STCS INTERMEDIARY CA

CERTIFICATION PRACTICE STATEMENT

Document Classification : Public

Version Number : 1.7

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 Intermediary CA Certificate Practice Statement
Custodian Department:	STCS Cybersecurity
Owner:	STCS Policy Authority
Version Number:	1.7
Document Status:	Final

Author(s):	Katekani Hlabathi	
	Security Consultant	Signature/Date
Reviewer:	Ahmed E. Abdelhamid	Ahmed E. Abdelhamid
	STCS Cybersecurity Advisory	Signature/Date
Official Reviewer:	Mohamed A. Breik	Signed by: Mohamed A. Breik Signed at: 2019-12-23 18:28:18 Reason: Witnessing Mohamed A.
	STCS Cybersecurity Advisory	Signature/Date
Approved by:	Fahad I. Aljutaily	Signed by: faljutaily Signed at: 2019-12-23 22:07:46 Reason: Witnessing faljutaily
	STCS Cybersecurity VP (STCS PKI Committee Chair)	Signature/Date

Document Revision History

Version	Date	Author(s)	Revision Notes
1.0	17/02/2019	STCS	Initial Draft
1.1	07/08/2019	K Hlabathi	Final Draft
1.2	02/09/2019	M de Waal, K Hlabathi	Final
1.3	18/09/2019	Katekani Hlabathi	Final incorporating NCDC comments
1.4	03/10/2019	Katekani Hlabathi	Final incorporating second Deloitte and NCDC review. Split document into separate CPS'es for all CAs
1.5	26/11/2019	Katekani Hlabathi	Final document for NCDC final review
1.6	16/12/2019	Katekani Hlabathi	Final document for approval and publishing
1.7	23/12/2019	Katekani Hlabathi	Added one more signatory. For signatures 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 Qualified CA (STCS QUCA) 13
1.3.4 STCS Identity CA (STCS IDCA) 13
1.3.5 STCS Policy Authority (STCS PA) 13
1.3.6 STCS PKI Committee 13
1.3.7 Relying Parties 14

1.4 Certificate Usage 14
1.4.1 Appropriate Certificate Uses 14
1.4.2 Prohibited Certificate Uses 14

1.5 Policy Administration 14
1.5.1 Administration Organization 14
1.5.2 Contact Person 14
1.5.3 Person Determining CPS Suitability for the Policy 15
1.5.4 CPS Approval 15

1.6 Definitions and Acronyms 15

2 Publication and Repository Responsibilities 15

2.1 Repositories 15
2.1.1 Repository Obligations 15

2.2 Publication of Certification Information 16
2.2.1 Publication of Certificates and Certificate Status 16
2.2.2 Publication of CA Information 16
2.2.3 Interoperability 16

2.3 Time or Frequency of Publication 17

2.4 Access Controls on Repositories 17

3 Identification and Authentication 17

3.1 Naming 17
3.1.1 Types of Names 17
3.1.2 Need for Names to be Meaningful 17
3.1.3 Anonymity or Pseudonymity of Subscribers 18
3.1.4 Rules for Interpreting Various Name Forms 18
3.1.5 Uniqueness of Names 18
3.1.6 Recognition, Authentication and Role of Trademarks 18

3.2 Initial Identity Validation 18
3.2.1 Method to Prove Possession of Private Key 18
3.2.2 Authentication of Issuer Identity 19
3.2.3 Identity-Proofing of Individual Identity 19
3.2.4 Non-verified Subscriber Information 19
3.2.5 Validation of Authority 19

3.2.6 Criteria of Interoperation 19

3.3 Identification and Authentication for Re-key Requests 19
3.3.1 Identification and Authentication for Routine Re-Key 19
3.3.2 Identification and Authentication for Re-key After Revocation 20

3.4 Identification and Authentication for Revocation Requests 20

4 Certificate Life-Cycle Operational Requirements 20

4.1 Certificate Application 20
4.1.1 Submission of Certificate Application 21
4.1.2 Enrollment Process and Responsibilities 21

4.2 Certificate Application Processing 21
4.2.1 Performing Identity-proofing Functions 21
4.2.2 Approval or Rejection of Certificate Applications 21
4.2.3 Time to Process Certificate Applications 21

4.3 Certificate Issuance 22
4.3.1 CA Actions During Certificate Issuance 22
4.3.2 Notification of Certificate Issuance 22

4.4 Certificate Acceptance 22
4.4.1 Conduct Constituting Certificate Acceptance 22
4.4.2 Publication of the Certificate by the CA 22
4.4.3 Notification of Certificate Issuance by the CA to Other Entities 22

4.5 Key Pair and Certificate Usage 23
4.5.1 SUB-CA Private Key and Certificate Usage 23
4.5.2 Relying Party Public Key and Certificate Usage 23

4.6 Certificate Renewal 23

4.7 Certificate Re-Key 23
4.7.1 Circumstances for Certificate Re-key 24
4.7.2 Who can Request a Certificate Re-key 24
4.7.3 Processing Certificate Re-keying Requests 24
4.7.4 Notification of Re-Keyed Certificate Issuance to Subscriber 24
4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 24
4.7.6 Publication of the Re-keyed Certificate by the CA 24
4.7.7 Notification of Certificate Issuance by the CA to Other Entities 24

4.8 Certificate Modification 24

4.9 Certificate Revocation and Suspension 24
4.9.1 Circumstance for Revocation of a Certificate 25
4.9.2 Who Can Request Revocation of a Certificate 25
4.9.3 Procedure for Revocation Request 25
4.9.4 Revocation Request Grace Period 25
4.9.5 Time within which CA must Process the Revocation Request 26
4.9.6 Revocation Checking Requirements for Relying Parties 26
4.9.7 CRL Issuance Frequency 26
4.9.8 Maximum Latency of CRLs 26
4.9.9 Online Revocation Checking Availability 26
4.9.10 Online Revocation Checking Requirements 26
4.9.11 Other Forms of Revocation Advertisements Available 26
4.9.12 Special Requirements Related To Key Compromise 26
4.9.13 Circumstances for Certificate Suspension 26
4.9.14 Who Can Request Suspension 27
4.9.15 Procedure for Suspension Request 27

4.9.16 Limits on Suspension Period....27
4.9.17 Circumstances for Terminating Suspended Certificates....27
4.9.18 Procedure for Terminating the Suspension of a Certificate....27
4.10 Certificate Status Services....27
4.11 End of Subscription....27
4.12 Key Escrow and Recovery....27
5 Facility Management and Operational Controls....28
5.1 Physical Security Controls....28
5.1.1 Site Location and Construction....28
5.1.2 Physical Access....28
5.1.3 Power and Air Conditioning....29
5.1.4 Water Exposure....29
5.1.5 Fire Prevention and Protection....29
5.1.6 Media Storage....30
5.1.7 Waste Disposal....30
5.1.8 Off-Site Backup....30
5.2 Procedural Controls....30
5.2.1 Trusted Roles....30
5.2.2 Number of Persons Required per Task....32
5.2.3 Identity-proofing for Each Role....32
5.2.4 Separation of Roles....32
5.3 Personnel Controls....32
5.3.1 Background, Qualifications and Experience Requirements....32
5.3.2 Background Check and Clearance Procedures....32
5.3.3 Training Requirements And Procedures....33
5.3.4 Retraining Frequency and Requirements....33
5.3.5 Job Rotation Frequency and Sequence....33
5.3.6 Sanctions for Unauthorized Actions....33
5.3.7 Contracting Personnel Requirements....33
5.3.8 Documentation Supplied to Personnel....33
5.4 Audit Logging Procedures....34
5.4.1 Types of Events Recorded....34
5.4.2 Frequency of Processing Data....35
5.4.3 Retention Period for Audit LOG....35
5.4.4 Protection of Security Audit Data....35
5.4.5 Audit LOG Backup Procedures....35
5.4.6 Audit Collection System (Internal or External)....36
5.4.7 Notification to Event-Causing Subject....36
5.4.8 Vulnerability Assessments....36
5.5 Records Archival....36
5.5.1 Types of Events Archived....36
5.5.2 Retention Period for Archive....37
5.5.3 Protection of Archive....37
5.5.4 Archive Backup Procedures....37
5.5.5 Requirements for Time-Stamping of Records....37
5.5.6 Archive Collection System (Internal or External)....37
5.5.7 Procedures to Obtain and Verify Archive Information....38
5.6 Key Changeover....38
5.7 Compromise and Disaster Recovery....38
5.7.1 Incident and Compromise Handling Procedures....38

