- Issue National Center for Digital Certification (NCDC) compliant certificates to the STCS Issuing Certificate Authorities that it signs,
- Manage certificate life cycle for the Subscriber certificates issued under this STCS Identity CA hierarchy; and
- Operate a directory of issued Subscriber certificates; and
- Operate the CRL directory.

The STCS Identity CA is owned by STCS and operates under the Saudi National Root-CA. This is achieved by the Saudi National Root-CA issuing a digitally signed CA Certificate that authenticates the Public Key of the STCS Identity CA.

The STCS Identity CA is hosted in the STCS data centre which is responsible for managing the STCS Identity CA operations.

This CPS complies with the Saudi National PKI Certificate Policy and in line with Internet Request for Comment (RFC) 3647 [RFC 3647]. Sections that are not applicable to STCS Identity CA are labelled “No Stipulation”

1.1 OVERVIEW

This Certification Practice Statement (CPS) establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by the STCS Identity CA as governed by the STCS Identity CA Certificate Policy (STCS Identity CA CP).

More specifically, this CPS describes the practices that the STCS Identity CA employs for:

- Securely managing the core infrastructure that supports the PKI hosted at the STCS data centre, and
- Issuing, managing, revoking and renewing subscriber certificates
- The technical, procedural and personnel management in accordance with the requirements of the STCS Identity CA CP.

Any use of or reference to this CPS outside the context of the STCS Identity CA and Saudi National PKI is completely at the using party’s risk. The terms and provisions of STCS Identity CA CPS shall be interpreted under and governed by the STCS Identity CA CP and STCS Operations Policies and Procedures.

It is the responsibility of all parties applying for or using a Digital Certificate issued under the STCS Identity CA CPS, to read the STCS Identity CP and the PKI Disclosure Statement (PDS) to understand the practices established for the lifecycle management of the Certificates issued by the STCS Identity CA.

1.1.1 CERTIFICATE POLICY

X.509 certificates issued by the STCS Identity CA to sub-CAs will contain a registered OID in the certificate policy extension that in turn shall be used by a Relying Party (RP) to decide whether a certificate is trusted for a particular purpose.

1.1.2 RELATIONSHIP BETWEEN THE CP AND THE CPS

This CPS establishes the practices for the issuance, acceptance, maintenance, use, reliance upon, and revocation of digital certificates issued by STCS Identity CA as governed by the STCS Identity CA CP and related documents which describe STCS Identity CA requirements and use of Certificates.

1.1.3 SCOPE

This CPS applies to certificates issued by the STCS Identity CA.

STCS operates a Public Key Infrastructure Services (STCS PKI) under the Saudi National Root CA. The STCS PKI has core offerings of public key infrastructure (PKI) services and digital trust services designed to enable electronic signature for business entities and individuals. To achieve this goal, the STCS PKI operates a publicly chained Intermediary CA that is chained to the Saudi National Root CA that is operated by the NCDC.

Under the STCS Intermediary CA, there are Sub-CA Issuing Certificate Authorities (Sub-CAs) that issue certificates to end subscribers, herein referred to as Issuing CAs. The two Issuing CAs are the STCS Qualified CA (STCS QUCA) and the STCS Identity CA (STCS IDCA). The full hierarchy of the STCS PKI is indicated in Figure 1.

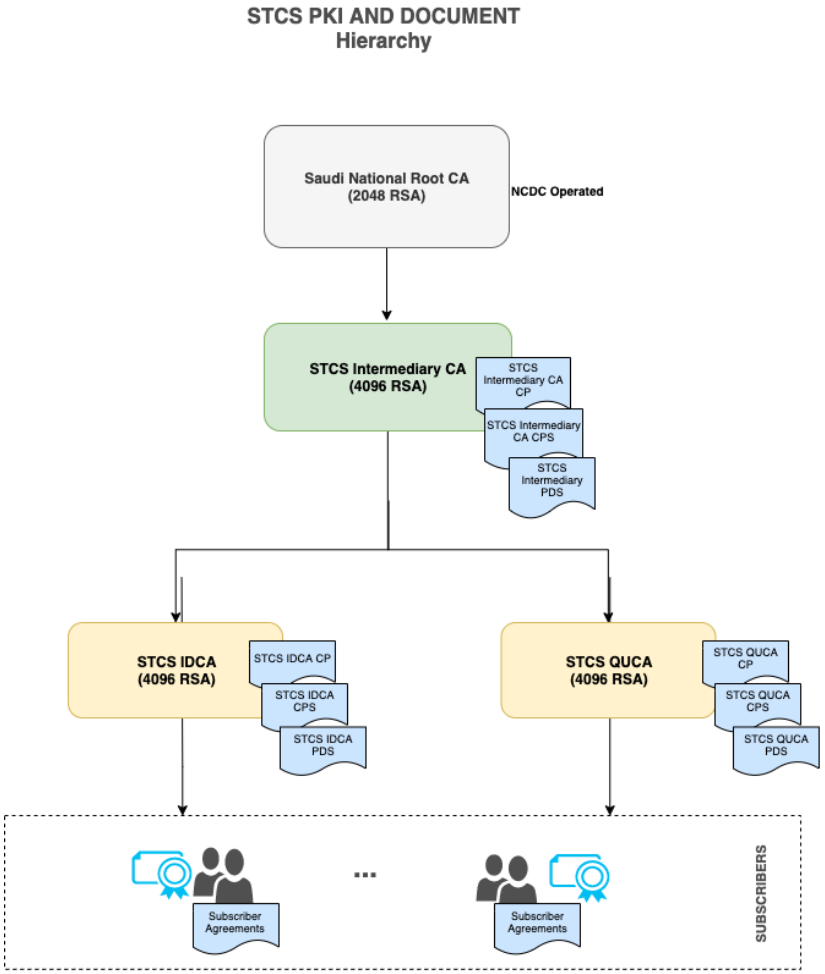


Figure 1. STCS PKI and Governance Hierarchy

1.2 Document Name and Identification

This document is the STCS Identity CA Certification Practice Statement (CPS), and is identified by the following object identifier (OID):

OID: 2.16.682.1.101.5000.1.4.1.2.1.22

1.3 PKI Participants

The following are roles relevant to the administration and operation of the STCS Identity CA under the STCS Identity CA CPS.

1.3.1 STCS Public Key Infrastructure services (STCS PKI)

The STCS PKI is an umbrella term referring to the STCS as an organization that runs PKI services under the Saudi National Root-CA. The STCS PKI implements a three-tier PKI Architecture consisting of an offline intermediate CA (STCS Intermediary CA), and two Issuing CA's under it, these being the STCS Qualified CA (STCS QUCA) and STCS Identity CA (STCS IDCA). These Issuing CAs will issue subscriber certificates, OCSP responder certificates and other certificates required by PKI components. The Issuing CAs will issue certificates to Subscribers in accordance with each respective Issuing CA's CP and corresponding CPS,

their RA Agreement, Subscriber Agreement, Relying Party Agreement, and the Saudi National PKI Policy.

STCS as an entity is responsible for:

- Control over the designation of CAs and RAs;
- Performance of all aspects of the services, operations and infrastructure related to the STCS PKI.
- Conduct regular internal security audits;
- Assist in audits conducted by or on behalf of NCDC; and

1.3.2 STCS INTERMEDIARY CA

The STCS Intermediary CA is an offline CA that is chained to the Saudi National Root. It issues certificates to the Issuing CAs underneath in the PKI hierarchy, including this STCS Identity CA.

1.3.3 STCS IDENTITY CA (STCS IDCA)

The STCS Identity CA is an online Issuing CA that is chained to the STCS Intermediary CA, which in turn is chained to the Saudi National Root CA. It issues authentication certificates used to identify subscribers. The subscribers can be individuals or organizational entities.

1.3.4 REGISTRATION AUTHORITY (RA)

STCS Identity CA may, in addition to issuing certificates itself, appoint Registration Authorities (RAs) to perform the Subscriber Identification and Authentication and Certificate request and revocation functions defined in this CPS and related documents.

The Registration Authority (RA) is obligated to perform certain functions pursuant to an RA Agreement including the following:

- Process Certificate application requests in accordance with this CPS, STCS Identity CA CPS and applicable RA Agreement, and other policies and procedures with regard to the Certificates issued;
- Maintain and process all supporting documentation related to the Certificate application process;
- Process Certificate Revocation requests in accordance with STCS Identity CA CP and CPS, applicable RA Agreement, and other relevant operational policies and procedures with respect to the Certificates issued. Without limitation to the generality of the foregoing, the RA shall request the revocation of any Certificate that it has approved for issuance according to the stipulations in this CPS;
- Comply with the provisions of its RA Agreement and the provisions of the STCS Identity CA CP and CPS including, without limitation to the generality of the foregoing, compliance with any compliance audit requirements; and
- Follow STCS Privacy Policy in accordance with STCS Identity CA CP and CPS and applicable RA Agreement.

1.3.5 STCS POLICY AUTHORITY (STCS PA)

The STCS Policy Authority (STCS PA) is an assigned role responsible for the development, maintenance of the STCS PKI Policies, amongst other duties.

1.3.6 STCS PKI COMMITTEE

The STCS PKI Committee is responsible for the approval of PKI Policies and overseeing the security operations of the STCS PKI. The members of this committee are appointed by the VP of the Cybersecurity unit of STCS.

1.3.7 SUBSCRIBERS

Subscribers are individuals (end users) or entities (organizations) to whom certificates are issued. Subscribers are bound by the conditions of use of certificates as contained in the Subscriber Agreement. In general, the subscriber asserts that he or she uses the key and certificate in accordance with the STCS Identity CP and this CPS.

1.3.8 RELYING PARTIES

A Relying Party in this context is the entity that relies on the validity of the binding of the STCS Identity CA (and signed Issuing CAs) identity to a public key. The Relying Party is responsible for checking the validity of the certificate by examining the appropriate certificate status information, using validation services provided by the STCS Identity CA. A Relying Party's right to rely on a certificate issued under this CPS, requirements for reliance, and limitations thereon, are governed by the terms of the STCS Identity CA CP and the Relying Party Agreement.

Relying Parties shall use the Saudi National PKI, and rely on a certificate that has been issued under the STCS Identity CA CP if:

- The certificate has been used for the purpose for which it has been issued, as described in the STCS Identity CA CP
- The Relying Party has verified the validity of the digital certificate, using procedures described in the Relying Party Agreement;
- The Relying Party has accepted and agreed to the Relying Party Agreement at the time of relying on the certificate; it shall be deemed to have done so by relying on the certificate; and
- The relying party accepts in totality, the certificate policy applicable to the certificate, which can be identified by reference of the certificate policy OID mentioned in the certificate.

1.3.9 ONLINE CERTIFICATE STATUS PROTOCOL RESPONDER

- Online Certificate Status Protocol (OCSP) Responders and Simple Certificate Validation Protocol (SCVP) status providers may provide revocation status information or full certification path validation services respectively. The STCS Identity CA may make their Certificate status information available through an OCSP responder in addition to any other mechanisms they wish to employ. The STCS Identity CA shall publish status information for the certificates it issues in a Certificate Revocation List (CRL).

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

STCS Identity CA (STCS IDCA) issues Subscriber certificates used for Identification purposes. The certificates can be used to authenticate the subscriber to services and applications requiring the use of certificates as an additional method for authentication.

The STCS IDCA issues certificates under this CPS only to those Subscribers who have signed their acceptance of a Subscriber Agreement in the appropriate form and whose application for certificates has been approved by the CA.

The following level of assurance are offered to applicants in the form of end entity certificates issued by the STCS IDCA. The Level of Assurance is in line with levels described in the Saudi National PKI Policy.

Assurance Level	Description of Assurance Level
Low Assurance Certificates	These certificates provide a low level of assurance to publicly available products and services. These certificates provide little confidence in the accuracy or legitimacy of the claimed identity. It requires a no or low level of binding between the claimed identity of the entity named in the certificate and the subscriber. It is intended for subscribers handling information of little or no value.
Medium Assurance Certificates	The certificates issued at this level provide medium confidence in the accuracy or legitimacy of the claimed identity. Identity assertions at this level are appropriate for transactions with serious or substantial consequences to Relying Parties. Identity at this level is verified with authoritative sources.
High Assurance Certificates	The certificates issued at this level provide high confidence in the accuracy or legitimacy of the claimed identity. It is intended of subscribers handling information of high value and that can have catastrophic consequences to Relying Parties. Identities at this level is verified with authoritative sources on the basis of a face to face or equivalent method.

1.4.2 PROHIBITED CERTIFICATE USES

Certificates issued under this CPS are not authorized for use in any circumstances or in any application which could lead to death, personal injury or damage to property, or in conjunction with on-line control equipment in hazardous environments such as in the operation of nuclear facilities, aircraft navigation or communications systems, air traffic control or direct life support machines, and the STCS Identity CA shall not be liable for any claims arising from such use.

1.5 POLICY ADMINISTRATION

1.5.1 ADMINISTRATION ORGANIZATION

This CPS is administered by the STCS Policy authority (STCS PA) and is based on policies established under the STCS Identity CA CP (see section 1.3.1).

1.5.2 CONTACT PERSON

Queries regarding STCS Identity CA CPS shall be directed at:

Email: 909@stc.com.sa

Telephone: 909

Any formal notices required by this CPS shall be sent in accordance with the notification procedures specified in section 9.12.2 of this CPS.

1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE POLICY

The STCS PA is responsible for ensuring approval of this CPS and establishing that the STCS Identity CA conforms to the requirements of the STCS Identity CA CP in accordance with policies and procedures specified by STCS.

1.5.4 CPS APPROVAL

The CPS shall be effective upon approval by the STCS PKI Committee. Procedure for approval and amendments are covered under section 9.12.1 of this CPS.

