STCS INTERMEDIARY CA

CERTIFICATION PRACTICE STATEMENT

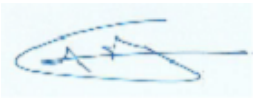
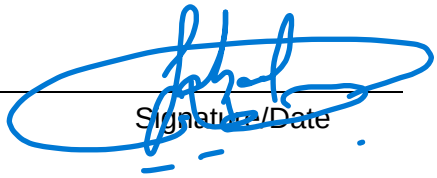
Document Classification : Public

Version Number : 2.1

Issue Date: 30 September 2021

Document Reference

Item	Description
Document Title:	STCS Intermediary CA Certificate Practice Statement
Custodian Department:	Cybersecurity
Owner:	Solutions' Policy Authority
Version Number:	2.1
Document Status:	Final

Author(s):	Katekani Hlabathi	
	Security Consultant	Signature/Date
Official Reviewer:	Solutions' Policy authority	
	PKI Consultant	Signature/Date
Approved by:	Fahad I. Aljutaily	
	Sirar by stc CEO	Signature/Date

Document Revision History

Version	Date	Author(s)	Revision Notes
1.0	17/02/2019	Solutions	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
1.8	22/07/2020	Solutions Policy Authority	Updates based on regular review
1.9	17/08/2020	Solutions Policy Authority	Addressing the comments received during the period of time audit
2.0	09/09/2020	Solutions Policy Authority	Addressing the comments received from NCDC
2.1	30/09/2021	Solutions' Policy Authority	Annual review

Document Control

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

Digitally Signed Copy of this document shall be stored at Solutions' PKI Repository.

Table of Contents

1 INTRODUCTION

The Government of Saudi Arabia has embarked on an ambitious e-transaction program, recognizing that there is a tremendous opportunity to better utilize information technology to improve the quality of care/service, lower the cost of operations, and increase customer satisfaction. To ensure the secure, efficient transmission and exchange of information electronically, the Kingdom of Saudi Arabia has created a National Public Key Infrastructure. Named the National Center for Digital Certification (NCDC), NCDC is created by an act of law and its mandate is stipulated in the Saudi e-Transactions Act and its bylaws.

Solutions, a subsidiary of the Saudi Telecommunications Company (STC) operates a Public Key Infrastructure (PKI) under the Saudi National PKI. Solutions' PKI has core offerings of digital trust services designed to enable electronic signature and authentication services for business entities and individuals. To achieve this goal, Solutions' PKI operates a publicly chained Intermediary Certificate Authority (CA) that is Root signed by the Saudi National Root CA that is operated by the NCDC.

Solutions' Intermediary is called STCS Intermediary CA (hereinafter, the Intermediary CA), underneath, there are subordinate Issuing Certificate Authorities (hereinafter, Issuing CAs) that issue certificates to end-users. The two Issuing CAs signed by the Intermediary CA are:

- STCS Qualified Certificate Authority (STCS QUCA) and
- STCS Identity Certificate Authority (STCS IDCA)

The full hierarchy of Solutions' PKI is indicated below:

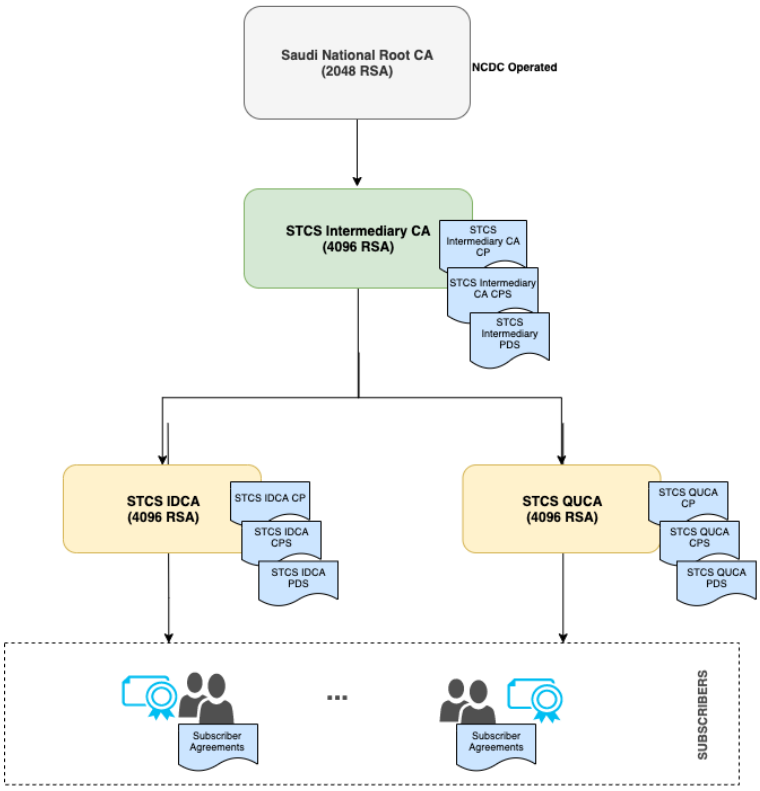


Figure 1-Solutions' PKI and Governance Hierarchy

This CPS complies with the stipulations of the STCS Intermediary CA Certificate Policy (CP), in addition to the following requirements:

- Saudi National PKI Policy,
- Saudi National Root CA CPS,
- RFC3647 — Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework. Sections that are not applicable to the QUCA are labelled “No Stipulation”. Where necessary, additional information is presented in subsections to the standard structure,
- RFC5280 — Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,
- Current version of the AICPA/CICA, WebTrust Principles and Criteria for Certification Authorities v2.2, and
- Adobe Approved Trust List (AATL) Certificate policies.

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 Intermediary CA as governed by the Intermediary CA Certificate Policy (hereinafter, the CP). This applies only to the Issuing CAs’ certificates issued under the hierarchy of the SCTS Intermediary CA

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

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

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

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

It is the responsibility of all parties applying for or using a Digital Certificate issued under the Intermediary CA CP and this CPS to understand the practices established for the lifecycle management of the Certificates issued by the Intermediary CA.

1.1.1 CERTIFICATE POLICY

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

1.1.3 INTERACTION WITH OTHER PKIS

The Intermediary CA will not be cross certified with other CAs, it will only be chained to the NCDC Root CA.

1.1.4 SCOPE

This CPS applies to all certificates issued by the Intermediary CA. The Intermediary CA operates under the Saudi National PKI hierarchy and owned by Solutions. Solutions has delegated the operations of its PKI to Sirar by stc for issuance and management of certificates and revocation lists. Sirar by stc is a sister company to Solutions, both parties have signed an agreement where Sirar by stc has committed to operate Solution's policies and procedures including applicable CPs and CPSs.

The Intermediary CA is an offline CA, that issues certificates to the approved Issuing CAs, that in turn issue subscriber certificates.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the 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 Intermediary CA under this CPS.

Several parties constitute the participants of the Intermediary CA. The parties mentioned hereunder including the Certification Authorities, Solutions' PKI Committee (hereinafter, the PKI Committee), subscribers and relying parties are collectively called PKI participants.

1.3.1 CERTIFICATION AUTHORITIES

Solutions' PKI is an umbrella term referring to Solutions as an organization that runs PKI services under the Saudi National Root CA. Solutions' PKI implements a Two-tier PKI Architecture consisting of an offline intermediary CA (STCS intermediary CA), and two Issuing CAs under it, these being the STCS Identity CA (IDCA) and the STCS Qualified CA (QUCA). These Issuing CAs issue subscriber certificates, OCSP responder, timestamping certificates and other certificates required by the internal PKI components. The Issuing CAs issue certificates to Subscribers in accordance with each respective CP and the CPS, their RA Agreement, Subscriber Agreement, Relying Party Agreement, and the Saudi National PKI Policy.

Solutions 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 Solutions' PKI.

1.3.1.1 SAUDI NATIONAL ROOT CA

The Saudi National Root CA is the trust anchor for the entire Saudi National PKI. It is self-signed CA and operated by NCDC.

1.3.1.2 STCS INTERMEDIARY CA

The 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.

1.3.1.3 STCS QUALIFIED CA (QUCA)

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

1.3.1.4 STCS IDENTITY CA (IDCA)

The STCS IDCA is an issuing Certificate Authority under the Intermediary CA. It issues authentication certificates used to identify end-users.

1.3.2 REGISTRATION AUTHORITIES

Solutions runs its own RA function for the Intermediary CA through Sirar by stc, which is tasked to request issuance and revocation of a certificate under this CPS. The RA team's role is to execute the Intermediary CA operational cycle, including the key ceremonies for the QUCA and IDCA, as well as the generation of OCSP certificates and the Certificate Revocation Lists (CRL).

1.3.3 SUBSCRIBERS

The subscribers of ***STCS*** Intermediary CA are Issuing CAs that are owned and operated by Solutions.

These subscribers:

- are identified in the Subject field of their certificate, issued by the Intermediary CA
- control the private key corresponding to the public key that is listed in their certificate.