5.7.2 Recovery Procedures If Computing Resources, Software, and/or Data Are Corrupted....38
5.7.3 Recovery Procedure if CA Private Key is Compromised....39
5.7.4 Business Continuity Capabilities after a Disaster....39

5.8 CA Termination....40
5.8.1 CA Termination....40

6 Technical Security Controls....40

6.1 Key Pair Generation and Installation....40
6.1.1 Key Pair Generation....40
6.1.2 Private Key Delivery to end-entities....41
6.1.3 Public Key Delivery to Certificate Issuer....41
6.1.4 CA Public Key Delivery to Relying Parties....41
6.1.5 Key Sizes....41
6.1.6 Public Key Parameters Generation and Quality Checking....41
6.1.7 Key Usage Purposes....41

6.2 Private Key Protection and Crypto-Module Engineering Controls....42
6.2.1 Cryptographic Module Standards and Controls....42
6.2.2 CA Private Key Multi-Person Control....42
6.2.3 Private Key Escrow....42
6.2.4 Private Key Backup....42
6.2.5 Private Key Archival....42
6.2.6 Private Key Transfer Into or From a Cryptographic Module....42
6.2.7 Private Key Storage on Cryptographic Module....42
6.2.8 Method of Activating Private Keys....42
6.2.9 Methods of Deactivating Private Keys....43
6.2.10 Methods of Destroying Private Keys....43
6.2.11 Cryptographic Module Rating....43

6.3 Other Aspects of Key Pair Management....43
6.3.1 Public Key Archive....43
6.3.2 Certificate Operational Periods and Key Usage Periods....43

6.4 Activation Data....43
6.4.1 Activation Data Generation and Installation....43
6.4.2 Activation Data Protection....44
6.4.3 Other Aspects of Activation Data....44

6.5 Computer Security Controls....44
6.5.1 Specific Computer Security Technical Requirements....44
6.5.2 Computer Security Rating....44

6.6 Life-Cycle Security Controls....44
6.6.1 System Development Controls....44
6.6.2 Security Management Controls....45
6.6.3 Life Cycle Security Ratings....45

6.7 Network Security Controls....45

6.8 Time Stamping....46

7 Certificate, CRL and OCSP Profiles....46

7.1 Certificate Profile....46
7.1.1 Version Numbers....46
7.1.2 Certificate Extensions....46
7.1.3 Algorithm Object Identifiers....46
7.1.4 Name Forms....47
7.1.5 Name Constraints....47

7.1.6 Certificate Policy Object Identifier 47
7.1.7 Usage of Policy Constraints Extension 47
7.1.8 Policy Qualifiers Syntax and Semantics 47
7.1.9 Processing Semantics for the Critical Certificate Policy Extension 47

7.2 CRL Profile 47
7.2.1 STCS Intermediary CA CRL Profile 47
7.2.2 Version Numbers 48
7.2.3 CRL and CRL Entry Extensions 48

7.3 OCSP Profile 48
7.3.1 Version Number 48
7.3.2 OCSP Extensions 48

8 Compliance Audit and Other Assessments 48

8.1 Frequency of Audit or Assessments 48

8.2 Identity and Qualifications of Assessor 49

8.3 Assessor's Relationship to Assessed Entity 49

8.4 Topics Covered By Assessment 49

8.5 Actions Taken As A Result of Deficiency 49

8.6 Communication of Results 50

9 Other Business and Legal Matters 50

9.1 Fees 50
9.1.1 Certificate Issuance/Renewal Fee 50
9.1.2 Certificate Access Fees 50
9.1.3 Revocation or Status Information Access Fee 50
9.1.4 Fees for Other Services 50
9.1.5 Refund Policy 50

9.2 Financial Responsibility 50
9.2.1 Insurance Coverage 51
9.2.2 Other Assets 51
9.2.3 Insurance/warranty Coverage for End-Entities 51

9.3 Confidentiality of Business Information 51
9.3.1 Scope of Confidential Information 51
9.3.2 Information not within the Scope of Confidential Information 52
9.3.3 Responsibility to Protect Confidential Information 52

9.4 Privacy of Personal Information 52
9.4.1 Privacy Plan 52
9.4.2 Information Treated as Private 52
9.4.3 Information not Deemed Private 53
9.4.4 Responsibility to Protect Private Information 53
9.4.5 Notice and Consent to Use Private Information 53
9.4.6 Disclosure Pursuant to Judicial/Administrative Process 53
9.4.7 Other Information Disclosure Circumstances 53

9.5 Intellectual Property Rights 53

9.6 Representations and Warranties 53
9.6.1 STCS Intermediary CA Representations and Warranties 53
9.6.2 RA Representations and Warranties 54
9.6.3 Relying Parties Representations and Warranties 54
9.6.4 Subscriber Representations and Warranties 54

9.7 Disclaimers of Warranties 54

9.8 Limitations of Liability 55

9.9 Indemnities 55

9.10 Term and Termination 56

9.10.1 Term 56
9.10.2 Termination 56
9.10.3 Effect of Termination and Survival 56

9.11 Individual Notices and Communications with Participants 56

9.12 Amendments 56

9.12.1 Procedure for Amendment 56
9.12.2 Notification Mechanism and Period 56
9.12.3 Circumstances under which OID must be changed 57

9.13 Dispute Resolution Procedures 57

9.14 Governing Law 57

9.15 Compliance with Applicable Law 57

9.16 Miscellaneous Provisions 57

9.16.1 Entire Agreement 57
9.16.2 Assignment 57
9.16.3 Severability 58
9.16.4 Enforcement (Attorney Fees/Waiver of Rights) 58
9.16.5 Force Majeure 58

9.17 Other Provisions 58

9.17.1 Fiduciary Relationships 58
9.17.2 Administrative Processes 58

Appendix-A: Certificate Types & Policies 59

A.1 Certificate types supported 59

A1.1 STCS Intermediary CA Certificate 59
A.1.2 STCS QUCA Certificate 60
A.1.3 STCS IDCA Certificate 61

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 Intermediary Certification Authority. In particular, this CPS establishes the processes and procedures the STCS Intermediary CA follows to:

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

The STCS Intermediary 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 Intermediary CA.

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

This CPS complies with the stipulations of the STCS Intermediary Certificate Policy (CP), Saudi National PKI Certificate Policy and in line with Internet Request for Comment (RFC) 3647 [RFC 3647]. Sections that are not applicable to STCS Intermediary 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 Intermediate CA as governed by the STCS Intermediate CA Certificate Policy (STCS Intermediate CA CP). This applies only to the sub-CA certificates issued under the hierarchy of the SCTS Intermediary CA

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

- Securely managing the core infrastructure that supports the PKI hosted at the STCS data center, and
- Issuing, managing, revoking and renewing Level-2 Issuing CA certificates
- The technical, procedural and personnel management in accordance with the requirements of the STCS Intermediary CA CP.

The STCS Intermediary CA only issues sub-CA certificates and does not issue end subscriber certificates

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

It is the responsibility of all parties applying for or using a Digital Certificate issued under the STCS Intermediary CA CP, to read the CP and the PKI Disclosure Statement (PDS) to

understand the practices established for the lifecycle management of the Certificates issued by the STCS Intermediate CA.

1.1.1 CERTIFICATE POLICY

X.509 certificates issued by the STCS Intermediary 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 Intermediary CA as governed by the STCS Intermediary CA CP and related documents which describe STCS Intermediary CA requirements and use of Certificates.

1.1.3 SCOPE

This CPS applies to Subordinate CA certificates issued by the STCS Intermediary CA.

STCS operates a Public Key Infrastructure (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 Subordinate Issuing Certificate Authorities (Sub-CA) 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.