1.6 DEFINITIONS AND ACRONYMS

The terms used in this document shall have the meanings as defined in the prevailing CABForum Baseline Requirements (www.cabforum.org)

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The STCS Identity CA issued certificates and certificate revocation lists (CRLs) will be published in repositories. STCS shall operate Repositories to support the STCS Identity CA operations. The repositories shall be directories that provide access through the Lightweight Directory Access Protocol (LDAP) and through HTTP. Repositories may reside on dedicated directories or may be part of a separate directory that serves broader purposes than just supporting the PKI.

STCS operates repositories to support operations on a 24x7 basis.

2.1.1 REPOSITORY OBLIGATIONS

The repository capabilities that STCS will deploy shall include:

- LDAP Directory Server System that is also accessible through the Lightweight Directory Access Protocol (LDAP, version 3) or Hypertext Transfer Protocol (HTTP);
- Availability of the information as required by the certificate information posting and retrieval stipulations of this CPS and STCS Identity CA CP; and
- Access control mechanisms when needed to protect repository availability and information.

The STCS Identity CA shall post CRLs to an LDAP directory and/or an HTTP-based web server. STCS has instituted access controls, including strong authentication of authorized Relying Parties, to promote consistent access to STCS INDENTITY CA issued certificates and CRLs and to prevent modification or deletion of information.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 PUBLICATION OF CERTIFICATES AND CERTIFICATE STATUS

The STCS Identity CA maintains repositories that allow Relying Parties to make on-line enquiries regarding revocation and other certificate status information. STCS Identity CA shall be providing Relying Parties with information on how to find the appropriate repository to check certificate status and, if OCSP (Online Certificate Status Protocol) is available, how to find the appropriate OCSP responder. This information shall be published on the CA repository https://www.stcs.com.sa/repository and included in the certificate itself.

STCS Identity CA repositories shall contain the following PKI related elements:

- Subscriber certificates: Subscriber certificates shall be made publicly available; and
- CRLs: CRLs shall be made publicly available to allow relying parties to verify the status of certificates.

The STCS PA will decide on directory access restrictions to prevent misuse and unauthorized harvesting of information

2.2.2 PUBLICATION OF CA INFORMATION

The CPS shall be made available to all STCS Identity CA PKI Participants at STCS website https://www.stcs.com.sa/repository. This web site is the only source for up-to-date documentation and STCS Identity CA reserves the right to publish newer versions of the documentation without prior notice.

Additionally, the STCS Identity CA will publish an approved, current and digitally signed version of its CP and PDS.

2.3 TIME OR FREQUENCY OF PUBLICATION

Certificates are published promptly following their generation and issuance. CRL publication is in accordance with section 4.9.7 of the STCS Identity CA CP. Other certificate status information is published in accordance with the provisions of this CPS.

Updates to this CPS are published in accordance with section 9.12.2 of this CPS.

This CPS and any subsequent changes should be made available to the participants as set forth in section 2.2.2 within two weeks of approval by the STCS PKI Committee.

2.4 ACCESS CONTROLS ON REPOSITORIES

Certificates and certificate status information in the repository shall be made available to the STCS PKI participants and other parties on a 24X7 basis as determined by the applicable agreements and STCS Privacy Policy, and subject to routine maintenance.

STCS will protect repository information not intended for public dissemination or modification through the use of strong authentication, access controls, and an overall Information Security Management System that prevents unauthorized access to information.

The controls employed by STCS shall prevent unauthorized persons from adding, deleting or modifying repository entries. Access restrictions shall be implemented on directory search to prevent misuse and unauthorized harvesting of information.

This CP and accompanying PDS and CPS documents are provided as public documents and not subject to access control restrictions.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

Each Certificate must have a unique identifiable Distinguished Name (DN) according to the X.500 standard. Naming conventions for STCS Identity CA are approved by the STCS PKI Committee.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

The subject name contained in certificates issued by the STCS Identity CA must ensure association exists between the name and the entity to which it belongs.

The Distinguished name (DN) of certificates and CRLs issued under the STCS Identity CA shall have the Issuer field of set to the following (LDAP Notation):

CN=STCS IDCA, O=STCS, C=SA

The common name in the Subscriber DN will represent the Subscriber in a way that is easily understandable for humans. The certificate types supported by the STCS Identity CA are covered in Appendix-A of this document.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

The STCS Identity CA may not issue anonymous or pseudonymous certificates.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

STCS Identity CA shall only use Uniform Resource Indicators (URIs) in accordance with the applicable Internet Engineering Task Force (IETF) standards. Subject Alternative Name forms are interpreted in accordance with applicable ISO and IETF Standards. The following table provides the rules for interpreting the various name forms.

Name Form	Standard
DN	X.500
URL	RFC-1738
Internet e-mail address	RFC-822
DNS	RFC-1034

3.1.5 UNIQUENESS OF NAMES

All distinguished names shall be unique across the STCS Identity CA. After a subscriber certificate expires or is revoked, the name can be re-used to re-issue a new certificate to the same subscriber.

The STCS Identity CA will be configured in such a manner as to enforce name uniqueness for certificates that it issues. The STCS Identity CA is responsible for ensuring name uniqueness

in subscriber certificates issued by it. Additional naming attributes for uniquely identifying the subject include serial number, email, etc.

3.1.6 RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS

Certificate applicants are prohibited from using names in their certificate application that infringe upon the Intellectual Property Rights of others. The STCS Identity CA and its RAs, however, does not verify whether a certificate applicant has Intellectual Property Rights in the name appearing in a certificate application.

The STCS Identity CA may revoke a Certificate upon receipt of a properly authenticated order from NCDC, an arbitrator, or court of competent jurisdiction requiring the revocation of a Certificate or Certificates containing a Subject name in dispute.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

The STCS Identity CA generates keys on secure cryptographic tokens for subscribers. The generation of the keys are in control of the subscribers. The Private key corresponding to the certificate is held securely within the token and never leaves the protection mechanisms provided by the secure token. A self-signed PKCS#10 certificate signing request (CSR) is generated by the token for the STCS Identity CA.

Software keys are generated using trustworthy computing equipment. If generated by the subscriber, the subscriber shall generate the keys in trustworthy systems and provide a self-signed certificate signing request in PKCS#10 format.

The STCS Identity CA shall inspect the contents of the CSR during the signing process and confirm that the details match those in the certificate application documentation. At minimum the following details shall be inspected to confirm the correctness thereof:

- Subject Distinguished Name (DN)
- Acceptable Key lengths and Algorithms

3.2.2 IDENTITY-PROOFING OF ORGANIZATION IDENTITY

The STCS IDCS shall verify the identity of an organization, and the applicant's authority to request certificates on behalf of the organization, in accordance with procedures set forth in this CPS.

If the subject of the certificate is to include the organization's name or address of the organization, the STCS Identity CA or RA, as the case may be, shall verify the identity and address of the organization. The organization's address shall also be verified to confirm if it is the same address where the organization conducts its operation. The CA or RA shall verify these details using documentation provided by the applicant or verifying against any of the following:

- A government agency within the jurisdiction of the organization's legal existence or recognition;

- A third-party database that is periodically updated and considered a reliable data source
- A site visit by the CA, RA or third party who is acting on behalf of the CA; or
- An attestation letter written by a lawyer, a judge or other third party that is customarily relied upon for such information

The RAs shall act in accordance with this CPS and all STCS Identity CA collateral documentation. In doing so, it will comply with the corresponding practices, procedures and policies described therein.

For collection and verification of information provided by the certificate subscriber applicant, RAs shall follow the processes based on the certificate type requirements defined by the STCS Identity CA. The applicable process is defined in Appendix-A of this CPS.

3.2.3 IDENTITY-PROOFING OF INDIVIDUAL IDENTITY

STCS Identity CA is responsible for the identification and authentication of Subscribers. This process is performed by the RAs. The RAs will ensure that the applicant's identity information is verified in accordance with the STCS Identity CA requirements defined in this CPS.

The RAs shall act in accordance with this CPS and all STCS Identity CA collateral documentation. In doing so, it will comply with the corresponding practices, procedures and policies described therein.

The type of authentication process to be followed will depend on the type of certificate applied for. STCS Identity CA offers three types of certificates:

- Low Level of Assurance Certificates – will verify email of the applicant
- Medium Level of Assurance Certificates – in addition to Low Level, requires a Government or National Issued Identity document
- High Level of Assurance Certificates – In addition to requirements in Medium Assurance also face to face or in-person verification. Other features such as biometrics are also verified.

Detailed requirements for the different certificate types are provided in Appendix-A in this document.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

Non-verified information shall not be included in certificates issued under STCS Identity CA, unless specifically mentioned in the Certificate Types section in Appendix-A of the CPS.

3.2.5 VALIDATION OF AUTHORITY

The STCS Identity CA or RA shall, before certificate issuance, ensure that the applicant has specific rights, entitlements or permissions to obtain a certificate on behalf of the organization that is the subject of the certificate.

The following information shall be submitted by the applicant and verified by the STCS Identity CA or RA:

- Letter of authority from an authorized representative of the organization, giving permission to the applicant to apply for the certificate
- Proof of Identity (e.g. national Identity document) of the applicant.
- Email address of the applicant, if it is to be included, shall be verified
- Contact details in the letter of authority shall be provided and verified by communicating, via a reliable means, to confirm that the applicant represents the organization.

3.2.6 CRITERIA OF INTEROPERATION

No stipulation.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY

Subscribers are required to obtain new key pairs at least once every three years. (The usage periods for CA and Subscriber private keys are described in section 6.3.2.) During the Re-keying process the STCS Identity CA will create a new certificate with the same characteristics as the old certificate but with a new and different key pair and serial number. This new certificate may be given a new validity period or use the validity period that appeared in the old certificate.

When it has been less than three (3) years since the time the Subscriber was identified by the RA, the STCS Identity CA will authenticate an electronic request for a new certificate using the currently valid certificate issued to the Subscriber by the STCS Identity CA.

Where it has been longer than three (3) years from the time that the Subscriber's identity has been authenticated, then the Subscriber certificate re-key will follow the same procedures as the initial certificate issuance process.

For routine re-key of RA Certificate refer to STCS Operations Policies and Procedures.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

If a Subscriber Certificate is revoked, the Subscriber shall go through the same initial identity-proofing process as per respective certificate type to obtain a new certificate.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

Prior to the revocation of a Subscriber certificate, the STCS Identity CA shall verify that the revocation has been requested by an entity authorized to request revocation.

Acceptable procedures for authenticating the revocation requests include:

- Having the Subscriber submit a Challenge Phrase (or the equivalent thereof), and revoking the Certificate automatically if it matches the Challenge Phrase (or the equivalent thereof) on record;
- Receiving a message from a Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked; or

- Communication with the requesting entity to provide reasonable assurances that the person or organization requesting revocation is who they claim to be. Such communication, depending on the circumstances, may include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

If a secure request for revocation is received, the certificate status should be put in Suspend mode, until further verification is carried out.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The RA will perform the following steps when an applicant applies for a certificate:

- Establish the applicant's authorization to obtain a certificate;
- Establish and record the identity of the applicant; and
- Transmit to the STCS Identity CA a confirmation that the Applicant has met the authentication requirements and the information which is to appear in the Certificate.

The STCS Identity CA will perform the following steps when it receives the confirmation and certificate information from the RA:

- Verify that the transmission is from an authorized RA;
- Verify the private key ownership by the applicant. This can be achieved by verifying the signature and information in the PKCS#10 request.
- Generate the Certificate relating to that Applicant; and
- Transmits the Certificate to the Applicant and/or to the requesting RA.

Communication between the STCS Identity CA and the RA are authenticated and protected from modification through the use of digitally signed messages and by requiring the CA and RA to validate the integrity and authenticity of the messages. These communications are transmitted via a secure protocol. Where shared secrets are transmitted electronically, these transmissions are conducted over encrypted channels using cryptographic mechanisms that are commensurate with the strength of the public/private key pair being used. Any out-of-band communications will protect the confidentiality and integrity of the data.

4.1.1 SUBMISSION OF CERTIFICATE APPLICATION

Subscriber certificate applicants, including those applying for a device or entity certificate, will follow the application process specified in Appendix-A of this document, including complying with identity proofing requirements in section 3.2.3

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

4.1.2.1 Subscriber Certificates

Subscriber certificate applicants shall agree to the terms of the Subscriber Agreement and undergo an enrollment process consisting of:

- Completing a Certificate Application and providing true and correct information;
- Providing identity proof and fulfilling the requirements of the applicable certificate type as defined in Appendix-A
- Generating, or arranging to have generated, a key pair;
- Delivering his/her public key to the RA; and
- Demonstrating possession of the private key corresponding to the public key delivered to the RA, as specified in section 3.2.1 of this CPS.

4.1.2.2 RA Certificates

An entity wishing to become RA under the STCS Identity CA shall agree to the terms of the RA Agreement as part of the application process. The RA applicants shall provide their credentials to demonstrate their identity and contact information during the application process. The private key for RA certificates shall be generated by the CA in accordance with the Operations Procedures.

All applicants shall agree to the terms and conditions of the applicable Agreement, such as: Subscriber Agreement, Relying Party or Registration Authority Agreement. Identification and Authentication process is described in the CPS under section 3.2.3.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTITY-PROOFING FUNCTIONS

RAs shall perform identification and authentication of all required Subscriber information as described in section 3.2.3 of this CPS.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

The RA will approve an application for a subscriber certificate if the following criteria are met;

- Successful identification and authentication of all required Subscriber information as described in the Subscriber Agreement and outlined in section 3.2 of this CPS.