1.3.4 RELYING PARTIES

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

Relying Parties shall rely on a certificate that has been issued under this CPS if:

- The certificate has been used for the purpose for which it has been issued, as described in this CPS;

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

1.3.5 OTHER PARTICIPANTS

1.3.5.1 Solutions' PKI Committee

Solutions' PKI Committee operates as the governance function for Solutions' PKI. It groups the necessary functions for this purpose including the policy, compliance and design functions. The PKI Committee provides strategic direction and continuously supervises the PKI operations team. This committee is appointed by Solutions.

1.3.5.2 Solutions' Policy Authority (Solutions' PA)

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

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

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

OCSP Responder certificates are used to sign responses for certificate status information requests.

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 Solutions' shall not be liable for any claims arising from such use.

1.5 POLICY ADMINISTRATION

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

This CPS is administered by the Solutions' PA (member of the PKI Committee) and approved by the PKI Committee. The chairperson of the PKI Committee signs-off on the approved documents by the PKI Committee.

1.5.2 CONTACT PERSON

Queries regarding 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

Solutions' PA is responsible for ensuring that the Intermediary CA CPS conforms to the requirements of this CPS in accordance with policies and procedures specified by Solutions' PKI. The PA shall ensure that the CPS, after ensuring conformity to this CPS, is approved by the PKI Committee.

1.5.4 CPS APPROVAL PROCEDURES

Changes or updates to this CPS document must be made in accordance with the stipulations of Saudi e-Transactions act and bylaws and the provisions contained in this CPS and are subject to PKI Committee. The PKI Committee reviews the initial version of this CPS and any subsequent updates. The PKI Committee interacts with NCDC to formally approve major changes on this document.

The approved changes shall be published as set forth in section 2.2.2.

1.6 DEFINITIONS AND ACRONYMS

The following sections contain the definitions of terms and acronyms. The source of a definition is cited when available.

Activation Data — Secret information, other than cryptographic keys, that are required to operate cryptographic modules that need to be protected; for example, a PIN, a password or pass-phrase, or a manually held key share

Audit Report — A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements

CA — Certification Authority

CA Certificate — A certificate for one CA's public key issued by another CA

Certificate — An electronic document that uses a digital signature to bind a public key and an identity.

CCTV — Closed Circuit TV

Certificate Policy (CP) — A named set of rules that indicates the applicability of a certificate to a particular community/class of application with common security requirements

Certification Practice Statement (CPS) — A statement of the practices which a certification authority employs in issuing certificates

Certification Practice Statement (CPS) — A statement of the practices which a certification authority employs in issuing and managing certificates.

Control — "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration, but in no case less than 10%
Country — Either a member of the United Nations OR a geographic region recognized as a Sovereign State by at least two UN member nations

CRL — Certificate Revocation List

DRP — Disaster Recovery Plan

DN — Distinguished Name

FIPS — Federal Information Processing Standards

HSM — Hardware Security Module, a device designed to provide cryptographic functions, especially the safekeeping of private keys

HTTP — Hyper Text Transfer Protocol

HVAC — Heating, Ventilation and Air Conditioning

IEC — International Electro-technical Commission

IETF — Internet Engineering Task Force

IPSEC — Internet Protocol Security

ISO — International Standards Organization

Issuer — The name of the CA that signs the certificate

Issuing Certification Authority (Issuing CA) — In the context of a particular certificate, the issuing CA is the CA that issued the certificate

ITU — International Telecommunications Union

Key Compromise — A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value. A Private Key is also considered compromised if methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys) or if there is clear evidence that the specific method used to generate the Private Key was flawed

KGC — Key Generation Ceremony, the complex procedure for the generation of a CA's private key

LDAP — Lightweight Directory Access Protocol, a common standard for accessing directories

OID — Object Identifier, a value (distinguishable from all other such values) which is associated with an object. (ITU-T X680) Referred in many RFCs and used in the ASN.1 encoding of certificates

OSCP — Online Certificate Status Protocol

PA — Policy Authority

PIN — A Personal Identification Number or password used to protect the private information and keys on hardware tokens

PKCS # 1 — Public-Key Cryptography Standards (PKCS) #1

PKCS # 7 — Cryptographic Message Syntax

PKCS #10 — Certification Request Syntax Specification

PKCS #12 — Personal Information Exchange Syntax published by RSA Security

PKI — Public Key Infrastructure

PKIX-CMP — Internet X.509 Public Key Infrastructure - Certificate Management Protocol