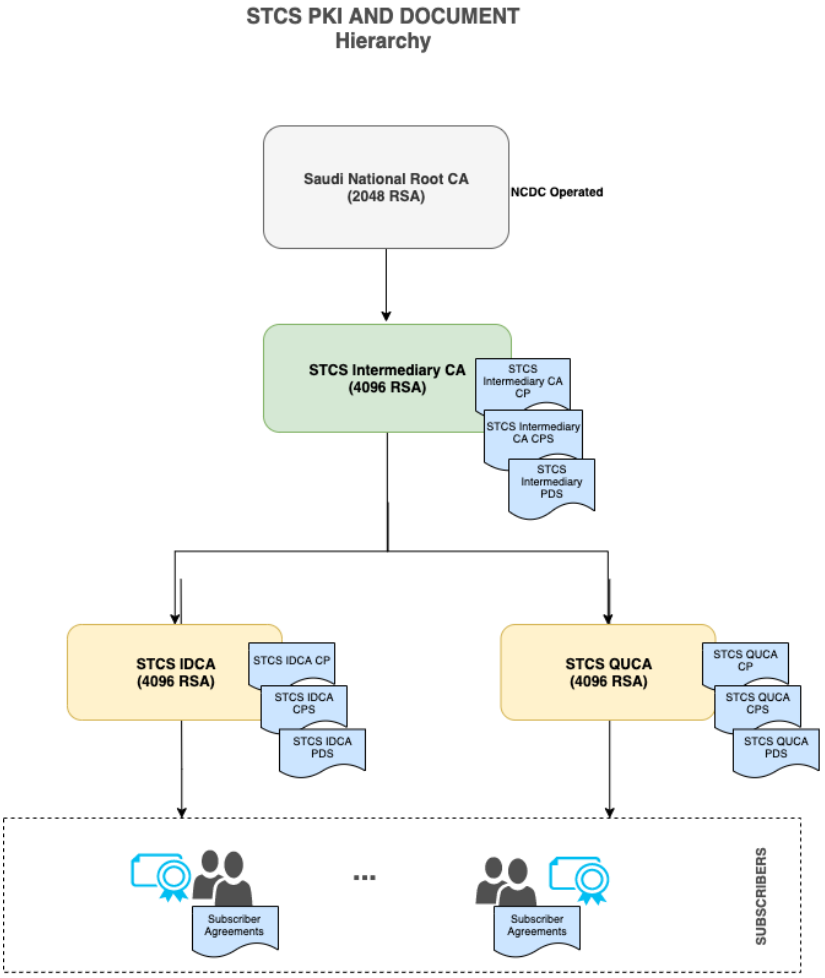

Figure 1. STCS PKI and Governance Hierarchy

1.2 Document Name and Identification

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

OID: 2.16.682.1.101.5000.1.4.1.2.1.2

1.3 PKI Participants

The following are roles relevant to the administration and operation of the STCS Intermediary CA under the STCS Intermediary CA CP.

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

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 (STCS QUCA and STCS IDCA) underneath in the PKI hierarchy.

1.3.3 STCS QUALIFIED CA (STCS QUCA)

The STCS QUCA is an issuing Certificate Authority under the STCS Intermediary CA. It issues certificates for the Digital Trust Services enabled by digital signature certificates.

1.3.4 STCS IDENTITY CA (STCS IDCA)

The STCS IDCA is an issuing Certificate Authority under the STCS Intermediary CA. It issues authentication certificates used to identify end subscribers. The subscribers can be individuals or organizational entities.

1.3.5 STCS POLICY AUTHORITY (STCS PA)

STCS Policy Authority (STCS PA) is a role within the STCS PKI responsible for the governance of the STCS PKI. The STCS PA is responsible for the following:

- Ensuring the operation of the STCS Intermediary CA comply with the requirements of the STCS Intermediary CA CP, PDS, CPS and STCS PKI Operations Policies and Procedures;
- Review and approve the Subscriber Agreement, Relying Party Agreement and other related Agreements based on the STCS PKI specific business requirements;
- Seeking resolution of disputes between participants operating in its domain;

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.

1.3.7 RELYING PARTIES

A Relying Party in this context is the entity that relies on the validity of the binding of the STCS Intermediate 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 Intermediate CA. A Relying Party's right to rely on a certificate issued under this CP, requirements for reliance, and limitations thereon, are governed by the terms of the STCS Intermediary 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 Intermediary CA CP if:

- The certificate has been used for the purpose for which it has been issued, as described in the STCS Intermediary 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.

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

STCS Intermediate CA only issues Sub-CA certificates for the issuing certificate authorities that are part of the PKI hierarchy. In particular it issues certificates to the STCS QUCA and STCS IDCA Certificate Authorities.

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 Intermediary 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 PA (Policy Authority) and is based on policies established under the STCS Intermediary CA CP (see section 1.3.1).

1.5.2 CONTACT PERSON

Queries regarding STCS Intermediary 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 approving this CPS and establishing that the STCS Intermediary CA conforms to the requirements of the STCS Intermediary 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 Intermediary CA issued certificates and certificate revocation lists (CRLs) will be published in repositories. STCS shall operate Repositories to support the STCS Intermediary 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 and replicates STCS Intermediary CA issued certificates and CRLs to additional repositories in order to enhance the overall performance and provide high availability for its validation services.

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 Intermediary CA CP; and
- Access control mechanisms when needed to protect repository availability and information.

The STCS Intermediary 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 Intermediary 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 Intermediary CA maintains repositories that allow Relying Parties to make on-line enquiries regarding revocation and other certificate status information. STCS Intermediary CA shall be providing Relying Parties with information on how to find the appropriate repository to check certificate status.

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

- Subordinate CA certificates: CA 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 CP shall be made available to all STCS Intermediary 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 Intermediary CA reserves the right to publish newer versions of the documentation without prior notice.

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

STCS Public LDAP directory and the website https://www.stcs.com.sa/repository are the only authoritative sources for:

- All publicly accessible certificates issued by STCS Intermediary CA; and
- The certificate revocation list (CRL) for the STCS Intermediary CA.

2.2.3 INTEROPERABILITY

Repository information is stored using technology that supports the following industry standards and schema:

- LDAP v3 operations;
- LDAP search filters;
- LDAP v3 intelligent referral;
- DSML (Directory Service Markup Language) v2;
- X.509 digital certificates;
- HTTP.

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 Intermediary 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 Intermediary CA PKI participants and other parties on a 24X7 basis as determined by the applicable agreements and STCS Privacy Policy, and subject to routine maintenance.

The STCS Intemediary CA 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.

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 Intermediary CA, STCS QUCA and STCS IDCA are approved by the STCS PKI Committee.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

The subject name contained in certificates issued under the STCS PKI Hierarchy must be meaningful in the sense that the STCS Intermediary CA is provided with proper evidence of the association existing between the name and the entity to which it belongs.

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

CN=STCS Intermediary CA, O=STCS, C=SA

The DN (LDAP Notation) in the Subject field of the Sub-CA certificates that are issued will be:

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

CN=STCS QUCA, O=STCS, CA=SA

The common name in the Subscriber DN will represent the Subscriber (in this case the Sub-CAs) in a way that is easily understandable for humans. The certificate types supported by the STCS Intermediary CA are covered in Appendix-A this document.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

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

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

STCS Intermediary 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 Intermediary CA's. Names shall not be re-used for another Sub-CA. After a Sub-CA certificate expires or is revoked, the name can be re-used to re-issue a certificate to the same Sub-CA.

The STCS Intermediary CA will be configured in such a manner as to enforce name uniqueness for certificates that it issues. The STCS Intermediary CA is responsible for ensuring name uniqueness in Sub-CA certificates issued by it. Additional naming attributes for uniquely identifying the subject include serial number, etc.

3.1.6 RECOGNITION, AUTHENTICATION AND ROLE OF TRADEMARKS

No Stipulation

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

The STCS Intermediary CA shall accept certificate signing requests (CSR) from the Issuing CAs that have demonstrated possession of the Private key by using a self-signed PKCS#10 request.

The STCS Intermediary CA shall inspect the contents of the CSR during the signing process and confirm that the details match those in the Key Ceremony Script 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 AUTHENTICATION OF ISSUER IDENTITY

The STCS Intermediary CA operates under the Saudi National PKI and as such complies with the requirements as set forth by the NCDC. The STCS Intermediary CA does not issue certificates to other entities other than its own Subordi Issuing CAs (IDCA and QUCA).

3.2.3 IDENTITY-PROOFING OF INDIVIDUAL IDENTITY

3.2.3.1 Identity-Proofing of End User Subscribers

No stipulation. The STCS Intermediary CA does not issue certificates to end users

3.2.3.2 Identity-Proofing of Device Subscribers

No stipulation.

3.2.3.3 Identity-Proofing of Organizational Entities

No Stipulation.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

No Stipulation.

3.2.5 VALIDATION OF AUTHORITY

The STCS PKI Committee shall verify the rights conferred to the applicant of a Subordinate Issuing CA to request a certificate. The approval together with a form of identity shall be verified as part of the Key Ceremony process.

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

The usage periods for the Sub-CA private keys are described in section 6.3.2. During the Re-keying process the STCS Intermediary 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.

The authentication of a Routine Re-key shall follow the same procedure as the initial certificate issuance. This shall be performed as part of a scripted Key Ceremony.

3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION

Where the information contained in a Sub-CA certificate has changed or there is a known or suspected compromise of the private key, the STCS Intermediary CA must authenticate a re-key in the same manner as for initial registration. A Key Ceremony process shall be constituted and followed to generate new keys for the revoked Sub-CA certificate.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

Prior to the revocation of a Sub-CA certificate, the STCS PKI Committee shall verify that the revocation has been requested by an authorized person.