The RA will reject a certificate application if:

- Identification and authentication of all required Subscriber information as described in the Subscriber Agreement cannot be completed;
- The Subscriber fails to furnish supporting documentation upon request;
- The Subscriber fails to respond to notices within a specified time; or
- The RA believes that issuing a certificate to the Subscriber may bring the STCS Identity CA into disrepute.

Policies specific to each certificate type have been detailed in the Certificate Types section in Appendix-A of this CPS. It is mandatory to comply with all policies specific to the respective certificate type.

For RA certificate under STCS Identity CA, the CA shall ensure that its RA which is applying for certification meets the entitlement requirements for RA certification. Detailed procedure is described in STCS Operations Policies and Procedures.

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

Certification applications is processed within a commercially reasonable time in accordance with the CPS or any agreement signed with the PKI participants. The STCS Identity CA shall not be held liable for any processing delays initiated by the applicant or for events outside the CA's control.

4.3 CERTIFICATE ISSUANCE

When the RA receives a request for certificate from a Subscriber, the RA will:

- Verify the identity of the Subscriber;
- Verify the authority of the requestor and the integrity of the information in the certificate request;
- Ensure the subscriber signs the Subscriber Agreement, and
- Verify that the subscriber possesses the private key corresponding to the certificate signing requests, for subscriber generated keys
- Submit the certificate request to the STCS Identity CA.

Upon receiving a validated certificate request from RA, the STCS Identity CA will create and sign the Subscriber certificate and deliver it to the Subscriber using a secure method.

All authorization and other attribute information received from an applicant are verified before inclusion in the certificate, unless such verification is not required for specific attributes, identifiers, and/or Certificate Types in Appendix-A of this CPS. The STCS Identity CA, through its RA, is responsible for verifying the data to be included in the Certificate. At a minimum the RA will follow the steps described in section 3.2 of the STCS Identity CA CP and this CPS.

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

Following successfully completion of the registration process, the STCS Identity CA will create and sign the subscriber certificate if all certificate requirements have been met and make the certificate available to the requesting party. The following actions shall be performed by the STCS Identity CA

- Verify the source and authenticity of the request
- Inspect the contents of the CSR to ensure accuracy
- Sign the certificate signing request
- Notify the requesting party of the availability of the certificate

4.3.2 NOTIFICATION OF CERTIFICATE ISSUANCE

The STCS IDENTITY shall notify Subscribers, either directly or through the RA that they have created the Subscriber Certificate and provide Subscribers with access to the Certificates by notifying them, using the email address provided during application, that their Certificates are available. For in-person applications, notification may also take the form of verbal notification.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

Certificate acceptance is governed by the agreements set out between the RA and Applicants, any requirements imposed by STCS Identity CA CP, this CPS and the relevant agreements under which the certificate is being issued.

The use of a Certificate or the reliance upon a Certificate signifies acceptance by that person of the terms and conditions of the CP, this CPS and applicable agreements by which they irrevocably agree to be bound.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

The Subscriber certificates will be published, once accepted, in the appropriate repository as described in section 2.1 of this CPS.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

No Stipulation.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

Subscribers may only use the Private key and associated public key contained in the certificate once accepted. The Subscribers shall only use their Private Keys for the purposes as contained in the certificate extensions such as key usage, extended key usage, certificate policies etc.

Subscribers shall protect their private keys from unauthorized use and shall discontinue use of private key(s) following expiration or revocation of the associated certificate.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

Relying parties shall accept the terms of the Relying Party Agreement as a condition for relying on any of the STCS Identity CA Issued certificates. Reliance on a certificate must be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party must obtain such assurances for such reliance to be deemed reasonable. Before any act of reliance, Relying Parties shall independently assess:

- The appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by the STCS Identity CA CP. The Relying Party is solely responsible for assessing the appropriateness of the use of a Certificate;
- That the certificate is being used in accordance with the KeyUsage field extensions included in the certificate; and
- The status of the certificate and all the CA's in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party shall not rely on the certificate or shall make its own determination given any reasons furnished for such a revocation.

If the Relying Party deems that the use of the Certificate is appropriate, it shall utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying the Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain.

4.6 CERTIFICATE RENEWAL

Certificate renewal is the issuance of a new certificate without changing the public key or any other information in the certificate. Certificate renewal is supported for STCS Identity CA issued certificates to Subscribers.

4.6.1 CIRCUMSTANCES FOR CERTIFICATE RENEWAL

Certificate renewal is supported for the STCS Identity CA issued certificates subject to the following conditions:

- The certificate to be renewed must not have been revoked;
- All details of the certificate remain accurate and no new validation of identity is required

4.6.2 WHO MAY REQUEST CERTIFICATE RENEWAL

The STCS Identity CA may accept a request for renewal of certificates from the original holder of the certificate. Such requests shall be validated using mechanisms such as challenge response. The request for renewal may originate from the following:

- An RA for its own RA certificate
- An RA on behalf of a subscriber
- A subscriber for his own individual certificate
- An authorized representative for an Organizational certificate.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

The STCS Identity CA may only process the certificate renewal after confirming the authenticity of such a request. The validation may reuse the original documentation used during first issuance. STCS Identity CA may request additional information before the certificate renewal request may be performed. Such request will be processed as soon as is commercially reasonable to do so.

Should the validation fail, the certificate shall not be renewed. The subscriber has the option to apply for a new certificate, and such application shall follow the applicable procedures for a new certificate application.

4.6.4 NOTIFICATION OF RENEWED CERTIFICATE ISSUANCE

The STCS Identity CA shall notify the subscriber of the renewed certificate using the same method as that of original issuance.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

Acceptance procedures for renewed certificate shall follow the same conditions as the original certificate acceptance.

4.6.6 PUBLICATION OF A RENEWAL CERTIFICATE

Publication of renewed certificate shall be done at the same location as the original certificate.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Generally, STCS Identity CA does not notify other entities of a renewed certificate apart from the requesting party.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate (key update) refers to the issuance of new certificate with a different key pair and serial number while retaining other subject information from old certificate.

The new Certificate may be assigned a different validity period and/or signed using a different Issuing CA private key.

4.7.1 CIRCUMSTANCES FOR CERTIFICATE RE-KEY

The STCS Identity CA may re-key certificates of provided that the following conditions are met:

- The certificate to be re-keyed must not have been revoked;
- All details of the certificate remain accurate and no new validation of identity is required.

Automatic updates of managed digital IDs and any or all of the certificates constituting the digital ID may also be performed within one month of the certificate expiry date

4.7.2 WHO CAN REQUEST A CERTIFICATE RE-KEY

Certificate re-key may be requested by:

- An RA for its own RA certificate
- An RA on behalf of a subscriber, if requested by the subscriber
- A subscriber for his own individual certificate
- An authorized representative for an Organizational certificate.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

STCS Identity CA shall follow procedures to ensure that the person or organization seeking to update an end-user Subscriber Certificate is in fact the Subscriber, a sponsor of a device or a representative of an entity. Acceptable procedures are through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key.

Other than the above mentioned procedures, an RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in section 3.3.1 of this CPS for the authentication of an original Certificate Application.

4.7.4 NOTIFICATION OF RE-KEYED CERTIFICATE ISSUANCE TO SUBSCRIBER

Notification of issuance of a re-keyed certificate to Relying Parties shall follow the same procedures as notification for newly issued Subscriber certificates.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RE-KEYED CERTIFICATE

Conduct constituting acceptance of a re-keyed certificate is in accordance with section 4.4.1 of this CPS.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

The re-keyed certificate is published as per publication procedure as per section 2.2.1

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Generally, STCS IDENTITY does not notify other entities of a re-keyed certificate apart from the requesting STCS representative.

4.8 CERTIFICATE MODIFICATION

The STCS Identity CA does not support any form of subscriber certificate modification. Should the subscriber wishes to change details of an existing certificate the following shall apply:

- The existing certificate shall be revoked
- The new details requested shall be verified including the confirmation of the identity information of the subscriber
- Once the information is successfully validated a new certificate shall be issued the same way a new certificate is issued.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

A Certificate shall be revoked/suspended when the binding between the Subject and the Subject's Public Key defined within a Certificate is no longer considered valid.

The CA and/or RA will notify subscribers of certificate revocation or suspension using any or all of the below methods:

- Access to the CRL in the CA repository;
- Email notification to subscriber (Such notification is deemed complete, once the email is sent by STCS Identity CA to the subscriber's registered email address); or
- Telephonic notification to subscriber.

The STCS Identity CA will notify other participants of certificate revocation or suspension through access to the CRL in the CA repository.

4.9.1 CIRCUMSTANCE FOR REVOCATION OF A CERTIFICATE

The STCS Identity CA shall revoke Certificates of Subscribers for the following non-exhaustive reasons:

- A Subscriber contravened any provisions of the Saudi e-Transactions Act and Bylaws made there under;
- The Subscriber has failed to meet its obligations under this CPS or any other applicable Agreements, regulations, or laws;

- STCS Identity CA suspects or determines that revocation of a Certificate is in the best interest of the integrity of the CA;
- The STCS Identity CA determines that a Certificate was not issued correctly in accordance with this CPS;
- There has been an improper or faulty issuance of a certificate due to:
  - A material prerequisite to the issuance of the Certificate not being satisfied;
  - A material fact in the issued certificate is known, or reasonably believed, to be false.
- The Subscriber of the certificate asks for his/her certificate to be revoked due to:
  - The Subscriber's private key is suspected to be compromised;
  - The cryptographic storage device of the Subscriber is lost or stolen;
  - If the Subscriber no longer wishes to use the certificate.
- Subscriber or another authorized agent asks for his/her certificate to be revoked;
- If the Subscriber is no longer part of the organization, i.e. affiliation to the organization is no longer valid; and
- The Subscriber agreement, or Registration Authority's Agreement in the case of an RA, has been terminated.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on a CRL and/or specified as revoked by an OCSP Responder.

4.9.2 WHO CAN REQUEST REVOCATION OF A CERTIFICATE

The following entities can request revocation of a certificate:

- NCDC can request the revocation of any certificates issued by any CA participating in the Saudi National PKI;
- The STCS PA can request the revocation of any certificates issued under its authority;
- An RA can request the revocation of any of their Subscribers Certificate;
- The RA for their own certificate, if any suspected misuse has been attributed to their given Certificates;
- Subscribers, if any suspected misuse has been attributed to their given Certificates, can request a revocation; and
- A legal, judicial or regulatory agency in Saudi Arabia, can request certificate revocation, within applicable laws and in coordination with NCDC.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). The STCS Identity CA shall authenticate the request as well as the authorization of the requester in accordance with the applicable Agreements.

4.9.3.1 Procedure for Requesting the Revocation of a Subscriber Certificate

The request for a subscriber certificate revocation shall be authenticated as described in section 3.4 of this CPS. The subscriber (or any authorized party) can follow an online or a manual process to request the revocation.

Upon successful authentication, the certificate shall be revoked and placed on a CRL which shall be issued in accordance with section 4.9.7 of this CPS. Where OCSP services are provided, the OCSP Responder will be updated accordingly.

4.9.3.2 Procedure for Requesting the Revocation of an RA Certificate

An RA requesting revocation of its RA certificate is required to communicate the request to the STCS PA. The PA shall – after following provisions in the relevant RA Agreement, Operations Policies or Procedures – approve the revocation. The PA may also initiate the revocation of an RA certificate if it is deemed to be necessary or in the best interest of the STCS Identity CA.

Upon approval, the RA certificate shall be revoked and placed on a CRL which shall be issued in accordance with section 4.9.7 of this CPS. Where OCSP services are provided, the OCSP Responder will be updated accordingly.

4.9.4 REVOCATION REQUEST GRACE PERIOD

Revocation request grace period is not permitted once a revocation request has been verified.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

STCS Identity CA shall process authorized revocation requests within a commercially reasonable time.

4.9.6 REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES

Relying Parties are required to comply with the Relying Party Agreement requirements for signature validation, which prescribe how certificate status information is to be obtained and used. Relying Parties may check Certificate status by consulting the most recent CRL from the CA that issued the Certificate on which the Relying Party wishes to rely upon. The CA shall provide Relying Parties with information on how to find the appropriate CRL, repository, or OCSP responder (where available) to check for revocation status.

4.9.7 CRL ISSUANCE FREQUENCY

The STCS Identity CA shall issue CRLS within 24 hours after revocation a Subscriber certificate.

4.9.8 MAXIMUM LATENCY OF CRLS

STCS Identity CA may provide access to an OCSP Responder covering the certificates they issue. The OCSP responses shall conform to RFC6960 and the OCSP responder's certificate must be signed by the STCS Identity CA. The OCSP service shall be available 24 hours a day with reasonable time allocated to maintenance.

4.9.9 ONLINE REVOCATION CHECKING AVAILABILITY

The OCSP service shall be available 24 hours a day with reasonable time allocated to maintenance.

4.9.10 ONLINE REVOCATION CHECKING REQUIREMENTS

The STCS Identity CA shall provide Online revocation and status checking to its relying parties. The STCS Identity CA shall update information provided via an OCSP at least every four days. The OCSP responses from this service will not exceed an expiration time of ten days.

OCSP Responders that receive a request for status of a Certificate that has not been issued, shall not respond with a "good" status for such Certificates.

The STCS Identity CA shall require OCSP requests to contain the following data:

- Protocol Version
- Service request
- Target certificate identifier

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

No other forms of revocation advertisements shall be provided other than the CRL and OCSP services.