Policy Qualifier — Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate

Private Key — The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key

Public Key — The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages, so that they can be decrypted only with the holder's corresponding Private Key

Public Key Infrastructure — A set of hardware, software, people, procedures, rules, policies and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography

RA — Registration Authority

Re-Key — Ceasing use of a key pair and then generating a new key pair to replace it

Relying Party — A recipient of a certificate who acts in reliance on that certificate/digital signatures verified using that certificate

Renewal — Issuance of a new certificate to the subscriber without changing the subscriber’s public key or any other information in the certificate

Repository — A trustworthy system for storing and retrieving certificates or other information relevant to certificates

RSA — The acronym for the inventors of the RSA algorithm; Ron Rivest, Adi Shamir and Leonard Adleman

Secret Shares — A set of devices, smart cards, PINs, etc. used with MofN control

SHA — Secure Hash Algorithm

S/MIME — Secure Multipurpose Internet Mail Extensions

SSL/TLS — Secure Sockets Layer/Transport Layer Security

Sponsor — An individual or organization authorized to vouch for another individual in their employment or an electronic device in their control
SubjectAltName — A certificate attribute field that often contains the subject's e-mail address

Subject — A subject is the entity named in a certificate

Subscriber — A subject who is issued a certificate

Trusted Role — Those individuals who perform a security role that is critical to the operation or integrity of a PKI

UPS — Uninterruptible Power Supply

URI — Universal Resource Identifier, a URL, FTP address, email address, etc.

X.501 — A common standard for directory entry naming (ITU)

X.509 — A public key certificate specification originally developed as part of the X.500 directory specification, often used in public key systems; it is now governed by IETF standards

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

Solutions maintains its PKI repositories in the form of directories and/or secure URL locations where relevant certificates and the certificate status information (e.g. CRLs) will be published. The repositories provide access through the standard HTTP protocol.

Solutions' PKI repositories are available on a 24/7 basis and designed in such a way as to maintain high availability throughout operations.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 PUBLICATION OF CERTIFICATES AND CERTIFICATE STATUS

Solutions' maintains repositories that allow Relying Parties to make on-line enquiries regarding revocation and other certificate status information. The Intermediary CA provides Relying Parties with information as part of the certificate on how to find the appropriate repository to check certificate status as well as how to find the appropriate OCSP (Online Certificate Status Protocol) responder.

Solutions' PKI repositories contain the following PKI related elements:

- Issuing 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 Intermediary CA publishes CRLs including any changes since the publication of the previous CRL, at regular intervals. The URL where a CRL is published is mentioned in section 7.1 as part of the certificate profile of each certificate file.

2.2.2 PUBLICATION OF CA INFORMATION

The CPS shall be made available to all Intermediary CA PKI Participants at Solutions' website https://solutions.com.sa/repository/. This web site is the only source for up-to-date documentation and Intermediary CA reserves the right to publish newer versions of the documentation without prior notice. Additionally, Solutions publishes an approved, current and digitally signed version of the CPS at the same repository.

2.2.3 INTEROPERABILITY

Repositories used to publish CA certificates and CRLs are based on standard HTTP distribution points.

2.3 TIME OR FREQUENCY OF PUBLICATION

The Issuing CAs certificates is published in the repository as soon as possible after issuance. CRLs are issued within 24 hours after revocation. Each CRL includes a monotonically increasing sequence number for each CRL issued.

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 PKI Committee and NCDC.

2.4 ACCESS CONTROLS ON REPOSITORIES

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

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

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

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

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

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

The subject name contained in certificates issued under the Solutions' PKI Hierarchy must be meaningful in the sense that the 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 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 Issuing CAs' 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 Issuing CAs) in a way that is easily understandable for humans.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

The Intermediary CA does not issue anonymous or pseudonymous certificates.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

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

The Intermediary CA is configured in such a manner as to enforce name uniqueness for certificates that it issues. The Intermediary CA is responsible for ensuring name uniqueness in the Issuing CAs' 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

Names can only contain trademarks in case the subscriber has the legal right to use the trademark in question. Where applicable, The Intermediary RA enforces this verification as part of the certificate enrolment process.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

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

3.2.3 IDENTITY-PROOFING OF INDIVIDUAL IDENTITY

The Intermediary CA does not issue certificates for individuals.

3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

All subscriber information contained within certificate issued by the Intermediary CA is verified by the Intermediary RA.