Acceptable procedures for authenticating the revocation requests include:

- A request for revocation of a Sub-CA is initiated by an authorized person within STCS, such as the Policy Authority;
- The STCS PKI Committee shall approve such requests
- Revocation of the Sub-CA shall be performed using a scripted and witnessed process.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The STCS PKI Committee shall consider applications for Sub-CA certificate generation as part of a new CA establishment. The STCS PKI Committee shall only accept applications for Sub-CA establishment from Trusted employees within STCS.

The STCS PKI Committee shall perform the following steps when an application for a new certificate is received:

- Establish the applicant’s authorization to request the establishment of a CA;
- Establish and record the identity of the applicant;
- Verify the existence of a signed request to establish the Sub-CA.
- Approve the Key generation Script and set the date for the Key Ceremony

The STCS Intermediary CA will perform the following after approval by the STCS PKI Committee:

- Constitute the Key Shareholders and relevant parties for the STCS Intermediary CA;
- Activate the STCS Intermediate CA key;
- Generate the Certificate relating to that Sub-CA; and
- Transmits the Certificate to the requesting Sub-CA.
- Publish the Sub-CA key to the repository

4.1.1 SUBMISSION OF CERTIFICATE APPLICATION

Applications for the establishment of internal Sub-CAs under the STCS Intermediary CA shall be made to the STCS PKI Committee. The STCS PKI Committee shall consider the request and advice the requester of the outcome.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

4.1.2.1 Issuing CAs

The authorized personnel shall make the enrolment request for a new Sub-CA to the STCS PKI Committee. The following documentation shall at minimum accompany such a request:

- Formal request form
- Sub-CA Key Generation Script
- Other supporting documentation

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTITY-PROOFING FUNCTIONS

No Stipulation.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

The STCS PKI Committee will approve an application for a Sub-CA certificates if the following criteria are met;

a. Successful identification and authentication of the requesting party.
b. Requisite documentation is provided
c. The request for the Sub-CA establishment is not inconsistent with the requirement and provisions of the STCS Intermediary CP and this CPS

The STCS PKI Committee will reject a certificate application if:

a. Identification and authentication of the requesting party cannot be completed;
b. The requester fails to furnish supporting documentation upon request; or
c. The STCS PKI Committee believes that approving the establishment of the Sub-CA may bring the STCS Intermediary CA into disrepute or such an establishment is unlawful or inconsistent with the STCS Intermediary CA or Saudi National PKI Policies.

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

The STCS PKI Committee shall process the applications as soon as is reasonably possible after receipt of such applications. The time to process the application shall not exceed 90 days.

4.3 CERTIFICATE ISSUANCE

The STCS Intermediary CA shall issue Sub-CA certificates following the approval by the STCS PKI Committee.

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

Following successfully completion of the registration process, the STCS Intermediary CA will create and sign the Sub-CA 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 Intermediary CA

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

4.3.2 NOTIFICATION OF CERTIFICATE ISSUANCE

The STCS Intermediary CA shall notify the requesting party or applicant immediately of the issuance of the certificate. The issuance of the Sub-CA certificate is performed as part of a scripted Key Ceremony process.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

On receipt of the signed certificate from the STCS Intermediary CA, the Sub-CA may be established, and this action constitutes acceptance of the certificate by the Sub-CA.

The use of the Sub-CA Certificate or the reliance upon the Certificate signifies acceptance by that person of the terms and conditions of the CP and applicable agreements by which they irrevocably agree to be bound.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

The Sub-CA 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 SUB-CA PRIVATE KEY AND CERTIFICATE USAGE

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

Sub-CAs 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 Intermediary 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 Intermediary 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 Intermediary CA issued certificates to Sub-CAs. The conditions for Sub-CA renewals are as stipulated in the STCS Intermediary CA CP document.

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 private key.

4.7.1 CIRCUMSTANCES FOR CERTIFICATE RE-KEY

Prior to the expiration of an existing Sub-CA Certificate, it is necessary for the Sub-CA to update the certificate to maintain continuity of Certificate usage.

Manual Certificate re-key may be performed within or after one-month of certificate expiry.

The process for rekeying a Sub-CA certificate shall be done as part of a witnessed key ceremony process similar to the initial key generation and certificate issuance

4.7.2 WHO CAN REQUEST A CERTIFICATE RE-KEY

Certificate re-key may be requested by an authorized STCS representative. The requestor's identification shall be determined and verified by the STCS PKI Committee.

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

Processing of Sub-CA certificate re-keying request shall be initiated only after successful verification of the re-key request from an STCS authorized representative; In each case the STCS PKI Committee shall approve all re-key requests.

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 Sub-CA 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 in the appropriate repository.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

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

4.8 CERTIFICATE MODIFICATION

The STCS Intermediary CA does not support any form of Sub-CA certificate modification. The issued Sub-CA certificate must first be revoked, and a new process followed to Re-key the certificate as specified in section 4.7.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

A Sub-CA 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 STCS Intermediary 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 Intermediate Certificate Authority shall revoke Sub-CA Certificates for the following non-exhaustive reasons:

- The STCS Intermediary CA suspects or determines that the Sub-CA Private Key is compromised.
- If a Sub-CA contravenes any provisions of the Saudi e-Transactions Act and applicable Bylaws;
- The STCS Intermediary CA suspects or determines that revocation of a Sub-CA Certificate is in the best interest of the integrity of the STCS PKI Hierarchy;
- The STCS Intermediary CA determines that a Certificate was not issued correctly in accordance with this CP;

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed in a CRL.

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 PKI Committee can request the revocation of any of the Sub-CA certificates issued under the STCS Intermediary CA PKI Hierarchy;
- A legal, judicial or regulatory agency can request a revocation of any of the Sub-CA certificates.

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 Intermediary CA shall authenticate the request as well as the authorization of the requester in accordance with the applicable Agreements. The STCS PKI Committee has the final approval for the revocation of Sub-CA certificates.

4.9.3.1 Procedure for Requesting the Revocation of a Sub-CA Certificate

A CA requesting revocation of its CA Certificate is required to communicate the request to the STCS Policy Authority (PA). The STCS PA shall seek approval from the STC PKI Committee, which will then authorize the revocation of the Sub-CA certificate. The STCS PA may also initiate the Sub-CA certificate revocation if it deems necessary. The revoked CA certificate shall be published in the CRL of the STCS Intermediary CA.

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

The STCS Intermediary CA shall process authorized revocation requests within 24 hours.

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 and repository to check for revocation status.

4.9.7 CRL ISSUANCE FREQUENCY

The STCS Intermediary CA will publish its CRLs at least once every 6 months and within 24 hours of any Certificate revocation of its Sub-CAs.

4.9.8 MAXIMUM LATENCY OF CRLS

CRLs shall be published in the Repositories within 24 hours of Certificate revocation.

4.9.9 ONLINE REVOCATION CHECKING AVAILABILITY

No Stipulation.

4.9.10 ONLINE REVOCATION CHECKING REQUIREMENTS

No stipulation.

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

No Stipulation.

4.9.12 SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE

If STCS Intermediary CA discovers, or has a reason to believe, that there has been a compromise of the private key of the STCS Intermediary CA or any Issuing CA, STCS Intermediary CA will immediately declare a disaster and invoke the business continuity plan. STCS Intermediary CA will

1) Determine the scope of certificates that must be revoked,
2) Revoke the affected certificates as per STCS Intermediary CA procedures
3) Publish a new CRL as stipulated in section 4.9.7,
4) Generate new CA key pair as per STCS operations policies and procedures.

4.9.13 CIRCUMSTANCES FOR CERTIFICATE SUSPENSION

No Stipulation. Suspension is not permitted for a Sub-CA

4.9.14 WHO CAN REQUEST SUSPENSION

No stipulation.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

No stipulation.

4.9.16 LIMITS ON SUSPENSION PERIOD

No stipulation.

4.9.17 CIRCUMSTANCES FOR TERMINATING SUSPENDED CERTIFICATES

No stipulation.

4.9.18 PROCEDURE FOR TERMINATING THE SUSPENSION OF A CERTIFICATE

No stipulation.

4.10 CERTIFICATE STATUS SERVICES

The status of the STCS Issuing CA public certificates is available from CRL's in the repositories.

4.11 END OF SUBSCRIPTION

No stipulation.

4.12 KEY ESCROW AND RECOVERY

The STCS Intermediary CA does not support 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 PKI 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 (STCS Data Centre) housing the STCS PKI 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 CA equipment and records.

5.1.2 PHYSICAL ACCESS

STCS 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 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, are not allowed into such secured areas.