4.9.12 SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE

No stipulation, refer to section 4.9.1

4.9.13 CIRCUMSTANCES FOR CERTIFICATE SUSPENSION

Certificates may be suspended following circumstances outlined in section 4.9.1

4.9.14 WHO CAN REQUEST SUSPENSION

- NCDC can request the suspension of any certificate issued by any CA participating in the Saudi National PKI;
- The STCS PA or STCS PKI Committee can request the suspension of any certificates issued under its authority;
- An RA can request the suspension of one of their Subscribers Certificate;
- Subscribers, if any suspected misuse has been attributed to their given Certificates, can request a suspension; and
- A legal, judicial or regulatory agency can request a suspension.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

A request to suspend a certificate shall identify the certificate to be suspended, explain the reason for suspension, and allow the request to be authenticated (e.g., digitally or manually signed). The STCS Identity CA or RA shall authenticate the request as well as the

authorization of the requester in accordance with the applicable Agreements. For Suspension of RA Certificates refer to the RA Agreement pertaining to each RA.

The procedure for processing suspension requests is as follows:

- The request is submitted to the CA or RA;
- If a digital signature is used, the digital signature on the request is verified;
- The certificate is suspended;
- The CA may notify the entity once their certificates have been suspended;

Once suspended, the serial number of the Certificate and the date and time shall be added to the appropriate CRL and a reason code of “on hold” will be included in the CRL.

4.9.16 Limits on Suspension Period

The maximum period for which a Certificate can be suspended shall not exceed ninety (90) days.

4.9.17 Circumstances for Terminating Suspended Certificates

When the entity which requested the suspension of the certificate is satisfied that the circumstances for suspension are no longer valid, the suspension shall be terminated. Once reactivated, the certificate validity period will be subject to the initial validity period.

If the entity which requested the suspension of the certificate is satisfied that the circumstances for suspension are valid and prevailing, the certificate will be revoked.

When the period for suspension has reached limit period of suspension without resolution, the certificate will be revoked.

4.9.18 Procedure for Terminating the Suspension of a Certificate

A request to unsuspend a certificate shall identify the relevant certificate, the reason for unsuspension and a method to allow the request to be authenticated (e.g., digitally or manually signed). The STCS Identity CA shall authenticate the request as well as the authorization of the requester before a certificate is unsuspended.

4.10 Certificate Status Services

The status of the STCS Issuing CA public certificates is available from CRLs in the repositories and via OCSP responder services (where available). The STCS Identity CA shall keep the revocation entries on the CRL or OCSP until after the expiry date of the revoked certificate.

4.11 End of Subscription

Subscribers may end their subscription to certificate services by having their subscriber certificate revoked or letting it expire naturally.

4.12 KEY ESCROW AND RECOVERY

The STCS Identity CA does not support Subscriber Key Escrow.

5 FACILITY MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL SECURITY CONTROLS

STCS operates the STCS PKI (Intermediary and Issuing CAs), Repositories and OCSP responder at the STCS data center, with appropriate physical and procedural access controls for all hardware and software sub-systems used in the issuance and revocation of certificates. STCS limits access to functions critical to registration and certificate to personnel in Trusted Roles.

The STCS shall have physical and environmental security policies for systems used for certificate issuance and management which cover physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking & entering, and disaster recovery. Controls should be implemented to avoid loss, damage or compromise of assets and interruption to business activities and theft of information and information processing facilities

5.1.1 SITE LOCATION AND CONSTRUCTION

The location and construction of the facility housing the STCS Identity CA and STCS Data Center equipment is consistent with facilities used to house high value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, provides robust protection against unauthorized access to the STCS Identity CA equipment and records.

5.1.2 PHYSICAL ACCESS

STCS Identity CA systems are protected by at least four tiers of physical security, with access to the lower tier required before gaining access to the higher tier. Progressively restrictive physical access privileges control access to each tier. Sensitive STCS Identity CA operational activity, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Physical access is automatically logged, and video recorded. Additional tiers enforce individual access control through the use of biometric authentication. Unescorted personnel, including un-trusted employees or visitors, should not be allowed into such secured areas. STCS employ Security Personnel that continually monitor the facility hosting CA equipment on a 24x7 basis. STCS shall provide normal and emergency lighting to the CA facilities.

STCS shall ensure that the facilities used for the Issuing CA Certificate life cycle management are operated in an environment that physically protects the services from Compromise through unauthorized access to systems or data. An authorized employee should always accompany any unauthorized person entering a physically secured area. Physical protections should be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the systems hosting the STCS PKI operations. No parts of the STCS PKI premises shall be shared with other organizations within this perimeter.

5.1.3 POWER AND AIR CONDITIONING

STCS shall ensure that the power and air conditioning facilities are sufficient to support the PKI Operations environment.

The STCS Identity CA equipment shall have backup capability sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown. Any of the STCS Identity CA on-line servers (e.g., CAs hosting directories) shall be provided with Uninterrupted Power sufficient to support a smooth shutdown of the PKI operations.

5.1.4 WATER EXPOSURE

STCS shall ensure that the STCS Identity CA systems are protected from exposure to water sources. Additional prevention mechanisms such as using raised flooring must be employed where possible to minimize flood water damaging equipment.

5.1.5 FIRE PREVENTION AND PROTECTION

The STCS Identity CA equipment shall be housed in a facility with appropriate fire suppression and protection systems.

5.1.6 MEDIA STORAGE

STCS shall ensure that STCS Identity CA media is stored so as to protect it from accidental damage (such as water, fire, electromagnetic, etc.). Media that contains audit, archive or backup information is duplicated and stored in a location separate from the CAs.

5.1.7 WASTE DISPOSAL

Sensitive media and documentation that are no longer needed for operations are destroyed using appropriate disposal processes.

5.1.8 OFF-SITE BACKUP

Full system backups of CAs, sufficient to recover from system failure, are made on a periodic schedule as described in STCS Operations Policies and Procedures.

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the PKI is weakened. The functions performed in these roles form the basis of trust for all uses of the STCS Identity CA. The following are the trusted roles for STCS PKI:

- CA Administrator – general CA administration and approval of the generation, revocation and suspension of certificates
- CA Security Officer – overall responsibility for administering the implementation of the CA's security practices, cryptographic key lifecycle management functions
- Policy Authority – responsible for the overall development, maintenance and ensures approval of CA policies

- Operations Authority – responsible for the implementation of the CA policies and development of operational procedures and guidelines
- CA Auditor – internal auditor is responsible for ensuring the CA is operating in line with approved policies and procedures. The auditor is also responsible for checking that procedures are being followed correctly during Key Ceremonies
- CA Key Manager – responsible for CA Key Lifecycle management functions
- CA Key Shareholders – holders of the CA key components
- CA Developers – responsible for the development of CA systems

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

STCS shall ensure separation of duties for critical CA functions to prevent one person from maliciously using the PKI systems without detection. Each user's system access is limited to those actions for which they are required to perform in fulfilling their responsibilities. Separate individual shall fill each of the roles specified in STCS Trusted Roles document. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over the system operation.

A single person may be sufficient to perform tasks associated with a role, except for the activation of the STCS Identity CA certificate signing Private Key. Activation of the STCS Identity CA certificate signing Private Key shall require at least 3 people to present their credentials.

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

An individual shall identify and authenticate himself before being permitted to perform any actions set forth above for that role or identity.

5.2.4 SEPARATION OF ROLES

Individual CA personnel are specifically designated to the roles defined in section 5.2.1 of this CPS and STCS Trusted Roles document. The STCS Identity CA will ensure that no individual shall be assigned more than one Trusted Role.

5.3 PERSONNEL CONTROLS

5.3.1 BACKGROUND, QUALIFICATIONS AND EXPERIENCE REQUIREMENTS

All persons filling trusted roles shall be selected on the basis of skills, experience, loyalty, trustworthiness, and integrity. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the STCS Identity CA are set forth in the STCS Trusted Roles document and STCS Organization Structure document.

5.3.2 BACKGROUND CHECK AND CLEARANCE PROCEDURES

STCS conducts background investigations for all STCS PKI personnel including trusted roles and management positions. Background check shall take into account the following:

- Availability of satisfactory character reference, i.e. one business and one personal;
- A check (for completeness and accuracy) of the applicant's CV;

- Confirmation of claimed academic and professional qualifications;
- Independent identity check (National ID card, Passport or similar document);
- Interviews with references shall be done as required; and
- More detailed checks, such as criminal record checks.

Security clearance shall be repeated every 3 years for personnel holding trusted roles. All persons filling the Trusted Roles shall only be granted access to the STCS PKI systems once the background clearance procedures detailed above have been completed and confirmed.

5.3.3 TRAINING REQUIREMENTS

STCS shall ensure that all personnel receive appropriate training. Such training shall address relevant topics such as basic Public Key Infrastructure knowledge, security requirements, operational responsibilities and associated procedures.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

Individuals responsible for PKI roles are made aware of changes in the CA operation. Any significant change to the operations shall have a training (awareness) plan, and the execution of such plan shall be documented.

The STCS Identity CA shall review and update its training program at least once a year to accommodate changes in the CA system.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

The STCS Identity CA shall ensure that any change in the staff complement will not affect the operational effectiveness of the PKI services and security thereof.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

The STCS Identity CA shall take appropriate administrative and disciplinary actions against personnel who perform unauthorized actions (i.e., not permitted by the CP, CPS and/or other procedures) involving the STCS Identity CA or its repository.

5.3.7 CONTRACTING PERSONNEL REQUIREMENTS

Contractor personnel employed to perform functions pertaining to the STCS PKI Operations shall be subjected to the same processes, sanctions, assessment, security and operational procedure as permanent personnel. under adequate supervision and perform only assigned tasks.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

STCS will make available to its personnel its CP, CPS, and any relevant documents required to perform their duties.

5.4 AUDIT LOGGING PROCEDURES

Audit log files are generated for all events relating to the security of the STCS Identity CA, and other associated components. The security audit logs for each auditable event defined in this section are maintained in accordance with onsite retention period and for archive.

5.4.1 TYPES OF EVENTS RECORDED

The STCS PA shall ensure recording in audit log files all events relating to the security of the CA system hosted in STCS data centre. All security audit capabilities of the CA operating system and CA applications shall be enabled. Such events include, but are not limited to:

1. CA key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction; and
    b. Cryptographic device lifecycle management events.
2. Issuing CA Certificate lifecycle management events, including:
    a. Certificate requests, renewal, and re-key requests, and revocation;
    b. All verification activities stipulated in these Requirements and the Issuing CA's Certification Practice Statement;
    c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    d. Acceptance and rejection of certificate requests;
    e. Issuance of Certificates; and
    f. Generation of Certificate Revocation Lists.
3. Security events, including:
    a. Successful and unsuccessful PKI system access attempts;
    b. PKI and security system actions performed;
    c. Security profile changes;
    d. System crashes, hardware failures, and other anomalies;
    e. Firewall and router activities; and
    f. Entries to and exits from the STCS PKI facility.
    g. Equipment failure or electrical power outages
    h. Changes to CA configuration and system clock time

Log entries MUST include the following elements:

- Date and time of entry;
- Identity of the person making the journal entry; and
- Description of the entry.

All logs, whether electronic or manual, must contain the date and time of the event and the identity of the Entity which caused the event. The CA shall also collect, either electronically or manually, security information not generated by the CA system such as:

- Physical access logs;

- System configuration changes and maintenance;
- CA personnel changes;
- documentation relating to certificate requests and the verification;
- documentation relating to certificate revocation;
- Discrepancy and No compromise reports;
- Information concerning the destruction of sensitive information;
- Current and past versions of all Certificate Policies;
- Current and past versions of Certification Practice Statements;
- Vulnerability Assessment Reports;
- Threat and Risk Assessment Reports;
- Compliance Inspection Reports; and
- Current and past versions of Agreements.

5.4.2 FREQUENCY OF PROCESSING DATA

Audit logs are required to be processed periodically in accordance with STCS Audit and Compliance Policy.

5.4.3 RETENTION PERIOD FOR AUDIT LOG

The STCS Identity CA shall retain all system generated (electronic and manual) audit records onsite for a period not less than twelve months from the date of creation.

5.4.4 PROTECTION OF AUDIT LOG

The STCS Identity CA shall protect the electronic audit log system and audit information captured electronically or manually from unauthorized viewing, modification, deletion or destruction.

5.4.5 AUDIT LOG BACKUP PROCEDURES

STCS Identity CA shall back up all audit logs and audit summaries in a secure location and protected to the same degree as the originals.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

The audit collection system may be an internal system. The audit collection system must maintain integrity and availability of the data collected as detailed in the STCS Audit and Compliance Policy.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

Event-causing subject are not notified.

5.4.8 VULNERABILITY ASSESSMENTS

Routine vulnerability assessments of security controls shall be performed by STCS for its Issuing CAs and other PKI supporting systems hosted in the STCS data centre. Such assessments shall be held at least annually or as determined the Information Security Policy.

The STCS security program must include an annual Risk Assessment which includes identification of foreseeable internal and external threats, assess the likelihood and potential damage of these threats and assess the sufficiency of the policies, procedures, information systems and technology. The program must also ensure vulnerability assessments are performed, reviewed and revised following an examination of audit events.

Based on the Risk Assessment exercise, STCS shall develop, implement, and maintain a security plan to control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

5.5 RECORDS ARCHIVAL

5.5.1 TYPES OF EVENTS ARCHIVED

The STCS Identity CA archive records shall be sufficiently detailed to establish the proper operation of the CA, or the validity of any certificate (including those revoked or expired) issued by the CA. The STCS Identity CA shall make these archived records available to its Qualified Auditor upon request. The data to be archived may include, but not limited to the following:

- Audit data, as specified in section 5.4
- Data related to certificate requests, verifications, issuances and revocations
- CA Procedures, policies, subscriber agreements and compliance records
- Cryptographic device and key lifecycle information
- Systems management and change control activities

5.5.2 RETENTION PERIOD FOR ARCHIVE

The minimum retention periods for archive data are established in accordance with applicable regulatory guidance, laws, Agreements, and as specified by the STCS PA. STCS Identity CA's minimum retention period for archive data is established at 10 years.