3.2.5 VALIDATION OF AUTHORITY

The PKI Committee verifies 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 Issuing CA private keys are described in section 6.3.2. During the Re-keying process the 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

If any one of the Issuing CAs is revoked, the Intermediary CA must authenticate a re-key in the same manner as for initial registration. This will be done through a formal Key Ceremony process approved by the PKI committee to generate new keys for the revoked Issuing CA and certify the new keys.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUESTS

Prior to the revocation of Solutions' Issuing CA certificate, the PKI Committee shall verify that the revocation has been requested by authorized personnel.

Acceptable procedures for authenticating the revocation requests include:

- A request for revocation of the issuing CA is initiated by authorized personnel, such as the Solutions' Policy Authority;
- The PKI Committee shall approve such requests
- Revocation of the issuing CA shall be performed using a scripted and witnessed process.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The PKI Committee shall consider applications for Issuing CA certificate generation as part of a new CA establishment. The PKI Committee shall only accept applications for the Issuing CAs establishment from Trusted employees within Solutions' PKI.

The 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 Issuing CA.
- Approve the Key generation Script and set the date for the Key Ceremony

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

- Constitute the Key Shareholders and relevant parties for the Intermediary CA;
- Activate the Intermediary CA key;
- Generate the Certificate relating to that Issuing CA;
- Transmits the Certificate to the requesting Issuing CA; and
- Publish the Issuing CA certificate to Solutions' PKI repository.

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

Applications for the establishment of the internal Issuing CAs under the Intermediary CA shall be made by authorized personnel to the PKI Committee. The PKI Committee processes the request and advice the requester of the outcome.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

The PKI Committee authorize the setup of Issuing CAs and perform all necessary internal verification involving the PKI operations team. These verifications include the following steps:

- The conclusion of internal ceremony dry runs and a resulting report from the PKI Committee audit function
- The readiness of necessary key ceremony documents related to certifying Solutions' Issuing CA
- The confirmation from Solutions' PKI operations authority on the readiness of the operations team to operate the Issuing CAs post the go live ceremonies
- Approval from the PKI Committee for executing the necessary key ceremonies

Once the key ceremony procedure is finally approved by the PKI Committee, the certificate application processing for the Issuing CAs can then be planned and executed according to the approved key ceremony procedure.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

Refer to section 4.1 of this CPS. More details on the verification process shall be specified in the CPS.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

The PKI Committee will approve an application for a Issuing 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 Issuing CA establishment is not inconsistent with the requirement and provisions of the STCS Intermediary CA CP and this CPS

The 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 PKI Committee believes that approving the establishment of the Issuing CA may bring the Intermediary CA into disrepute or such an establishment is unlawful or inconsistent with the Intermediary CA or Saudi National PKI Policies.

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

The 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 Intermediary CA issues an Issuing CA certificate following the approval by the PKI Committee.

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

Certificate issuance operations for the Issuing CAs are executed in accordance with the approved key ceremonies procedures.

The pre-conditions for executing the ceremony are documented in clause 4.1 and 4.2. As part of the ceremony. At a minimum, the following verification steps are performed:

- Identity verification of all attendees
- Validation of the format of the certificate request (shall be in PKCS#10 format)
- Verification that the certificate request contains valid subscriber data (as per the provisions of this CPS)

Following the successful completion of the ceremony and the issuance of Solutions' issuing CA certificate, the Intermediary CA team inspects the file contents and performs a verification against the expected certificate format. The certificate is then handed over to the Issuing CA

team for further processing and import into the target Issuing CA systems. All parties that participated in the ceremony sign a ceremony report.

Further details on the certificate issuing process are documented in the related Solutions' key ceremony documentation.

4.3.2 Notification of Certificate Issuance

Following issuance and validation of the certificate content, Solutions' posts an issued certificate on the Solutions' PKI Repository.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

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

The use of the Issuing 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 Issuing CA Certificates will be published, once accepted, in the appropriate repository as described in section 2.1.

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 Issuing CA Private Key and Certificate Usage

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

The Issuing 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 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 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 Intermediary CA issued certificates to Issuing CAs.

4.6.1 CIRCUMSTANCES FOR CERTIFICATE RENEWAL

The STCS Intermediary CA may renew the Issuing CA certificates provided the following conditions are met:

- The original Issuing CA certificate to be renewed has not been revoked;
- The details in the original Issuing CA certificate remains accurate and that no new or additional validation is required.

Should the above not be met, a new Issuing CA certificate must be issued following a Key Generation process similar to what was followed for issuing the initial Issuing CA certificate.