The STCS PKI has implemented policies and procedures to ensure that the physical environments in which the STCS Intermediary CA systems are installed maintain a high level of security:

- STCS Intermediary CA systems are installed in a secure facility that is protected from outside networks, with all access controlled;
- STCS PKI is separated into a series of progressively secure areas; and
- The entrances and exits from the secure areas are under constant video surveillance and all systems that provide authentication, as well as those that record entry, exit and network activity, are in secured areas.

The security techniques employed are designed to resist a large number and combination of different forms of attack. The mechanisms STCS PKI uses include:

- Closed circuit television;
- Two-factor authentication using Biometrics and locks;

- Motion detectors;
- Human guards; and
- All the Networking and systems components including the certification components are installed in secure Data cabinets with locks from both sides.

To prevent tampering, cryptographic hardware is stored in a most secure area of the STCS Data Center, with access limited to authorized personnel.

The STCS Data Center uses human guards to continually monitor the access to the facility housing the CA equipment. STCS facility is never left unattended.

The security mechanisms employed are commensurate with the level of threat in the equipment environment.

5.1.3 POWER AND AIR CONDITIONING

STCS Data Center has a UPS and back-up electrical generators and sufficient back-up capability to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown.

The design of STCS PKI facilities ensures that no single point of failure is supported by providing the following measures:

- Two independent power supplies feeding the STCS Data Centre;
- Uninterruptible Power Supply units and stand-by generators for the entire building; and
- Switchover of the services to a backup facility in the case of an emergency or disaster as per STCS Business Continuity Plan.

A fully redundant air-conditioning system is installed in the PKI areas.

5.1.4 WATER EXPOSURE

STCS has taken reasonable precautions to minimize the impact of water exposure. These include installing the PKI equipment on elevated floors within the data center facility.

5.1.5 FIRE PREVENTION AND PROTECTION

STCS follows best practices and industry standard for fire prevention and protection of its data center. Some of the measures deployed include:

- Fire-resistant walls and pillars;
- Fire, smoke and gas detectors installed throughout the facility which are interconnected with the facilities alarm system;
- An adequate number of fire extinguishers have been provided with a suitable fire extinguishing agent. Mobile fire extinguishers are also provided in sufficient numbers within the facility; and
- The controls implemented comply with applicable safety regulations of the Kingdom of Saudi Arabia.

5.1.6 MEDIA STORAGE

Media storage under the control of STCS is subject to multiple-layer security storage requirements. STCS procedures include full back-up of the STCS Intermediary CA repositories and offsite storage in a physically separate location with security similar to that of the facility in which the CA activities are performed. Media is stored so as to protect them from accidental damage (e.g., water, fire, or electromagnetic). Media that contain audit, archive, or backup information are duplicated and stored in a location separate from the STCS Intermediary CA.

5.1.7 WASTE DISPOSAL

STCS security procedures provide that sensitive media and documentation that are no longer needed for operations are destroyed using secure disposal processes. For example, sensitive paper documentation is shredded, burned, or otherwise rendered unrecoverable. Electronic media is physically destroyed prior to disposal.

5.1.8 OFF-SITE BACKUP

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

The backup site has physical and procedural controls commensurate to that of the STCS PKI primary site.

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 by STCS to fill these roles will be extraordinarily responsible. The functions performed in these roles form the basis of trust for the entire STCS PKI hierarchy. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

At a minimum, the following roles are established:

1) CA Administrator

The CA Administrator role is responsible for:

- Installation, configuration, and maintenance of the CA hardware and software;
- Starting and stopping CA services;
- Generating and backing up CA keys;
- Backing up and restoring the database; and
- Establishing and maintaining CA system accounts;
- Configuring certificate profiles or templates and audit parameters; and

CA Administrators do not issue certificates to Subscribers.

2) CA Security Officer

The CA Officer role is responsible for:

- Verifying the accuracy of information included in certificates;
- Executing the issuance of certificates; and
- Executing the revocation of certificates.

3) CA Policy Authority

The CA Policy Authority role is responsible for:

- Overall development, maintenance and getting approval of the STCS PKI policies

4) CA Operations Authority

The CA Operations Authority role is responsible for:

- Implementation of the CA policies and development of operational procedures and guidelines

5) CA Auditor

The CA Auditor role is responsible for:

- Reviewing of audit logs from time to time
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with this CPS.

6) CA Key Manager

The CA Key Manager is responsible for the following:

- Keep an up to date record of the Cryptographic register
- The Key manager is the custodian of all key management activities and ensure compliance with crypto policies

7) CA Operator

The CA Operator role is responsible for:

- Daily operation and maintenance of the system equipment;
- System backup and recovery operations; and
- Storage media renewal.

8) CA Key Shareholders

- The CA key Shareholders are holders of the CA Key material components. They are required to be present for any CA key operations.

9) CA Developers

- The Developers are responsible for software development of CA systems and related interfaces.

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

STCS ensures 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 fills each of the roles specified in previous section and 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.

The STCS Intermediary CA will ensure that no single individual may gain access to CA private keys. At a minimum three individuals, must perform any CA system start-up, CA system shutdown, key backup or key recovery operation. The m/n deployed will be a 3 of 12 individuals required for the STCS Intermediary CA.

5.2.3 IDENTITY-PROOFING FOR EACH ROLE

Persons filling trusted roles shall undergo an appropriate security screening procedure before they can start their duties.

5.2.4 SEPARATION OF ROLES

Role separation, when required as set forth below, may be enforced either by the CA equipment, or procedurally, or by both means.

Individual CA personnel are specifically designated to the roles defined in section 5.2.1 and STCS Trusted Roles document. Individuals who assume a CA Security Officer role may not assume a CA Administrator or CA Auditor role. An individual assigned a CA Auditor role shall not perform any other trusted role. 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 are 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 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 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 security clearance.

Security clearance shall be repeated every 3 years for personnel holding trusted roles.

5.3.3 TRAINING REQUIREMENTS AND PROCEDURES

STCS will provide proper training to all personnel performing duties with respect to the operation of the STCS PKI, Repositories and OCSP Responder. Training shall cover the following aspects:

- PKI and Information Security concepts;
- All PKI software versions in use on the STCS PKI, Repositories and OCSP Responder systems;
- All STCS PKI duties that the personnel are expected to perform on STCS Intermediary CA;
- Disaster recovery and business continuity procedures; and
- The meaning and effect of the STCS Intermediary CA CP and this CPS.

Documentation of all personnel who received training and the level of training completed shall be maintained by STCS.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

Individuals performing PKI roles are made aware of changes in the STCS PKI operation. Any significant change to the operations will necessitate a training awareness plan, and the execution of such plan is documented. Examples of such changes are STCS PKI software or hardware upgrade, changes in automated security systems, and relocation of equipment.

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

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

The STCS Intermediary 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 Intermediary CA shall take appropriate administrative and disciplinary actions against personnel who perform unauthorized actions not permitted by the CP, CPS and/or other STCS Intermediary CA operational procedures.

5.3.7 CONTRACTING PERSONNEL REQUIREMENTS

When STCS uses a contractor to perform services, there will be adequate procedures with explicitly stated objectives and supervision will be in place to ensure that any tasks performed in accordance with the STCS Intermediary CA CP, this CPS, STCS PKI Policies as well as the requirements stipulated in the contractor's contract of employment. Contractor personnel shall be subject to the same sanctions as other personnel as set forth in Section 5.3.6.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

STCS provides sufficient documentation to its personnel in order for them to perform their job responsibilities competently and satisfactorily.

5.4 AUDIT LOGGING PROCEDURES

STCS has implemented and maintaining Trustworthy Systems to preserve an audit trail for material events and for key life cycle management, including key generation, backup, storage, recovery, destruction and management of cryptographic devices of the STCS Intermediary CA and other associated components.

STCS Intermediary CA systems generate audit log files for all events relating to the security of the STCS Intermediary CA and other associated components. All security audit logs are retained and made available for review during compliance audits. The security audit logs for each auditable event defined in this section are maintained in accordance with section 5.5.2 which governs the archive retention period for security audit data.

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.

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 in accordance with STCS Audit and Compliance Policy.

5.4.3 RETENTION PERIOD FOR AUDIT LOG

The STCS Intermediary CA shall retain all system generated (electronic and manual) audit records onsite for a period not less than twelve (12) months from the date of creation.

5.4.4 PROTECTION OF SECURITY AUDIT DATA

Read access to the journal information is granted to personnel requiring this access as part of their duties. Only authorized roles can obtain access.

The journal is stored in the text files and access to this is protected against unauthorized access by the CA application and through special security measures on the operating system level.