The STCS Identity CA shall retain all documentation relating to the STCS Identity CA certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least ten years after any Certificate based on that documentation ceases to be valid.

5.5.3 PROTECTION OF ARCHIVE

Only authorized individuals shall be permitted to review the archive. The contents of the archive shall not be released except as determined by NCDC, STCS PA, or as required by law. Records and material information relevant to use of, and reliance on, a certificate shall be archived. Archive media shall be stored in a secure storage facility separate from the original storage media. Any secondary site must provide adequate protection from environmental threats such as temperature, humidity and magnetism. Data to be migrated periodically to fresh media; and protection against obsolescence of hardware, operating systems, and other software, by, for example, retaining as part of the archive the hardware, operating systems, and/or other software in order to permit access to and use of archived records over time.

5.5.4 ARCHIVE BACKUP PROCEDURES

Only one copy of the archive is maintained. In other words, archive itself is not backed up.

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

Certificates, CRLs, and other revocation database entries shall contain time and date information. System logs shall be time stamped and systems use a dedicated time server to maintain synchronized time.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

The type of Archive Collection System, whether internal or external, is specified in STCS Archival Policy.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

Information on how the archive information is created, verified, packaged, transmitted and stored is detailed in STCS Archival Policy. These policies and procedures are updated and augmented to reflect the legal and best practice requirements for managing and protecting electronic records. Only authorized STCS Identity CA personnel shall have access to the archives.

5.6 KEY CHANGEOVER

The CA system utilized by the STCS Identity CA may periodically perform key rollover, allowing CA keys to be changed periodically as required to minimize risk to the integrity of the STCS Identity CA. Once changed the new key is used for certificate signing purposes. The unexpired older keys are used to sign CRL's until all certificates signed by the unexpired older private key have expired. The old key shall be protected to the same degree as the active key.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

If the STCS Identity CA detects a potential hacking attempt or other form of compromise to the CA, it shall perform an investigation in order to determine the nature and the degree of damage. If the STCS Identity CA Private key is suspected of compromise, the procedures outlined in STCS Incident Management Procedures shall be followed. Otherwise, the scope of potential damage shall be assessed in order to determine if the STCS Identity CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

The STCS Identity CA shall invoke its Incident Management Procedures in the event of the following non-exhaustive events:

- Suspected or detected compromise of the CA system;
- Physical or electronic attempts to penetrate the CA system;
- Denial of Service attacks on a CA system component; and
- Any incident preventing the CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

The STCS Identity CA shall maintain backup copies of hardware, system, databases, and private keys in order to rebuild the STCS Identity CA capability in case of software and/or data corruption. If necessary, the procedures as outlined in the STCS Operations Policy and Business Continuity Plan shall be enacted.

5.7.3 CA PRIVATE KEY COMPROMISE RECOVERY PROCEDURES

The STCS Identity CA shall develop and maintain Disaster Recovery Policies and Procedures. The recovery procedures shall contain procedures for the recovery of the CA private key, and same shall be followed in the case of the STCS Identity CA Private Key compromise.

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

STCS has developed a robust Business Continuity Management System for critical PKI services to provide the minimum acceptable level of assurance to its subscriber for service availability.

All STCS critical infrastructure equipment at the primary site (STCS data center) have built-in hardware fault-tolerance and configured to be highly available with auto-failover switching. STCS currently maintains copies of backup media and infrastructure system software, which include but are not limited to PKI services related critical data, database records for all certificates issued and audit related data at its offsite business continuity and disaster recovery storage facilities.

STCS Business Continuity Management System (BCMS) demonstrates the capability to restore or recover critical PKI services at the primary site within one week in the event of service(s) non-availability.

Business Continuity Management components at STCS are being regularly tested, verified, and updated to be operational to address crisis situation in the event of a disruption. For security reasons details of these plans are not publicly available.

STCS business continuity plan includes:

- Conditions for activating the plan;
- Emergency procedures;
- Fall-back procedures;
- Resumption procedures;
- A maintenance schedule for the plan;
- Awareness and education requirements;
- The responsibilities of the individuals;
- Recovery time objective (RTO);
- Recovery point objective (RPO);
- Regular testing of contingency plans;
- The CA’s plan to maintain or restore the CA’s business operations in a timely manner following interruption to or failure of critical business processes;
- A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;

- Acceptable system outage and recovery time;
- Procedure/frequently of backup copies for essential business information and software are taken; and
- Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

STCS has developed recovery plans to mitigate the effects of the following events that are likely to occur; natural, man-made or equipment failure related disasters.

STCS has implemented an alternate recovery site as per industry standards to provide full recovery of critical PKI services within one week following a disaster at the primary site. STCS Business Continuity Policy contains further details.

5.8 CA OR RA TERMINATION

5.8.1 CA TERMINATION

When it is necessary to terminate the STCS Identity CA, the impact of the termination must be minimized as much as possible in light of the prevailing circumstances and is subject to the applicable STCS Identity CA Agreements. Procedures to be followed for the termination of the STCS Identity CA shall be developed, and must at a minimum include the following:

- Ensure minimal disruption caused by the termination of the CA
- Ensure notification of Subscribers, Relying Parties and other relevant Stakeholders, such as the NCDC
- Ensure certificate status information services are provided and maintained for the duration of the termination
- Ensure process for revoking certificates are maintained

STCS shall nominate a custodian of the STCS Identity CA archival records in case of the STCS Identity CA termination.

Should a successor CA be appointed to take over the functions of the STCS Identity CA, such a successor shall, to the extent as it is practical and reasonable, assume the same rights, obligations and duties as the terminated STCS Identity CA.

5.8.2 RA TERMINATION

In the event of STCS Identity CA terminating an RA, the termination shall be done in such a way to minimize the impact of the termination to the subscribers. Procedures for the termination of the CA shall be developed and shall at minimum address the following:

- Ensure minimal disruption caused by the termination of the RA
- Ensure notification of Subscribers, Relying Parties and other relevant Stakeholders
- Ensure process for revoking certificates are maintained

STCS Identity CA shall ensure certificate records maintained by the terminated RA are kept secure and available.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

Key pair generation for STCS Identity CA will be witnessed and attested to by a party separate from the STCS Identity CA operator or the CA administrator as mentioned in the Key Generation Script for each CA.

Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys. The STCS PKI CAs shall use Hardware Security Modules (HSMs) for CA key generation and storage. HSM's should be minimum FIPS 140-2 Level 3 validated.

STCS Identity CA key pair generation is performed by multiple trusted personnel using trustworthy systems and processes that provide security and required cryptographic strength for the generated keys.

The STCS Identity CA and Issuing CAs key pair is generated in pre-planned Key Generation Ceremony in accordance with the requirements of NCDC. The activities performed during the Key Generation Ceremony are video recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by STCS PKI management.

For Subscriber and RA Private keys generated in cryptographic hardware, the key pairs will be generated or protected, as the case may be, in cryptographic modules at least compliant to FIPS 140-2 Level 2 or higher. Keypairs generated in Software shall be generated using trustworthy computer systems.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBERS

The STCS shall deliver subscriber private keys in a secure format, such as in cryptographic tokens or smartcards when those keys are generated in cryptographic hardware.

Subscriber and RA keys generated in Software shall be delivered securely using secure standards such as PKCS#12 file format.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

The STCS Identity CA shall accept Issuing CA Public Keys that are cryptographically protected, such as those using PKCS#10 mechanisms from an authorized STCS representative. Such Public Key delivery shall be made as part of the Key Ceremony and as documented in the Key Ceremony Script.

Where private keys are not created in the presence of the Subscriber, they will be delivered electronically using industry standard based PKCS messages (e.g. PKCS#12) over secure protocols which provide equivalent or higher encryption strength than the key being transported or may be delivered on a hardware cryptographic module. In all cases, the following requirements are met:

- Anyone who generates a private signing key for a Subscriber does not retain any copy of the key after delivery of the private key to the Subscriber;
- The private key is protected from activation, compromise, or modification during the delivery process;
- The Subscriber acknowledges receipt of the private key;
- Delivery is accomplished in a way that ensures that the correct token and activation data are provided to the correct Subscriber.
    - For cryptographic modules, accountability by the RA for the location and state of the module is maintained until the Subscriber accepts possession of it.
    - For electronic delivery of private keys, the key material is encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data is delivered using a separate secure channel.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

The STCS Identity CA Public Key shall be delivered to the Relying Parties as part of the CA certificate, which is publicly accessible in the repository, https://www.stcs.com.sa/repository.

6.1.5 KEY SIZES

Key pairs shall be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs. Key sizes are described as below for all subscriber certificates issued by the STCS Identity CA. All FIPS-approved signature algorithms shall be considered acceptable. If NCDC determines that the security of a particular algorithm may be compromised, it shall direct STCS to revoke the affected certificates.

All certificates issued to subscribers shall use at least 2048-bit RSA, with Secure Hash Algorithm version 2 (SHA-256) in accordance with FIPS 186-2 or equivalent.

The key lengths of certificates issued by the STCS Identity CA are as follows:

- Subscriber Key Pairs: 2048 bits RSA
- RA Key Pairs: 2048 bits RSA
- OCSP Key Pair: 2048 bits RSA

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

The STCS Identity CA shall generate key pairs that comply with FIPS 186. The STCS Identity CA shall use reasonable techniques to validate the suitability of the Subscriber key pairs.

6.1.7 KEY USAGE PURPOSES

Public keys that are bound into certificates shall be certified for use in authenticating or signing, as specified by STCS Identity CA. The use of a specific key is determined by the key usage extension in the X.509 certificate. STCS Identity CA key is used for authentication and digital signature.

6.2 PRIVATE KEY PROTECTION AND CRYPTO-MODULE ENGINEERING CONTROLS

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

Cryptographic modules, smartcards or tokens employed for subscriber, OCSP Responder and RA private key protection issued by the STCS Identity CA shall comply with FIPS-PUB 140-2 “Security Requirements for Cryptographic Modules”, Level 2 and above.

6.2.2 SUBSCRIBER PRIVATE KEY MULTI-PERSON CONTROL

No stipulation. RAs, OCSP Responder and subscribers’ private keys are not under multi-person control.

6.2.3 PRIVATE KEY ESCROW

The STCS Identity CA does not escrow Subscriber Private keys as it does not issue encryption certificates.

6.2.4 PRIVATE KEY BACKUP

6.2.4.1 Backup of Subscriber Signing Private Key

STCS Identity CA does not backup Subscriber private keys.

6.2.5 PRIVATE KEY ARCHIVAL

The STCS Identity CA does not offer data encryption services, thus does not support the archival of Private Keys.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

The STCS Identity CA does not permit subscriber key transfer into and out of cryptographic modules or devices. Subscriber keys are generated in secure cryptographic devices and shall not be transferred out of those devices.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

The subscriber keys shall be stored in at least FIPS 140-2 level 2 compliant devices in encrypted form.

6.2.8 METHOD OF ACTIVATING PRIVATE KEYS

Subscriber Private keys shall be activated by providing a passphrase set on initial certificate generation by the subscriber.

6.2.9 METHODS OF DEACTIVATING PRIVATE KEYS

Subscriber private keys that have been activated shall not be left unattended. Subscribers are obliged to deactivate the private key by “logging out” of the cryptographic device or automatically after a period of inactivity as configured.

6.2.10 METHODS OF DESTROYING PRIVATE KEYS

No stipulation.

6.2.11 CRYPTOGRAPHIC MODULE RATING

As described in section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVE

The subscriber public key is archived as part of the certificate archive process.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY USAGE PERIODS

The table below details key usage, length and certificate lifetime for the corresponding keys:

Key/Certificate	Key Length in Bits	Maximum Validity Period
Subscriber keys	2048	36 months
RA keys	2048	36 months
OCSP Signing Key	2048	36 months

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

The activation data used to unlock subscriber private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected. Activation data shall be user selected.

6.4.2 ACTIVATION DATA PROTECTION

The Subscriber shall protect activation data from disclosure or compromise. If written down, it shall be secured at the level of the data that the associated cryptographic device is used to protect and shall not be stored with the cryptographic device.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

The computer security functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards.

At a minimum STCS data centre shall have (but not limited to) the following controls to ensure security of the systems:

- Integrity checks are performed on the operating system;
- Software packages are only installed from a trusted software repository;
- Minimal network connectivity;
- Authentication and authorization for all functions;
- Strong authentication and role-based access control for all vital functions;
- Disk and file encryption for all relevant data; and
- Proactive patch management.

6.5.2 COMPUTER SECURITY RATING

The STCS Identity CA Software shall comply with at least Common Criteria EAL2 or an equivalent security profile from other applicable standards.

6.6 LIFE-CYCLE SECURITY CONTROLS

6.6.1 SYSTEM DEVELOPMENT CONTROLS

The STCS Identity CA shall implement system development controls to protect the integrity of the CA operations. The controls shall include (but not limited to) the following:

- Use software that has been designed and developed under a formal, documented development methodology;
- Hardware and software procured are purchased in a fashion to reduce the likelihood that any particular component was tampered with;
- Hardware and software are developed in a controlled environment, and the development processes are defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software;
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location;
- The hardware and software are dedicated to performing CA activities. There are no other applications, hardware devices, network connections, or component software installed which are not part of the CA operation;
- Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the CA operations are installed on the equipment and are obtained from sources authorized by local policy. Issuing CA hardware and software are scanned for malicious code on first use and periodically thereafter; and

Hardware and software updates are purchased or developed in the same manner as original equipment; and are installed by trusted and trained personnel in a defined manner.