4.6.2 WHO MAY REQUEST CERTIFICATE RENEWAL

The request for renewal may only be made by authorized personnel. The PKI Committee shall approve all such requests.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

The renewal request may only be processed after receiving such a renewal request from the original authorized personnel or a representative. The PKI Committee shall process all Issuing CA Certificate Renewal Requests after satisfying itself of the authenticity and validity of the request.

4.6.4 NOTIFICATION OF RENEWED CERTIFICATE ISSUANCE

Issuing CA certificate renewals shall follow the same notification method as a new Issuing CA certificate issuance.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE

Issuing CA renewal certificate acceptance shall follow the same conditions for a new Issuing CA acceptance.

4.6.6 PUBLICATION OF A RENEWAL CERTIFICATE

The Issuing CA renewed certificate shall be published at the same location as the original certificate.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Generally, Intermediary CA does not notify other entities of a renewed Issuing CA certificate apart from requesting party.

4.7 CERTIFICATE RE-KEY

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

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

4.7.1 CIRCUMSTANCES FOR CERTIFICATE RE-KEY

Prior to the expiration of an existing Issuing CA Certificate, it is necessary for the Issuing 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 an Issuing CA certificate shall be done as part of a witnessed key ceremony process similar to the initial key generation and certificate issuance. The re-key operation shall invalidate any existing active certificate for an Issuing CA.

4.7.2 WHO CAN REQUEST A CERTIFICATE RE-KEY

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

4.7.3 PROCESSING CERTIFICATE RE-KEYING REQUESTS

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

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Notification of issuance of a re-keyed certificate to Subscribers follows the same procedures as notification for newly issued 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, Intermediary CA does not notify other entities of a re-keyed certificate apart from the requesting party.

4.8 Certificate Modification

The Intermediary CA does not support any form of Issuing CA certificate modification. The issued Issuing 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

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

The Intermediary CA will notify other participants of certificate revocation through access to the CRL at the Solutions' PKI repository or through the OCSP.

4.9.1 Circumstance for Revocation of a Certificate

The Intermediary CA shall revoke the Issuing CA Certificates for the following non-exhaustive reasons:

- The Intermediary CA suspects or determines that the Issuing CA Private Key is compromised.
- If a subordinate Issuing CA contravenes any provisions of the Saudi National PKI Policy, Saudi e-Transactions Act and applicable By-laws;
- The Intermediary CA suspects or determines that revocation of an Issuing CA Certificate is in the best interest of the integrity of Solutions' PKI Hierarchy;
- The Intermediary CA determines that a Certificate was not issued correctly in accordance with this CPS;

Whenever any of the above circumstances occur, the PKI Committee holds an exceptional meeting (if required) after the circumstances of certificate revocation were identified. The PKI Committee may request additional information/evidence. At the end of this process, the PKI Committee approves the CA certificate revocation and the CA certificate revocation process. The PKI committee also decides on the actions related to end-user certificates issued from the Issuing CA to be revoked. In case if the revocation is requested as part of a corrective action (as the case may be for the last 2 circumstances mentioned above), the PKI Committee may decide (as it see relevant and according to the applicable CP/CPS) to re-issue the certificate of the issuing CA as well as the end-user certificates signed the Issuing CA

certificate to be revoked. The PKI committee decisions are documented as part of the PKI Committee meeting minutes.

The certificate revocation ceremony is planned and executed after the CA certificate revocation is authorized by the PKI Committee. The revocation ceremony is witnessed by members of the PKI Committee. The outcome of the ceremony will be as follows:

- The CA certificate is revoked with the right revocation reason on the Intermediary CA system
- A CRL is generated by the Intermediary CA and placed on the target public location
- The PKI Committee may decide to publish a notice containing the details of the certificate being revoked and the revocation circumstances

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 PKI Committee can request the revocation of any of the Issuing CA certificates issued under the Intermediary CA PKI Hierarchy;
- A legal, judicial or regulatory agency can request a revocation of any of the Issuing 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 Intermediary CA shall authenticate the request as well as the authorization of the requester in accordance with the applicable Agreements. The PKI Committee has the final approval for the revocation of the Issuing CA certificates.

The revocation request ***of*** an Issuing ***CA Certificate*** shall be sent to the PKI Committee. The STC PKI Committee follows the process described in section 4.9.1 in order to authorize the revocation of the Issuing CA certificate. One the revocation is authorized; the Intermediary CA operation team follows the revocation procedure in order to revoke the subject certificate. The revoked CA certificate shall then be published in the CRL of the Intermediary CA.