5.4.5 AUDIT LOG BACKUP PROCEDURES

The journal is an integral part of the CA database and is therefore part of the daily backup. The entire database is encrypted on the disk as well as on the backup media.

Audit log backup procedures are in accordance with STCS Audit and Compliance Policy.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

The audit log or journal is an integral part of the CA software. The audit system ensures the integrity of the audit data being collected. In case of the audit system stopping to function, the STCS Intermediary CA shall determine whether to suspend or continue with operations.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

Event-causing subject are not notified.

5.4.8 VULNERABILITY ASSESSMENTS

STCS performs routine assessments of security controls. This self-assessment includes periodic review of error logs on systems, storage of assets and records, security audit data for alerts or irregularities, alarm logs, access logs, incident reports, and audit log analysis.

Apart from this, STCS data centre is constantly (24x7) monitored, and all attempts to gain unauthorized access to any of the services are logged and analyzed.

STCS performs third party penetration testing for STCS data centre infrastructure at least once a year and doing regular vulnerability assessment internally. Also Risk Assessment is performed at least once a year as per STCS Risk Assessment Methodology. STCS Risk Assessment exercise 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, technology.

Based on the Risk Assessment exercise, the STCS Intermediary CA 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 Intermediary CA archives 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 Intermediary CA shall make these audit logs available to its Qualified Auditor upon request.

a) Audit logs generated by the PKI CA software;
b) RA and other agreements;
c) Records pertaining to identification and authentication information;
d) Physical access logs;
e) System configuration changes and maintenance;
f) CA personnel changes;
g) Discrepancy and No compromise reports;
h) Information concerning the destruction of sensitive information;
i) Current and past versions of all Certificate Policies;

j) Current and past versions of Certification Practice Statements;

k) Vulnerability Assessment Reports;

l) Threat and Risk Assessment Reports;

m) Compliance Inspection Reports;

n) Documents identifying all personnel who received CA related training and the level of training completed; and

o) The STCS Intermediary CA shall archive any necessary keys and passwords for a period of time sufficient to support the functionalities.

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's minimum retention period for archive data is established at 10 years.

The STCS Intermediary CA shall retain all documentation relating to 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.

Applications needed to process the archive data shall also be maintained for the archival retention period.

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 component itself. Any secondary site must provide adequate protection from environmental threats such as temperature, humidity and magnetism.

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 obtained from the Time Server.

System logs are automatically 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 the 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.

5.6 KEY CHANGEOVER

To minimize risk from compromise of a CA's private signing key, the key will be changed often. Once changed, only the new key will be used for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed using the associated Private Key have also expired. If the old Private Key is used to sign CRLs that contain certificates signed with that key, only then the old key may be retained. If the old key is retained, it shall be protected just as the new key.

The new certificate shall be distributed to the repository in the same manner as the original certificate.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

In the event that a potential hacking attempt or other form of compromise to the STCS Intermediary CA occurs, STCS shall perform an investigation to determine the degree of potential damage. The STCS PA shall notify NCDC if any of the following occurs;

- 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 a CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL.

The STCS PA shall be notified by the NCDC if any of the following cases occurs;

- NCDC plans to revoke the STCS Intermediary CA certificate, for whatever reason;
- Any incident preventing the NCDC Root CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL;

If the STCS Intermediate CA private key is suspected of compromise, The STCS Intermediary CA shall re-establish operational capabilities as quickly as possible in accordance with the procedures set forth in the STCS PKI Operations Policy and Business Continuity Plan.

5.7.2 RECOVERY PROCEDURES IF COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to STCS PKI management and STCS PKI's incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, STCS PKI Operations Policy and Business Continuity procedures will be enacted.

5.7.3 RECOVERY PROCEDURE IF CA PRIVATE KEY IS COMPROMISED

In the event of the STCS Intermediary CA being compromised, lost or destroyed or suspected to have been compromised, the STCS Intermediary CA, after investigation of the problem, shall decide if the STCS Intermediary CA Certificate should be revoked. If so, then:

- All the Sub-CA representatives will be notified at the earliest feasible opportunity; and
- A new STCS Intermediary Key Pair shall be generated or an alternative existing CA hierarchy shall be used to create new Sub-CA Certificates.

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);
- 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 any kind of natural, man-made or equipment failure related disaster.

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 TERMINATION

5.8.1 CA TERMINATION

In the event that the STC Intermediary CA ceases operation, it must notify its Sub-CAs in writing at least one month before termination of operations and arrange for the continued retention of the CA's keys and information. The following procedures shall apply in the case of the STCS Intermediary CA termination:

1 give the NCDC notice of its intention to cease operations 90 days before ceasing issue certificates;
2 before the ceasing to act as a CA, advertise its intention to terminate its operations in its website and other media as applicable and in such other manner as the NCDC may determine;
3 give all its Sub-CAs of each unrevoked or unexpired Certificate issued by it 60 days' notice by sending an electronic mail to the Sub-CA representative of its intention to cease acting as a CA;
4 ensure that discontinuing its operations causes minimal disruption to its Sub-CAs and to relying parties and other persons who need to verify the Certificates;
5 Ensure the procedures for CA records archival are followed as stipulated in the STCS Intermediary CA CP

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

The STCS Intermediary CA key pair generation is performed by multiple trusted personnel using trustworthy systems and processes that provide for the security and required cryptographic strength for the generated keys. For the STCS PKI (Intermediary and subordinate CAs), the Hardware Security Modules (HSM's) used for key generation meet the requirements of FIPS 140-2 Level 3.

The STCS Intermediary CA key pair is generated in pre-planned Key Generation Ceremonies in accordance with the requirements of NCDC. The activities performed in 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 Intermediary CA management.

6.1.2 PRIVATE KEY DELIVERY TO END-ENTITIES

The STCS Intermediary CA does not generate private keys to its end entities (Sub-CAs). The end entities generate the Private key as part of the Key ceremony process.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

The Subordinate CA Public Key must be transferred to STCS Intermediate CA using a method designed to ensure that:

- The Public Key is not changed during transit; and
- The sender possesses the Private Key that corresponds to the transferred Public Key.

Delivery of public keys shall be achieved with a certificate request using a recognized secure protocol such as PKCS#10.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

Acceptable methods are specified in section 6.1.4 of the STCS Intermediary CA CP.

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. All FIPS-approved signature algorithms shall be considered acceptable.

All certificates issued shall use 4096 bit RSA, with Secure Hash Algorithm version (SHA-256) in accordance with FIPS 186-2 or equivalent. TLS or another protocol providing similar security to accomplish any of the requirements of this CPS shall use triple-DES or AES (minimum 128 bit key strength) for symmetric keys, and 4096 bit RSA or equivalent for asymmetric keys.

The STCS Intermediary CA implement the following key sizes under its hierarchy:

1) STCS Intermediary CA Key Pair: 4096 bits
2) STCS IDCA Key Pair : 4096 bits
3) STCS QUCA Key Pair: 4096 bits

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

The STCS Intermediary CA shall generate public keys in accordance with industry standards such as FIPS 186 and check public key parameters for their validity.

6.1.7 KEY USAGE PURPOSES

Keys may be used for the purposes and in the manner described in same section of the STCS Intermediary CA CP.

6.2 PRIVATE KEY PROTECTION AND CRYPTO-MODULE ENGINEERING CONTROLS

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

See section 6.1.1 of this CPS for the description of the cryptographic modules.

6.2.2 CA PRIVATE KEY MULTI-PERSON CONTROL

Multi-person control of the STCS Intermediary CA private key is achieved using an “m-of-n” split key knowledge scheme. STCS Intermediary CA keys can only be accessed on the physical and logical level by adhering to '3 out of 12' control, meaning that 3 of the 12 persons are present.

6.2.3 PRIVATE KEY ESCROW

See section 4.12 of this document.

6.2.4 PRIVATE KEY BACKUP

STCS uses the mechanisms provided by the HSM’s to backup the STCS Intermediary CA signing key. A second copy may be kept at the CA backup location identified as business continuity location. A third copy may be kept at the CA backup location identified as disaster recovery location. Procedures for STCS Intermediary CA signing Private Key backup are detailed in STCS PKI Backup and Restore Procedures. The CA signing key is backed up under the same multi-person control as the original signature keys.

6.2.5 PRIVATE KEY ARCHIVAL

The STCS Intermediary CA does not archive Private Keys.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

The STCS Intermediary CA shall generate, activate and store private keys in FIPS 140-2 Level 3 or above rated Hardware Cryptographic Modules. When the Private Keys are outside the HSM, they shall be kept in encrypted form.