6.6.2 SECURITY MANAGEMENT CONTROLS

The configuration of the STCS Identity CA systems as well as any modifications and upgrades shall be documented and controlled. There shall be a mechanism for detecting unauthorized modification to software or configuration. A formal configuration management methodology

shall be used for installation and on-going maintenance of the system. During initial installation the CA software is checked to ensure that it is the same software that came from the vendor (e.g. by comparing checksums)

6.6.3 LIFE CYCLE SECURITY RATINGS

No Stipulation

6.7 NETWORK SECURITY CONTROLS

The STCS Identity CA shall employ appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such protection mechanisms may include network security and firewall management, port restrictions and IP address filtering. Unused services shall be turned off.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment.

6.8 TIME STAMPING

Time stamping shall be supported for the Certificates, CRLs, and other revocation database entries containing time and date information. The STCS Identity CA shall ensure the synchronization of CA components using a trusted time source, such as a Network Time Protocol (NTP) service or an atomic clock.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

This section contains the rules and guidelines followed by this CA in populating X.509 certificates and CRL extensions. The certificates issued by this STCS Identity CA are subscriber certificates (individuals, organizations).

7.1.1 VERSION NUMBERS

The STCS Identity CA shall issue X.509 v3 certificates (populate version field with integer "2").

7.1.2 CERTIFICATE EXTENSIONS

STCS Identity CA and its RA's critical private extensions shall be interoperable in their intended community of use.

Subscriber certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by STCS Identity CA CP. Any optional or additional extensions shall be non-critical and shall not conflict with the certificate and CRL profiles defined in this CPS.

7.1.3 ALGORITHM OBJECT IDENTIFIERS

STCS Identity CA shall sign Subordinate Certificates using any one of the following:

sha256WithRSAEncryption algorithm (1.2.840.113549.1.1.11).

sha384WithRSAEncryption algorithm (1.2.840.113549.1.1.12).

ecdsawithsha256 algorithm (1.2.840.10045.4.3.2)

ecdsawithsha384 algorithm (1.2.840.10045.4.3.3)

ecdsawithsha512 algorithm (1.2.840.10045.4.3.4)

The algorithm identifier of the subject Public Key shall be:

rsaEncryption (OID: = 1.2.840.113549.1.1.1).

7.1.4 NAME FORMS

Certificates issued by STCS Identity CA contain the full X.500 distinguished name of the certificate issuer and certificate subject in the issuer name and subject name fields. Distinguished names are in the form of an X.501 printable string.

7.1.5 NAME CONSTRAINTS

No Stipulation.

7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER

Certificates issued under this CPS shall assert a certificate policy OID.

7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION

No Stipulation

7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS

No stipulation.

7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICY EXTENSION

Processing semantics for the critical certificate policy extension shall conform to X.509 certification path processing rules.

7.2 CRL PROFILE

The STCS Identity CA CRL Profile is shown below:

7.2.1 STCS IDENTITY CA CRL PROFILE

Field	Content	Comment
Version	1	
Algorithm	SHA256withRSA	
Issuer	CN=STCS IDCA O=STCS C=SA	
This update	*<issue date>*	Date CRL was issued
Next update	*<issue date + 4 days>*	Or immediately upon revocation
AuthorityKeyIdentifier	Parent CA's Subject Key Identifier	
CRL number	<number>	Integer that is incremented sequentially

7.2.2 VERSION NUMBERS

The STCS INDENTITY CA shall issue X.509 version two (v2) CRLs (populate version field with integer "1").

7.2.3 CRL AND CRL ENTRY EXTENSIONS

Critical private extensions shall be interoperable in their intended community of use. CRLs shall have the CRL number and Authority Key Identify extensions set.

7.3 OCSP PROFILE

No Stipulation.

7.3.1 VERSION NUMBER

No Stipulation.

7.3.2 OCSP EXTENSIONS

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The STCS PA shall be responsible for overseeing compliance of the STCS Identity CA to the CP and corresponding CPS. The STCS PA shall ensure that the requirements of the STCS Identity CA CP and CPS and the provisions of applicable Agreements with subscribers are implemented and enforced. STCS Identity CA shall undergo annual WebTrust audits whose results shall be submitted to NCDC if requested.

The STCS PKI Committee shall also ensure periodical audits (at least annually) to its RAs are conducted to ensure compliance with the RA agreements and provisions of the STCS Identity CP and CPS.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

The STCS Identity CA shall be subjected to periodic WebTrust compliance audits which are no less frequent than once a year and after each significant change to the deployed procedures and techniques. Similarly, the STCS PKI Committee under the direction of the STCS PA, has the right to require periodic inspections of its RAs to validate that the RAs are operating in accordance with the STCS Identity CA CP and/or RA agreement. The STCS Identity CA may internally audit each delegated third party's compliance against defined requirements on an annual basis.

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

The annual audit of the STCS Identity CA shall be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme;
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme; and
- Bound by law, government regulation, or professional code of ethics.

A licensed WebTrust auditor will be appointed by STCS Identity CA for the audit.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

To provide an unbiased and independent evaluation, the auditor and audited party shall not have any current or planned financial, legal or other relationship that could result in a conflict of interest.

8.4 TOPICS COVERED BY ASSESSMENT

The compliance audits will verify whether the STCS PKI operations environment is in compliance with the applicable CP, CPS and supporting operational policies and procedures. The term STCS PKI Operations environment defines the total environment and includes:

- All documentation, records;
- Contracts/agreements;
- Compliance with applicable Law;
- Physical and logical controls;
- Personnel and approved roles/tasks;
- Hardware (e.g. servers, desktops, hardware security modules, network devices and security devices); and
- Software and information.

The auditor shall provide the STCS PA and/or NCDC with a compliance report highlighting any discrepancies.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If irregularities are found by the auditor, the audited party (STCS Identity CA) shall be informed in writing of the findings. The audited party must submit a report to the auditor or directly to NCDC or STCS PA, as determined by NCDC, as to any remedial action the audited party will take in response to the identified deficiencies. This report shall include a time for completion to be approved by the auditor, or by NCDC as appropriate.

Where an audited party fails to take remedial action in response to the identified deficiencies, NCDC shall be informed by the auditor and shall take the appropriate action, according to the severity of the deficiencies.

- Noting the deficiencies but allowing the STCS Identity CA to continue operations until the next planned, or newly scheduled, inspection;
- Request the suspension of the offending CA's certificate; or
- Request the revocation of the offending CA's certificate.

8.6 COMMUNICATION OF RESULTS

An Audit Compliance Report, including identification of corrective measures taken or being taken by the audited party, shall be provided to the STCS PA and/or NCDC as applicable.

The STCS INDENTITY CA shall make the Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, an explanatory letter is to be signed by the Qualified Auditor.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 CERTIFICATE ISSUANCE/RENEWAL FEE

The STCS Identity CA may charge fees for certificate issuance or renewal. Fees may also be charged for certificate reissuance or re-key.

9.1.2 CERTIFICATE ACCESS FEES

The STCS Identity CA may charge access fees at its discretion to any database which stores issued certificates.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEE

The STCS Identity CA does not charge fees to access certificate status information via the CRL.

9.1.4 FEES FOR OTHER SERVICES

The STCS Identity CA may charge fees for other services such as timestamping.

9.1.5 REFUND POLICY

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

The STCS Identity CA disclaims all liability implicit or explicit due to the use of any certificates issued by the STCS Issuing CAs which certify public keys of subscribers.

9.2.1 INSURANCE COVERAGE

The STCS Identity CA shall hold insurance cover in lieu of its performance and obligations that is deemed sufficient by the CA:

- Commercial general liability insurance with policy limits as determined by STCS;
- Professional Liability (Errors and Omissions) Insurance with policy limits as determined by STCS

9.2.2 OTHER ASSETS

STCS Identity CA shall have sufficient financial resources to maintain their operations and perform their duties.

9.2.3 INSURANCE/WARRANTY COVERAGE FOR END-ENTITIES

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

Information pertaining to the STCS Identity CA may be made publicly available at the discretion of the STCS INDENTITY CA Policy Authority. Specific confidentiality requirements for business information are defined in STCS Privacy Policy and the associated agreements.

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

9.3.1.1 Registration Information

All registration records are considered to be confidential information, including:

- Certificate applications, whether approved or not;
- Certificate information collected as part of the registration process;
- Completed Subscriber Agreements;
- Any corporate or personal information held by STCS Identity CAs related to the application and issuance of Certificates is considered confidential and will not be released without the prior consent of the relevant holder, unless required otherwise by law or to fulfill the requirements of STCS Identity CA CP, and in accordance with STCS Privacy Policy.

9.3.1.2 Certificate Information

The reasons for a certificate being suspended or revoked is considered confidential information, with the sole exception of the revocation of the STCS Identity CA due to:

- The compromise of their private key, in which case a disclosure may be made that the private key has been compromised; or
- The termination of the STCS Identity CA in which case prior disclosure of the termination may be given.

9.3.1.3 PKI Documentation

STCS Document Control Policy specifies which documents are considered to be confidential.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

9.3.2.1 Certificate Information

Certificates published in the public repositories are not considered to be confidential information.

9.3.2.2 PKI Documentation

The following documents are public documents and are not considered to be confidential information:

- The STCS Identity CA CP;
- The STCS Identity CA CPS;
- The STCS Identity CA Public Disclosure Statements;

- STCS Dispute Resolution Policy;
- STCS Privacy Policy; and
- Any other policy documents which are classified public.

9.3.2.3 Disclosure of Certificate Revocation Information

Certificate revocation information is provided via the CRL in the repositories.

9.3.3 Responsibility to Protect Confidential Information

All STCS Identity CA PKI participants shall be responsible for protecting the confidential information they possess in accordance with STCS Privacy Policy and applicable laws and Agreements.

9.4 Privacy of Personal Information

Any personal identifying information collected by STCS RAs shall be protected in accordance with STCS Privacy Policy. The STCS Identity CA shall use reasonable measures to protect personal identifying information from disclosure to any third party.

9.4.1 Privacy Plan

All personally identifying information as defined by STCS Privacy Policy shall be protected from unauthorized disclosure.

9.4.2 Information Treated as Private

Any information about Subscribers that is not publicly available through the content of the issued certificate, repository and online CRL's is treated as private.

9.4.3 Information not Deemed Private

Information appearing in Subscriber Certificates such as the organization name, and public key will not be deemed private. STCS Privacy Policy identifies the personally identifiable information that can be collected to enable issuance of a certificate.

9.4.4 Responsibility to Protect Private Information

Access to STCS Identity CA held private information shall be restricted to those with an official need-to-know basis in order to perform their official duties.

9.4.5 Notice and Consent to Use Private Information

Requirements for notice and consent to use private information are defined in the respective Agreements and STCS Privacy Policy.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

Any disclosure shall be handled in accordance with STCS Privacy Policy.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

Any disclosure shall be handled in accordance with STCS Privacy Policy.

9.5 INTELLECTUAL PROPERTY RIGHTS

The allocation of Intellectual Property Rights among STCS participants are governed by the applicable agreements.

The STCS PA retains exclusive rights to any products or information developed under or pursuant to the STCS Identity CA CPS.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 STCS INDENTITY CA REPRESENTATIONS AND WARRANTIES

STCS Identity CA provides representations and warranties in accordance with this CPS, respective agreements and applicable laws and regulations as below:

- Providing the operational infrastructure and certification services;
- Making reasonable efforts to ensure it conducts an efficient and trustworthy operation. “Reasonable efforts” include but are not limited to operating in compliance with:
  - Documented CP, PDS and CPS;
  - Documented STCS Operations Policies and Procedures; and
  - Within applicable agreements, Saudi Law and regulations.
- At the time of Certificate issuance; STCS Identity CA implemented procedures for verifying accuracy of the information contained within it before installation and first use;
- Implemented procedures for reducing the likelihood that the information contained in the Certificate is not misleading;
- Maintaining 24x7 publicly accessible repositories with current information and replicates STCS Identity CA issued certificates and CRLs;
- For the CA’s, the Hardware Security Modules (HSM’s) used for key generation meet the requirements of FIPS 140-2 Level 3 to store the CA keys and take reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key CA private key is generated using multi-person control “m-of-n” split key knowledge scheme;
- Backing up of the CA signing Private Key is under the same multi-person control as the original Signing Key;
- Keep confidential, any passwords, PINs or other personal secrets used in obtaining authenticated access to PKI facilities and maintain proper control procedures for all such personal secrets;
- Use its private signing key only to sign certificates and CRLs and for no other purpose;
- Perform authentication and identification procedures in accordance with applicable Agreement and STCS Operations Policies and Procedures;
- Provide certificate and key management services in accordance with the CP and CPS; and

- Ensure that CA personnel use private keys issued for the purpose of conducting CA duties only for such purposes.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

The STCS Identity CA requires all RAs under its PKI Hierarchy to warrant that they are in compliance with the CP and may choose to include additional representations within this CPS or RA agreement.

9.6.3 RELYING PARTIES REPRESENTATIONS AND WARRANTIES

Relying Parties who rely upon the certificates issued under the STCS Identity CA PKI shall:

- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- Verify the Validity by ensuring that the Certificate has not expired;
- Establish trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by the X.509 Version 3 amendment;
- Ensure that the Certificate has not been suspended or revoked by accessing current revocation status information available at the location specified in the Certificate to be relied upon; and
- Determining that such Certificate provides adequate assurances for its intended use.

9.6.4 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

Subscribers are human individuals or organization entities to which certificates are issued.