4.9.4 REVOCATION REQUEST GRACE PERIOD

The Intermediary CA will revoke certificates as quickly as practical upon receipt of a legitimate revocation request, or at a time agreed by the PKI committee as long as the revocation is not due to a compromise. The Issuing CA are required to request revocation within one day after detecting the loss or compromise of the Private Key.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

The Intermediary CA processes authorized revocation requests within 24 hours or at a time agreed by the PKI committee as long as the revocation is not due to a compromise.

4.9.6 REVOCATION CHECKING REQUIREMENTS FOR RELYING PARTIES

Revocation information is offered to relying parties through CRLs published on the Solutions' PKI repository or through its OCSP responder. Relying parties shall use any of these methods while processing a certificate issued by the Intermediary CA.

4.9.7 CRL ISSUANCE FREQUENCY

The Intermediary CA will publish its CRLs at least once every 6 months and within 24 hours of any Certificate revocation of its Issuing 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

Certificate status information shall be provided through the OCSP for the Intermediary CA.

4.9.10 ONLINE REVOCATION CHECKING REQUIREMENTS

It is at the discretion of the relying party to decide whether using CRL or relying on OCSP.

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

The Intermediary CA will not provide other forms of revocation advertisements.

4.9.12 SPECIAL REQUIREMENTS RELATED TO KEY COMPROMISE

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

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

4.9.13 CIRCUMSTANCES FOR CERTIFICATE SUSPENSION

Not applicable.

4.9.14 WHO CAN REQUEST SUSPENSION

Not applicable.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.9.17 Circumstances for Terminating Suspended Certificates

Not applicable.

4.9.18 Procedure for Terminating the Suspension of a Certificate

Not applicable.

4.10 Certificate Status Services

The status of the Issuing CAs public certificates is made available through CRLs in the repositories as well as the OCSP responder.

4.10.1 Operational Characteristics

CRLs shall be published by on a public repository which is available to relying parties through HTTP protocol queries.

The OCSP responders shall expose an HTTP interface accessible to relying parties.

4.10.2 Service Availability

The repository, including the latest CRL, should be available 24X7 for at least 99% of the time.

4.10.3 Optional Features

No stipulation — this section is intentionally left blank.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

The Intermediary CA does not support Key Escrow.

5 FACILITY MANAGEMENT AND OPERATIONAL CONTROLS

5.1 PHYSICAL SECURITY CONTROLS

Solutions has delegated the operations of the Solutions' PKI (Intermediary and Issuing CAs), Repositories and OCSP responder to Sirar by stc which is a sister company to Solutions.

Solutions' PKI is hosted at Sirar by stc's data center, with appropriate physical and procedural access controls for all hardware and software sub-systems used in the issuance and revocation of certificates. Access to functions critical to registration and certification is limited to personnel in Trusted Roles

Solutions PKI shall enforce 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 (Sirar by stc's Data Center) hosting the Solutions' 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

Solutions' PKI 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.

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

- Intermediary CA systems are installed in a secure facility that is protected from outside networks, with all access controlled;
- Solutions' 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 Solutions' 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 Sirar by stc's Data Center, with access limited to authorized personnel.

Sirar by stc's Data Center uses human guards to continually monitor the access to the facility housing the CA equipment. Sirar by stc's 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

Sirar by stc's 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 Solutions' PKI facilities ensures that no single point of failure is supported by providing the following measures:

- Two independent power supplies feeding the Sirar by stc's 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 Solutions' Business Continuity Plan.

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

5.1.4 WATER EXPOSURE

Solutions 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

Solutions 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 is subject to multiple-layer security storage requirements. Procedures include full back-up of the 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 that they are protected 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 Intermediary CA.

5.1.7 WASTE DISPOSAL

Solutions' 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 Intermediary CA, sufficient to recover from system failure, are made on a periodic schedule as described in Solutions' Operations Policies and Procedures.

The backup site has physical and procedural controls commensurate to that of the Solutions' 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 Solutions to fill these roles will be extraordinarily responsible. The functions performed in these roles form the basis of trust for the entire Solutions' 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) Security Officer

The Security 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) Solutions' Policy Authority

The Solutions' Policy Authority role is responsible for:

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

4) 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.

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

Solutions 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 the Governance and

Operating Model document. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over the system operation.

The 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 Intermediary CA.

5.2.3 IDENTITY-PROOFING FOR EACH ROLE

Before exercising the responsibilities of a trusted role:

- Solutions shall confirm the identity of the employee by carrying out background checks.
- Solutions shall issue an access card to administrators who need to access equipment located in the secure enclave.
- Solutions shall provide the necessary credentials that allow administrators to conduct their functions.

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 the Governance and Operating Model 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 Governance and Operating Model document.