The STCS Intermediary CA keys can be cloned for secure backup from the master hardware cryptographic module to other hardware cryptographic module(s) using secure mechanisms so that they can be recovered if a major catastrophe destroys the productive set of keys.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

The STCS Intermediary CA’s private keys are stored on FIPS 140-2 Level 3 validated modules in encrypted form.

6.2.8 METHOD OF ACTIVATING PRIVATE KEYS

The STCS Intermediary CA’s private key shall be activated by a threshold number of Shareholders, as defined in STCS Operations Policies and Procedures, supplying their activation data. Such activation data shall be held on secure media and shall require the successful completion of a multi-person authentication process. A deactivated key shall be

kept encrypted or otherwise secured within the cryptographic module, to prevent unauthorized access.

6.2.9 METHODS OF DEACTIVATING PRIVATE KEYS

The STCS Intermediary CA's private keys shall be deactivated by a threshold number of shareholders, as defined in STCS Operations Policies and Procedures, by removing their secure media.

6.2.10 METHODS OF DESTROYING PRIVATE KEYS

The STSC Intermediary CA and Sub-CAs under the PKI hierarchy Private keys shall be destroyed as per STCS Cryptographic Devices Lifecycle Management Policy and Procedure, which shall be consistent with section 6.2.2 of the STCS Intermediary CA CP.

6.2.11 CRYPTOGRAPHIC MODULE RATING

The CA private keys are stored on FIPS 140-2 Level 3 validated Hardware Security Modules.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVE

The STCS Intermediary CA certificate (which contains the public key) is backed up and archived as part of the STCS Intermediary CA and STCS data centre routine backup procedures.

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
STCS Intermediary CA signing key and certificate	4096	118 months
STCS QUCA Signing Key and Certificate	4096	118 months
STCS IDCA Signing Key and Certificate	4096	118 months

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

The STCS Intermediary CA and Sub-CA cryptographic module activation data will be generated locally at the time of key generation by personnel in the trusted role and responsible for controlling the activation data.

6.4.2 ACTIVATION DATA PROTECTION

If written down CA cryptographic module activation data is placed into secure packages which are then stored within secure containers in a highly secured environment inside STCS data centre.

In addition, the activation data shall be secured at the same level as the cryptographic data for the STCS Intermediary CA and Sub-CAs. Such data shall be stored under multi-person control and shall not be stored with the cryptographic modules (HSMs).

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

The STCS Intermediary CA servers hosted in STCS data centre are protected by external firewalls that filter out all unwanted traffic. Additionally, the CA systems are hardened and equipped with a high-security operating system. Access to the system for System Administrators is granted only over secure and restricted protocols using strong public-key authentication.

STCS data centre has implemented layered security approach to ensure the security and integrity of the computers used to run the STCS Intermediary CA software. The following controls ensure the security of STCS data centre operated computer systems:

- Hardened 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

No Stipulation.

6.6 LIFE-CYCLE SECURITY CONTROLS

6.6.1 SYSTEM DEVELOPMENT CONTROLS

STCS employs the following System Development controls:

- STCS may use standard software from product vendors for version control. Where STCS uses its own software products, these have been developed using documented software development processes;

- Hardware and software procured to operate the CA is purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device);
- CA hardware and software configurations are dedicated to performing one task: the CA. No other applications, hardware devices, network connections, or component software that is not part of the CA operation will be installed;
- STCS undertakes all reasonable precautions to prevent malicious software from being loaded onto the CA equipment. Only applications required to perform the operation of the CA are procured. The CA hardware and software is scanned for malicious code on first use and periodically thereafter; and
- Hardware and software updates are purchased in the same manner as original equipment, and are installed by trusted and trained personnel according to policies and procedures established in STCS's Operations Policies and Procedures.

6.6.2 SECURITY MANAGEMENT CONTROLS

System security management shall be controlled by the privileges assigned to system accounts and by the trusted roles described in section 5.2.1, according to appropriate standards (e.g. ISO/IEC 27001:2013 or similar).

The configuration of the STCS Intermediary CA system as well as any modifications and upgrades must be documented and controlled in accordance with STCS Change Management Policy. A formal configuration management methodology must be used for installation, ongoing maintenance and evolution of the CA system. No upgrades shall be permitted without prior offline testing and assessment, and regular backups must be taken.

6.6.3 LIFE CYCLE SECURITY RATINGS

No stipulation.

6.7 NETWORK SECURITY CONTROLS

The Repository and CRL infrastructure will be connected to the internet in such a way so as to provide continuous service to Relying Parties. Redundancy is provided through the Repository and network infrastructure to prevent loss of service even during maintenance and backup procedures.

STCS data centre uses network design of multiple security layers making use of several security technologies including firewalls, intrusion prevention systems, anti-virus, anti-spyware software to protect network access to on-line STCS Intermediary CA's and Repository equipment. These technologies may limit the services allowed to and from the on-line CA's, Repository and OCSP Responder equipment to those authorized to have such access.

STCS data centre network security controls are designed to protect STCS infrastructure against network attacks. All unused network ports and services are turned off. These network security controls include effective firewall management, including port restrictions and IP address filtering.

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

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

Time derived from the time service shall be used for establishing the time of:

- Initial validity time of the Sub-CA Certificates;
- Revocation of Sub-CA Certificates;
- Posting of CRL updates;

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 detailed Certificate profile for the STCS Intermediary CA is described in the STCS PKI Certificate Profiles document, an internal STCS Operational document.

7.1.1 VERSION NUMBERS

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

7.1.2 CERTIFICATE EXTENSIONS

STCS Intermediary CA and its critical private extensions shall be interoperable in their intended community of use.

Subordinate certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by STCS Intermediary 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 Intermediary 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 Intermediary 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 Intermediate CA CRL Profile is shown below:

7.2.1 STCS INTERMEDIARY CA CRL PROFILE

Field	Content	Comment
Version	1	
Algorithm	SHA256withRSA	
Issuer	CN=STCS Intermediary CA O=STCS C=SA	
This update	*<issue date>*	
Next update	*<issue date + six months>*	Or immediately upon revocation

AuthorityKeyIdentifier	Issuing CA's Subject Key Identifier	
CRL number	<number>	

7.2.2 VERSION NUMBERS

The STCS Intermediary 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.

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

The STCS PKI Committee shall ensure adherence of the Sub-CAs to this CP, accompanying CPS and any applicable laws and regulations. The committee shall also ensure the Issuing CAs comply with audit requirements.

8.1 FREQUENCY OF AUDIT OR ASSESSMENTS

The STCS Intermediary CA shall be subjected to periodic compliance audits which are no less frequent than once a year and after each significant change to the deployed procedures and techniques.

The Subordinate Issuing CAs shall also be audited to ensure compliance against defined requirements on at least an annual basis.

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

The annual audit of the STCS Intermediary 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 Intermediary 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 Intermediary 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 CA to continue operations until the next planned, or newly scheduled, inspection;
- Suspending the CA's certificate; or
- Revoking the 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 Intermediary 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 Intermediary 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 Intermediary 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 Intermediary CA does not charge fees to access certificate status information via the CRL.

9.1.4 FEES FOR OTHER SERVICES

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

9.1.5 REFUND POLICY

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

The STCS Intermediary 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 Intermediary CA shall hold insurance cover in lieu of its performance and obligations under the following guidelines or that which is deemed sufficient by the STCS Intermediary CA:

- Commercial general liability insurance with policy limits of at least two (2) million US Dollars in coverage;
- Professional Liability (Errors and Omissions) Insurance with policy limits of at least five (5) million US Dollars

9.2.2 OTHER ASSETS

STCS Intermediary 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 Intermediary CA may be made publicly available at the discretion of NCDC and/or a STCS 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 CA Agreements;
- Any information requested by NCDC when it receives an application from a third party to operate as a CA or a Cross-Certified CA;
- Any corporate or personal information held by NCDC or STCS Intermediary 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 Intermediary 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 Saudi National Root-CA or the STCS Intermediary 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 Saudi National Root-CA or STCS Intermediary 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 Intermediary CA CP;
- STCS Intermediary 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 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 shall be protected in accordance with STCS Privacy Policy. STCS Intermediary 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 Subordinate 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 Intermediary 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 STCS Intermediary **CA** CP.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 STCS INTERMEDIARY CA REPRESENTATIONS AND WARRANTIES

STCS Intermediary CA provides representations and warranties in accordance with this CP, 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 Intermediary CA implemented procedure for verifying accuracy of the information contained within it before installation and first use;
- Implemented a procedure 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 Intermediary 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

No Stipulation

9.6.3 RELYING PARTIES REPRESENTATIONS AND WARRANTIES

Relying parties are required to act in accordance with the STCS Intermediary CA CP and the applicable Relying Party Agreement.