1. It is the responsibility of the Subscriber to:
    - Provide accurate and complete information at all times to the CA/RA, both in the certificate request and verification process defined by the CA/RA for specific Certificate type to be supplied by the STCS Identity CA;
    - Review and verify the Certificate contents for accuracy;
    - Secure private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware token, or other activation data that is used to control access to the Subscriber's private key;
    - Use the Subscriber Certificate only for its intended uses as specified by the STCS Identity CA;
    - Notify the CA/RA in the event that any information in the Certificate is, or becomes, incorrect or inaccurate;
    - Notify the CA/RA in the event of a key compromise immediately whenever the Subscriber has reason to believe that the Subscriber's private key has been lost, accessed by another individual, or compromised in any other manner;
    - Use the Subscriber Certificate in a manner that does not violate applicable laws in the Kingdom of Saudi Arabia; and
    - Upon termination of Subscriber Agreement, revocation or expiration of the Subscriber Certificate, immediately cease use of Private Key corresponding to the Public Key included in the Subscriber Certificate.

2. Subscriber agrees that any use of the Subscriber Certificate to sign or otherwise approve the contents of any electronic record or message is attributable to Subscriber. Subscriber agrees to be legally bound by the contents of any such electronic record or message.
3. Subscriber shall indemnify and hold the STCS Identity CA or RA acting on behalf of the STCS Identity CA, harmless from and against any and all damages (including legal fees), losses, lawsuits, claims or actions arising out of:
    - Use of Subscriber's Certificate in a manner not authorized by the STCS Identity CA or otherwise inconsistent with the terms of this Subscriber Agreement or the STCS Identity CA;
    - A Subscriber Certificate being tampered with by the Subscriber; or
    - Inaccuracies or misrepresentations contained within the Application. A Subscriber shall indemnify and hold the CA/RA harmless against any damages and legal fees that arise out of lawsuits, claims or actions by third parties who rely on or otherwise use Subscriber's Certificate, where such lawsuit, claim, or action relates to a Subscriber's breach of its obligations outlined in this Subscriber Agreement or the STCS Identity CA, a Subscriber's use of or reliance upon a Subscriber Certificate in connection with its business operations, a Subscriber's failure to protect its private key, or claims pertaining to content or other information or data supplied, or required to be supplied, by Subscriber.

9.7 DISCLAIMERS OF WARRANTIES

STCS, through its associated components, seeks to provide digital certification services according to international standards and best practices, using the most secure physical and electronic installations.

The STCS Identity CA provides no warranty, express, or implied, statutory or otherwise and disclaims any and all liability for the success or failure of the deployment of the STCS Identity CA or for the legal validity, acceptance or any other type of recognition of its own certificates, those issued by it, any digital signature backed by such certificates, and any products provided by STCS. The STCS Identity CA further disclaims any warranty of merchantability or fitness for a particular purpose of the above-mentioned certificates, digital signatures and products.

9.8 LIMITATIONS OF LIABILITY

Limitations on Liability:

- The STCS Identity CA will not incur any liability to any person to the extent that such liability results from their negligence, fraud or willful misconduct;
- The STCS Identity CA assumes no liability whatsoever in relation to the use of Certificates or associated Public-Key/Private-Key pairs issued under Certificate Policy for any use other than in accordance with Certificate Policy. Relying Parties will immediately indemnify the STCS Identity CA from and against any such liability and costs and claims arising there from;
- The STCS Identity CA will not be liable to any party whosoever for any damages suffered whether directly or indirectly as a result of an uncontrollable disruption of its services;
- Relying Parties shall bear the consequences of their failure to perform the Relying Party obligations described in the Relying Party agreement;

- STCS Identity CA denies any financial or any other kind of responsibility for damages or impairments resulting from its CA operation.

9.9 INDEMNITIES

Notwithstanding any limitations on its liability to its Sub-CAs and Relying Parties, STCS understands and acknowledges that the Application Software Suppliers who have supplied the CA software in use by the STCS Identity CA do not assume any obligation or potential liability of the STCS Identity CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, the STCS Identity CA SHALL defend, indemnify and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

The STCS Identity CA shall indemnify, defend and hold harmless the following parties:

- STCS, its directors, officers, employees, agents, consultants, and subsidiaries from any and all claims, damages, costs (including, without limitation, attorney's fees), judgments, awards or liability;
- Any parties relying on the STCS Intermediary Certificates or arising as a result of an infringement or violation of any patents, copyrights, trade secrets, licenses, or other property rights of any third party.

9.10 TERM AND TERMINATION

9.10.1 TERM

This CPS shall be effective upon approval by the STCS PKI Committee. The NCDC shall be notified of all changes to this document. Once the CPS becomes effective it is published in the repository. Amendments to this CPS upon approval become effective and replace the older version in the repository.

9.10.2 TERMINATION

This CPS as amended from time to time shall remain in force until it is replaced by a new version. The latest version of the STCS Identity CA CPS can be found at: https://www.stcs.com.sa/repository.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

Upon termination of this CPS, all STCS Identity CA participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

All communication between NCDC, NCDC PA, Saudi National Root-CA, and STCS Identity CA shall be in writing or via digitally signed communication. If in writing, the communication shall be signed on the appropriate organization letterhead. If electronically, a Digital Signature shall be made using a Private Key whose companion Public Key is certified using a Certificate meeting this CPS's Certificate assurance level.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

The STCS Identity CA shall review this CPS at least once per year. Errors, updates, or suggested changes to this CPS shall be communicated to STCS and/or NCDC. Such communication shall include a description of the change, a change justification, and contact information for the person requesting the change. Any technical changes in the STCS Identity CA shall be managed as per the STCS Change Management Policy.

STCS Identity CA reserves the right to change this CPS from time to time. STCS Identity CA will incorporate any such change into a new version of this CPS and, upon approval, publish the new version. The new CPS will carry a new version number.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

This CPS and any subsequent changes shall be made available to the STCS Identity CA participants within two weeks of approval. The STCS Identity CA reserves the right to amend this CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URL's, and changes to contact information. All the STCS PKI participants and other parties designated by the STCS Identity CA shall provide their comments to the STCS Identity CA in accordance with its rules. The STCS Identity CA's decision to designate amendments as material or non-material shall be at STCS Identity CA's sole discretion.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

The policy OID shall only change if the change in the CPS results in a material change to the trust by the relying parties, as determined by the STCS Identity CA.

9.13 DISPUTE RESOLUTION PROCEDURES

The use of certificates issued by the STCS Identity CA is governed by contracts, agreements, and standards set forth by STCS. Those contracts, agreements and standards include dispute resolution policy and procedures that shall be employed in any dispute arising from the issuance or use of a certificate governed by this CPS. Dispute Resolution mechanism is described in STCS Dispute Resolution Policy.

9.14 GOVERNING LAW

This CPS is governed by the laws of the Kingdom of Saudi Arabia.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to applicable national, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 ENTIRE AGREEMENT

No stipulation.

9.16.2 ASSIGNMENT

Except where specified by other contracts, no party may assign or delegate this CPS or any of its rights or duties under this CPS, without the prior written consent of the STCS PA.

9.16.3 SEVERABILITY

Should it be determined that one section of this CPS is incorrect or invalid, the other sections of this CPS shall remain in effect until the CPS is updated. The process for updating this CPS is described in section 9.12.

9.16.4 ENFORCEMENT (ATTORNEY FEES/WAIVER OF RIGHTS)

This document shall be treated according to laws of Kingdom of Saudi Arabia. Legal disputes arising from the operation of the STCS Identity CA will be treated according to laws of Kingdom of Saudi Arabia.

9.16.5 FORCE MAJEURE

The STCS Identity CA shall not be liable for any failure or delay in its performance under this CPS due to causes that are beyond its reasonable control, including, but not limited to, an act of God, act of civil or military authority, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and reasons beyond provisions of the governing law.

9.17 OTHER PROVISIONS

9.17.1 FIDUCIARY RELATIONSHIPS

Nothing contained in this CPS shall be deemed to constitute either STCS, or any of its subcontractors, agents, officers, suppliers, employees, partners, principals, or directors to be a partner, Affiliate, trustee, of any Relying Party or any third party, or to create any fiduciary relationship between the STCS Identity CA and any Relying party, or any third party, for any purpose whatsoever.

Nothing in this CPS or any Agreement between a third party and a Relying Party shall confer on any Customer, Relying Party, Applicant or any third party, any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf of the STCS Identity CA.

9.17.2 ADMINISTRATIVE PROCESSES

As specified in STCS Operations Policies and applicable Agreement

APPENDIX-A: CERTIFICATE TYPES

A.1 CERTIFICATE TYPES SUPPORTED

A1.1 DIGITAL IDENTITY CERTIFICATE SERVICE (IDS)

A.1.1.1 Digital Identity Certificate issuance requirements And Usage : LOW Assurance Certificate (LAC)

S. No.	Attribute	Digital Identity Certificate
1	Policy Name	STCS Low Assurance Digital Identity Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.21.5**
3	Subject	"CN=<English-Firstname> <English-Secondname> <English-Thirdname> <English-Lastname> <Arabic-Lastname> <Arabic-Thirdname> <Arabic-SecondName> <Arabic-FirstName> , **OU=<Low Assurance>,**OU=<optional searchbase(s)>, OU = STCS IDCA,O = STCS, C = SA".
4	Application Usage	STCS Digital Identity Certificates are subscriber certificates intended to identify or authenticate subscribers. They are issued under the STCS Identity CA (STCS IDCA). These Digital Identity certificates comply with the requirements of **Low Assurance Level** certificates as per Saudi National PKI Policy. These certificates are general purpose certificates that are not tied to any specific application or function. The applications using the STCS IDCA issued Digital Identity Certificates should honour Key Usage set in the certificates The Digital Identification certificate may also be used for other general or specific STCS IDCA purposes which are not covered explicitly above, provided that a Relying Party is able to reasonably rely on that certificate and the usage is as per the STCS IDCA practices, Subscribers agreement and not otherwise prohibited by law of Saudi Arabia. LOW Assurance Certificates are not Permitted to be issued to Organizations.
5	Verification Process	1. Applicant to submit application to the RA 2. ONLY email verification will be performed against the claimed identity. The RA verify that the subscriber's email exists and that the subscriber has control of the email address. 3. No binding of the identity of the applicant to the certificate will be done 4. The RA will validate the application and confirm applicant is the sole claimant of the identity to be included in the certificate
6	Key Pair Generation and Installation	Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys. **Low Assurance Certificate Keys are generated in Software.**
7	Certificate Issuance Process	Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following: • The applicant can apply for the certificate remotely without the need to visit the RA • RA shall confirm application for correctness and approve if all is in order • RA shall start the process of key generation and request certificate (subscriber will be required to input password to protect the private key) • If the subscriber generates his own keys, the RA shall confirm that the subscriber is in possession of the Private key corresponding to the certificate request. • The CA shall sign the request after validating it is from an approved RA
8	Key Usage	Digital Identification certificate and keys shall be used for authentication of/by name only.

S. No.	Attribute	Digital Identity Certificate
9	Private Key Protection	Private keys are generated in Software and subscribers shall protect the password that unlocks the private key
10	Certificate Lifetime	Up to 36 months (3 years)
11	Key Backup	The STCS IDCA shall not take any backup of the private keys of this certificate type.
12	Asymmetric Key Length	Minimum 2048 bits RSA
13	Certificate Re-key	Certificate re-key shall take place if a certificate has expired or is nearing expiry provided the certificate is not revoked and the subscriber information is still accountable In case of certificate rekey requested after expiry, a letter of permission from the appropriate signing authority is required for re-key of a Subscriber's certificate addressing the Subscriber and mentioning the type of certificate to be re-keyed. The Subscriber shall submit documents for identity validation and supporting documents for certificate re-key and follow the procedure as per the certificate issuance process. In case of certificate nearing expiry (as set in the CA policies), the re-key process may be performed by a supported client without revocation of the existing certificate.

A.1.1.2 Digital Identity Certificate issuance requirements And Usage : MEDIUM Assurance Certificate (MAC)

S. No.	Attribute	Digital Identity Certificate
1	Policy Name	STCS Medium Assurance Digital Identity Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.21.6**
3	Subject	"CN=<English-Firstname> <English-Secondname> <English-Thirdname> <English-Lastname> <Arabic-Lastname> <Arabic-Thirdname> <Arabic-SecondName> <Arabic-FirstName> <Organization Name> , **OU=<Medium Assurance>**,OU=<optional searchbase(s)>, OU = STCS IDCA,O = STCS, C = SA".
4	Application Usage	STCS Digital Identity Certificates are subscriber certificates intended to identify or authenticate subscribers (human subscribers or organizations). They are issued under the STCS Identity CA (STCS IDCA). These Digital Identity certificates comply with the requirements of **Medium Assurance Level** certificates as per Saudi National PKI Policy. These certificates are general purpose certificates that are not tied to any specific application or function. The applications using the STCS IDCA issued Digital Identity Certificates should honour Key Usage set in the certificates The Digital Identification certificate may also be used for other general or specific STCS IDCA purposes which are not covered explicitly above, provided that a Relying Party is able to reasonably rely on that certificate and the usage is as per the STCS IDCA practices, Subscribers agreement and not otherwise prohibited by law of Saudi Arabia. Medium Assurance Certificates can be issued to Natural Persons or Legal Persons (Organizations)
5	Verification Process	**A) Natural Persons** • Subscriber provide shall provide government issued identity document • Check that the subscriber is the sole claimant of the identity • RA to check the existence of the email address supplied and that the subscriber has control over it

S. No.	Attribute	Digital Identity Certificate
		• RA to check the government issued identity document and verify against authoritative sources for validity • A binding of the claimed identity shall be performed by checking the link between the claimed identity and the provided documents **B) Legal Persons (Organizations)** • Company or legal documents from a company registration authority shall be provided and verified • Identity document of the applicant and the authorization that confirms the permission to apply the certificate on behalf of the organization to be provided, and that the applicant is a member of the organization • RA shall verify the existence of the email address provided and that the subscriber/applicant has control over the email address • RA shall verify the existence of the organization by using a public register
6	Key Pair Generation and Installation	Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys. Subscriber may use Hardware Security device like smart card / tokens for key generation and storage. Software generated keys are also supported, provided the process complies with the requirements of FIPS 186. **If generated in Cryptographic device, the device must be certified to at least FIPS 140-2 Level 2 .** In addition, the Subscriber shall acknowledge receipt of the private key(s).
7	Certificate Issuance Process	Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following: • The Subscriber will be present at the RA for face-to-face identity verification or an equivalent electronic identity verification process • The RA will validate the documents submitted by the subscriber • The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner. • The subscriber will go to the RA customization centre (or remotely for software generated keys) • The Subscriber will plug his smart card / USB token into the customization device. • The Subscriber will enter the PIN of the smart card / USB token • The Subscriber will enter reference number and an authorization code to generate keys and download certificates. • The Client Software will generate the Subscriber's keys securely on his smart card / USB token. • The RA will authenticate the Subscriber using the reference number and authorization code and receive the certificate signing request using a secure protocol such as PKIX-CMP. Upon successful authentication, the RA shall request for the creating of the Subscribers certificates and transport them securely onto the Subscriber's smart cards / USB tokens once approved by the CA. **Software generated keys shall follow the same process, except there will be no cryptographic device for key generation or storage. Instead the certificate shall be made available via a PKCS#12 formatted file.**
8	Key Usage	Digital Identification certificate and keys shall be used for authentication of/by name only.
9	Private Key Protection	For keys generated in Software, Subscribers shall protect the password that unlocks the private key. For keys generated in Cryptographic devices, Subscribers shall protect their private keys in a FIPS 140-2 Level 2 or higher certified smart card or other hardware token/module. A Subscriber is obligated to secure the private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password,

S. No.	Attribute	Digital Identity Certificate
		hardware token, or other activation data that is used to control access to the Subscriber's private key. Generation and/or Storage of the authentication private keys shall only be done in FIPS 140-2 Level 2 or higher certified hardware.
10	Certificate Lifetime	Up to 36 months (3 years)
11	Key Backup	The STCS IDCA shall not take any backup of the private keys of this certificate type.
12	Asymmetric Key Length	Minimum 2048 bits RSA
13	Certificate Re-key	Certificate re-key shall take place if a certificate has expired or is nearing expiry provided the certificate is not revoked and the subscriber information is still accountable In case of certificate rekey requested after expiry, a letter of permission from the appropriate signing authority is required for re-key of a Subscriber's certificate addressing the Subscriber and mentioning the type of certificate to be re-keyed. The Subscriber shall be required to physically attend to the RA (or use the alternate approved process) for identity validation and submission of supporting documents for certificate re-key and follow the procedure as per the certificate issuance process. In case of certificate nearing expiry (as set in the CA policies), the re-key process may be performed by a supported client without revocation of the existing certificate. For token-based certificates, the subscriber still needs to present the token to the RA for the re-key process to take place.

A.1.1.3 Digital Identity Certificate issuance requirements And Usage: HIGH Assurance Certificate (HAC)

S. No.	Attribute	Digital Identity Certificate
1	Policy Name	STCS Digital Identity Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.21.7**
3	Subject	"CN=<English-Firstname> <English-Secondname> <English-Thirdname> <English-Lastname> <Arabic-Lastname> <Arabic-Thirdname> <Arabic-SecondName> <Arabic-FirstName> , **OU=<High Assurance>,**OU=<optional searchbase(s)>, OU = STCS IDCA,O = STCS, C = SA".
4	Application Usage	STCS Digital Identity Certificates are subscriber certificates intended to identify or authenticate subscribers. They are issued under the STCS Identity CA (STCS IDCA). These Digital Identity certificates comply with the requirements of **High Assurance Level** certificates as per Saudi National PKI Policy. These certificates are general purpose certificates that are not tied to any specific application or function. The applications using the STCS IDCA issued Digital Identity Certificates should honour Key Usage set in the certificates The Digital Identification certificate may also be used for other general or specific STCS IDCA purposes which are not covered explicitly above, provided that a Relying Party is able to reasonably rely on that certificate and the usage is as per the STCS IDCA practices, Subscribers agreement and not otherwise prohibited by law of Saudi Arabia.
5	Verification Process	**C) Natural Persons** • Subscriber provide shall provide government issued identity document • Check that the subscriber is the sole claimant of the identity

S. No.	Attribute	Digital Identity Certificate
		• A secondary feature such as a Biometric of the applicant shall be used • RA to check the existence of the email address supplied and that the subscriber has control over it • RA to check the government issued identity document and verify against authoritative sources for validity • A binding of the claimed identity shall be performed by checking the link between the claimed identity and the provided documents **D) Legal Persons (Organizations)** • Company or legal documents from a company registration authority shall be provided and verified • Identity document of the applicant and the authorization that confirms the permission to apply the certificate on behalf of the organization to be provided, and that the applicant is a member of the organization • RA shall verify the existence of the email address provided and that the subscriber/applicant has control over the email address • RA shall verify the existence of the organization by using a public register
6	Key Pair Generation and Installation	Key Pair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys, subscriber shall use Hardware Security device like smart card / tokens for key generation and storage. **All Digital Identification certificates MUST be generated and stored on the secured hardware meeting the minimum requirements as mentioned in the STCS Identity CA CP.** The Digital Identification Private keys must be generated and stored on FIPS 140-2 Level 2 or higher certified hardware token or smart card, and the RA shall not retain any copy of the subscriber Private Keys. In addition, the Subscriber shall acknowledge receipt of the private key(s).
7	Certificate Issuance Process	Certificates shall only be issued to Saudi nationals or residents of the Kingdom as per the following: • The Subscriber will be present at the RA for face-to-face identity verification or an equivalent electronic identity verification process • The RA will validate the documents submitted by the subscriber • The RA will complete the registration and will issue a reference number and an authentication code to the subscriber in a secured manner. • The subscriber will go to the RA customization center • The Subscriber will plug his smart card / USB token into the customization device. • The Subscriber will enter the PIN of the smart card / USB token • The Subscriber will enter reference number and an authorization code to generate keys and download certificates. • The Client Software will generate the Subscriber's keys securely on his smart card / USB token. • The RA will authenticate the Subscriber using the reference number and authorization code and receive the certificate signing request using a secure protocol such as PKIX-CMP. Upon successful authentication, the RA shall submit the request for certificate to the CA, which shall in turn sign the request and issue the Subscribers' certificates and transport them securely onto the Subscriber's smart cards / USB tokens.
8	Key Usage	Digital Identification certificate and keys shall be used for authentication of/by name only.
9	Private Key Protection	Subscribers shall protect their private keys in a FIPS 140-2 Level 2 or higher certified smart card or other hardware token/module. Subscriber is obligated

S. No.	Attribute	Digital Identity Certificate
		to secure the private key and take reasonable and necessary precautions to prevent loss, disclosure, modification, or unauthorized use of the private key. This includes password, hardware token, or other activation data that is used to control access to the Subscriber's private key. Generation and/or Storage of name authentication private keys shall only be done in FIPS 140-2 Level 2 or higher certified hardware.
10	Certificate Lifetime	Up to 36 months (3 years)
11	Key Backup	The STCS IDCA shall not take any backup of the private keys of this certificate type.
12	Asymmetric Key Length	Minimum 2048 bits RSA
13	Certificate Re-key	Certificate re-key shall take place if a certificate has expired or is nearing expiry provided the certificate is not revoked and the subscriber information is still accountable In case of certificate rekey requested after expiry, a letter of permission from the appropriate signing authority is required for re-key of a Subscriber's certificate addressing the Subscriber and mentioning the type of certificate to be re-keyed. The Subscriber shall be required to physically attend to the RA (or use the alternate approved process) for identity validation and submission of supporting documents for certificate re-key and follow the procedure as per the certificate issuance process. In case of certificate nearing expiry (as set in the CA policies), the re-key process may be performed by a supported client without revocation of the existing certificate. The subscriber still needs to present the token to the RA for the re-key process to take place.

A.1.2 RA IDENTITY CERTIFICATE (RA CERTIFICATE)

This is the Registration Authority (RA) Certificate Issued by the STCS Identity CA. The RA certificate is used to authenticate RA application requests to the CA if so implemented.

A.1.2.1 RA Certificate issuance requirements And Usage

S. No.	Attribute	RA Certificate
1	Policy Name	STCS IDCA RA Identity Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.21.8**
3	Subject	"CN=<Organization Name>, OU=<optional searchbase(s)>, OU = STCS IDCA, O = STCS, C = SA"
4	Application Usage	STCS IDCA RA Certificates are RA Identity Certificates. They are specifically issued to identify and authenticate RA requests to the CA, such as requesting subscriber certificates. They will be used by the RA applications that are authorized to manage subscribers and the corresponding lifecycle of their certificates. The RA applications using the STCS IDCA issued RA Certificate should honour the Key Usage and any Extensions set in the certificate. The RA certificates shall comply with the requirements for a **Medium (or Substantial)** Level of Assurance (LoA) as described in the Saudi National PKI Policy.

5	Verification Process	The process of verifying the STCS RA Identity certificate request is done as part of the RA Take on process or contract renewal process. The following process shall apply: • The Request for an RA certificate shall be requested by the STCS PA or authorized RA representative • The request shall be accompanied by a signed RA Agreement. • The request shall also be accompanied by documented evidence of the RA approval • The Identity of the requesting party shall be verified. If the applicant is an external party, the applicant shall produce a government issued identity document.
6	Key Pair Generation and Installation	Keypair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys. Where Cryptographic devices are used, the STCS RA Keypairs shall be generated using devices meeting the stipulated FIPS 140-2 Level.
7	Certificate Issuance Process	The certificate is issued as part of the Key Ceremony Process A signed PKCS#10 formatted CSR is provided to the STCS Identity CA that shall in turn sign the request. The signed certificate shall be returned to complete the process of the STCS QUCA configuration
8	Key Usage	The RA Identity certificate and keys shall be used to authenticate by name only.
9	Private Key Protection	The STCS RA Certificate Private Keys shall be protected using a Hardware Security Module meeting FIPS140-2 Level 2 requirements.
10	Certificate Lifetime	Up to 36 months (3 years)
11	Key Backup	The STCS IDCA shall never backup the Private key of this type of certificate
12	Asymmetric Key Length	Minimum 2048 bits RSA
13	Certificate Re-key	Certificate re-key shall take place if a certificate has expired or is nearing expiry provided the certificate is not revoked and the subscriber information is still accountable In case of certificate rekey requested after expiry, a letter of permission from the appropriate signing authority is required for re-key of a Subscriber's certificate addressing the Subscriber and mentioning the type of certificate to be re-keyed. The Subscriber shall be required to physically attend to the RA (or use the alternate approved process) for identity validation and submission of supporting documents for certificate re-key and follow the procedure as per the certificate issuance process. In case of certificate nearing expiry (as set in the CA policies), the re-key process may be performed automatically by a supported client without revocation of the existing certificate.

A.1.3 ONLINE CERTIFICATE STATUS PROTOCOL CERTIFICATE (OCSP CERTIFICATE)

The OCSP certificate is issued to the OCSP responder service. The certificate is used to sign OCSP requests.

A.1.3.1 OCSP Certificate issuance requirements And Usage

S. No.	Attribute	RA Certificate
1	Policy Name	STCS IDCA OCSP Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.21.9**
3	Subject	"CN=<OCSP Responder Name>, OU=<optional searchbase(s)>, OU = STCS IDCA, O = STCS, C = SA"
4	Application Usage	STCS IDCA OCSP Certificates are used for signing of OCSP responses. They are specifically issued to sign responses from an OCSP responder service. The OCSP Responder applications using the STCS IDCA issued OCSP Certificate should honour the Key Usage and any Extensions set in the certificate. The OCSP certificates shall comply with the requirements for a **Medium (or Substantial)** Level of Assurance (LoA) as described in the Saudi National PKI Policy.
5	Verification Process	The process of verifying the STCS OCSP certificate request is done as part of setting up the CA services (immediately after a Key Ceremony). The following process shall apply: • The Request for the OCSP certificate shall be requested by the STCS PA or authorized CA representative • The request shall be accompanied by documented evidence of the OCSP Responder service approval • The Identity of the requesting party shall be verified.
6	Key Pair Generation and Installation	Keypair generation must be performed using trustworthy systems and processes that provide the required cryptographic strength of the generated keys, and prevent the loss, disclosure, modification, or unauthorized use of such keys. Where Cryptographic devices are used, the STCS RA Keypairs shall be generated using devices meeting the stipulated FIPS 140-2 Level.
7	Certificate Issuance Process	A signed PKCS#10 formatted CSR is provided to the STCS Identity CA that shall in turn sign the request. The signed certificate shall be returned to complete the process of the STCS IDCA OCSP Responder configuration
8	Key Usage	The STCS IDCA OCSP certificate and keys shall be used to digitally sign responses.
9	Private Key Protection	The STCS IDCA OCSP Certificate Private Keys shall be protected using a Hardware Security Module meeting FIPS140-2 Level 2 requirements.
10	Certificate Lifetime	Up to 36 months (3 years)
11	Key Backup	The STCS IDCA shall never backup the Private key of this type of certificate
12	Asymmetric Key Length	Minimum 2048 bits RSA
13	Certificate Re-key	Certificate re-key shall take place if a certificate has expired or is nearing expiry provided the certificate is not revoked and the subscriber information is still accountable In case of certificate nearing expiry (as set in the CA policies), the re-key process may be performed automatically by a supported client without revocation of the existing OCSP certificate.