9.6.4 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

No stipulation.

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 Intermediary 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 Intermediary CA or for the legal validity, acceptance or any other type of recognition of its own certificates, those issued by it through other Subordinate entity, any digital signature backed by such certificates, and any products provided by STCS. The STCS Intermediary 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 Intermediary 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 Intermediary 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 Intermediary CA from and against any such liability and costs and claims arising there from;
- The STCS Intermediary 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 Intermediary 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 Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of the 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, except in the case where the CA is a government entity, the 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 RAs 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;
- The RA's own employees, arising from any of the RA's operations and activities as a RA, of any entity or services subordinated or outsourced by the RA; and
- Any parties relying on the RA's 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 Intermediary 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 Intermediary 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 Intermediary 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 the corresponding Issuing CA's Certificate assurance level.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

The STCS PA shall review this CPS at least once per year. Errors, updates, or suggested changes to this CPS shall be communicated to the STCS PA 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 Intermediary CA shall be managed as per the STCS Change Management Policy.

STCS Intermediary CA reserves the right to change this CPS from time to time. STCS Intermediary 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

The STCS PA 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 Saudi PKI participants and other parties designated by the STCS PA shall provide their comments to the STCS PA in accordance with NCDC rules.

The STCS PA's decision to designate amendments as material or non-material shall be at the PA's sole discretion.

Any changes to this CPS shall be made available within two weeks of approval by NCDC.

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 PA.

9.13 DISPUTE RESOLUTION PROCEDURES

Any dispute arising out of or related to the digital certificates issued by the STCS Intermediary CA shall initially be submitted to voluntary mediation. If mediation is not successful, then the dispute will be resolved by binding arbitration, in accordance with STCS Dispute Resolution Policy.

DISPUTE RESOLUTION COMMITTEE

The STCS PKI Dispute Resolution Committee will arbitrate on all claims or disputes arising out of or related to the operation of STCS CAs.

DISPUTE RESOLUTION POLICY

STCS PKI Dispute Resolution Policy is applicable to all participants of the STCS PKI.

9.14 GOVERNING LAW

This CPS will be governed and construed in accordance with the laws of the Kingdom of Saudi Arabia.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to national, state, local and foreign laws, rules and regulation, 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 any of its rights or duties under the STCS Intermediary CA 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 Intermediary CA will be treated according to the laws of the Kingdom of Saudi Arabia.

9.16.5 FORCE MAJEURE

The STCS Intermediary CA shall not be in default or liable for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or related to delays in performance or from failure to perform or comply with the terms of this CPS or the STCS Intermediary CA CP or any other related agreement due to any causes beyond its reasonable control, which causes include, without limitation, acts of God, riots and insurrections, terrorist activities, war, accidents, fire, strikes and other labour difficulties, embargoes, judicial action specifically preventing the operation of the STCS Intermediary CA, lack of or inability to obtain energy, or utilities, or acts of civil or military authorities.

9.17 OTHER PROVISIONS

9.17.1 FIDUCIARY RELATIONSHIPS

Nothing contained in this CPS shall be deemed to constitute either the STCS Intermediary CA, 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 Intermediary 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 Intermediary CA.

9.17.2 ADMINISTRATIVE PROCESSES

As specified in STCS Operations Policies and applicable Agreements.

APPENDIX-A: CERTIFICATE TYPES & POLICIES

A.1 CERTIFICATE TYPES SUPPORTED

A1.1 STCS INTERMEDIARY CA CERTIFICATE

A.1.1.1 STCS Intermediary CA Certificate issuance requirements And Usage

S. No.	Attribute	CA Certificate
1	Policy Name	STCS Intermediary CA Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.1.4**
3	Subject	"CN=STCS Intermediary CA, O = STCS, C = SA"
4	Application Usage	STCS Intermediary CA Certificates are CA Certificates and are not tied to any specific application or function. The applications using the STCS Intermediary CA issued CA Certificate should honour the Key Usage and any Extensions set in the certificate. The STCS Intermediary CA Certificate is used to sign Subordinate CA certificates and CRLs.
5	Verification Process	The process of verifying the STCS Intermediate CA certificate request is done as part of the Key Ceremony Process
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. STCS Intermediate CA KeyPairs shall be generated using Hardware Security Modules 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 NCDC who shall in turn sign the request. The signed certificate shall be returned to STCS to complete the process of CA configuration
8	Key Usage	The STCS Intermediate certificate and keys shall be used to sign Sub CA certificates and CRLs only
9	Private Key Protection	The STCS Intermediary CA Private Keys shall be protected using a Hardware Security Module meeting FIPS140-2 Level 3 requirements. Activation of the private key shall require multi-person control.
10	Certificate Lifetime	Up to 118 months (9 years, 10 months)
11	Key Backup	The STCS Intermediary CA shall backup the Private key using the same secure scheme as the Production Key
12	Asymmetric Key Length	Minimum 4096 bits RSA
13	Certificate Re-key	The STCS Intermediary CA Certificate re-key shall take place after the certificate is revoked and the CA information is still accountable or if a certificate has expired or is nearing expiry. In all cases the process shall be performed during a Key Ceremony.

A.1.2 STCS QUCA CERTIFICATE

This is the Subordinate Issuing CA certificate for the Qualified CA that is issued by the STCS Intermediary CA.

A.1.2.1 STCS QUCA Certificate issuance requirements And Usage

S. No.	Attribute	CA Certificate
1	Policy Name	STCS QUCA Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.11.4**
3	Subject	"CN=STCS QUCA, O = STCS, C = SA"
4	Application Usage	STCS QUCA Certificates are CA Certificates and are not tied to any specific application or function. The applications using the STCS QUCA issued CA Certificate should honour the Key Usage and any Extensions set in the certificate. The STCS QUCA Certificate is used to sign end entity subscriber certificates and CRLs.
5	Verification Process	The process of verifying the STCS QUCA certificate request is done as part of the Key Ceremony Process
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. STCS QUCA Key Pairs shall be generated using Hardware Security Modules 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 Intermediary 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 STCS QUCA certificate and keys shall be used to sign end entity subscriber certificates and CRLs only
9	Private Key Protection	The STCS QUCA CA Private Keys shall be protected using a Hardware Security Module meeting FIPS140-2 Level 3 requirements. Activation of the private key shall require multi-person control.
10	Certificate Lifetime	Up to 120 months (10 years)
11	Key Backup	The STCS QUCA shall backup the Private key using the same secure scheme as the Production Key
12	Asymmetric Key Length	Minimum 4096 bits RSA
13	Certificate Re-key	The STCS QUCA Certificate re-key shall take place after the certificate is revoked and the CA information is still accountable or if a certificate has expired or is nearing expiry. In all cases the process shall be performed during a Key Ceremony.

A.1.3 STCS IDCA CERTIFICATE

This is the Subordinate Issuing CA certificate for the Identity CA that is issued by the STCS Intermediary CA.

A.1.3.1 STCS IDCA Certificate issuance requirements And Usage

S. No.	Attribute	CA Certificate
1	Policy Name	STCS IDCA Certificate Policy
2	Policy OID	**2.16.682.1.101.5000.1.4.1.2.1.21.4**
3	Subject	"CN=STCS IDCA, O = STCS, C = SA"
4	Application Usage	STCS IDCA Certificates are CA Certificates and are not tied to any specific application or function. The applications using the STCS IDCA issued CA Certificate should honour the Key Usage and any Extensions set in the certificate. The STCS IDCA Certificate is used to sign end entity subscriber certificates and CRLs.
5	Verification Process	The process of verifying the STCS IDCA certificate request is done as part of the Key Ceremony Process
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. STCS IDCA Key Pairs shall be generated using Hardware Security Modules 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 Intermediary CA that shall in turn sign the request. The signed certificate shall be returned to complete the process of the STCS IDCA configuration
8	Key Usage	The STCS IDCA certificate and keys shall be used to sign end entity subscriber certificates and CRLs only
9	Private Key Protection	The STCS IDCA CA Private Keys shall be protected using a Hardware Security Module meeting FIPS140-2 Level 3 requirements. Activation of the private key shall require multi-person control.
10	Certificate Lifetime	Up to 120 months (10 years)
11	Key Backup	The STCS IDCA shall backup the Private key using the same secure scheme as the Production Key
12	Asymmetric Key Length	Minimum 4096 bits RSA
13	Certificate Re-key	The STCS IDCA Certificate re-key shall take place after the certificate is revoked and the CA information is still accountable or if a certificate has expired or is nearing expiry. In all cases the process shall be performed during a Key Ceremony.