5.3.2 BACKGROUND CHECK AND CLEARANCE PROCEDURES

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

- Availability of satisfactory character reference, i.e., one business and one personal;
- A check (for completeness and accuracy) of the applicant's CV;
- Confirmation of claimed academic and professional qualifications;
- Independent identity check (National ID card, Passport or similar document);
- Interviews with references shall be done as required; and
- More detailed checks, such as security clearance.

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

5.3.3 TRAINING REQUIREMENTS AND PROCEDURES

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

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

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

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

Individuals performing PKI roles are made aware of changes in the Solutions' 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 Solutions' PKI software or hardware upgrade, changes in automated security systems, and relocation of equipment.

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

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

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

5.3.7 CONTRACTING PERSONNEL REQUIREMENTS

When Solutions 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 Intermediary CA CP, this CPS, Solutions' 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

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

5.4 AUDIT LOGGING PROCEDURES

Solutions 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 Intermediary CA and other associated components.

Intermediary CA systems generate audit log files for all events relating to the security of the 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 PKI Committee ensures recording in audit log files all events relating to the security of the CA system hosted in Sirar by stc's data centcer. 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:
    c. Certificate requests, renewal, and re-key requests, and revocation;
    d. All verification activities stipulated in these Requirements and the Issuing CAs' Certification Practice Statement;
    e. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    f. Acceptance and rejection of certificate requests;
    g. Issuance of Certificates; and
    h. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
    i. Successful and unsuccessful PKI system access attempts;
    j. PKI and security system actions performed, such as:
        - the value of maximum authentication attempts is changed;
        - an administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
    k. Security profile changes;
    l. System crashes, hardware failures, and other anomalies;
    m. Firewall and router activities; and
    n. Entries to and exits from the Solutions' PKI facility.
    o. Equipment failure or electrical power outages
    p. Changes to CA configuration and system clock time

Log entries MUST include the following elements:

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

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

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

5.4.2 FREQUENCY OF PROCESSING DATA

The PKI Committee shall ensure that the designated personnel reviews log files at regular intervals to validate log integrity and ensure timely identification of anomalous events.

Designated personnel must report and perform follow-up of these events and any issues affecting audit log integrity.

Log files and audit trails shall be periodically archived for inspection by authorized personnel.

The log files shall be properly protected by an access control mechanism, so that no others can have access. Log files and audit trails shall be backed up.

All log entries include the following elements:

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

5.4.3 RETENTION PERIOD FOR AUDIT LOG

Solutions 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

Solutions backs up all audit logs and audit summaries in a secure location and protected to the same degree as the originals.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

The audit 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 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

Solutions 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, Sirar by stc's data centre is constantly (24x7) monitored, and all attempts to gain unauthorized access to any of the services are logged and analyzed.

Solutions performs third party penetration testing for Sirar by stc's 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 Solutions' Risk Assessment Methodology. Solutions' 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 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

Solutions shall retain in a trustworthy manner records of digital certificates, audit data, systems information and documentation. Solutions shall ensure that at least the following records are archived:

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:
   c. Certificate requests, renewal, and re-key requests, and revocation;
   d. All verification activities stipulated in these Requirements and the Issuing CAs' Certification Practice Statement;
   e. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
   f. Acceptance and rejection of certificate requests;
   g. Issuance of Certificates; and
   h. Generation of Certificate Revocation Lists and OCSP entries.
3. Security events, including:
   i. Successful and unsuccessful PKI system access attempts;
   j. PKI and security system actions performed, such as:
      - the value of maximum authentication attempts is changed;
      - an administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
   k. Security profile changes;
   l. System crashes, hardware failures, and other anomalies;
   m. Firewall and router activities; and
   n. Entries to and exits from the Solutions' PKI facility.
   o. Equipment failure or electrical power outages
   p. Changes to CA configuration and system clock time

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 PKI Committee. Solutions minimum retention period for archive data is established at ten (10) years.

The Intermediary CA shall retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least ten (10) 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 personnel shall be permitted to review the archive. The contents of the archive shall not be released except as determined by NCDC, PKI Committee, 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 Solutions' 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 Solutions' 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

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

The PKI Committee 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 PKI Committee shall be notified by the NCDC if any of the following cases occurs;

- NCDC plans to revoke the 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.

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 Solutions' PKI management and Solutions' PKI's incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, Solutions' 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 Intermediary CA being compromised, lost or destroyed or suspected to have been compromised, the Intermediary CA, after investigation of the problem, shall decide if the Intermediary CA Certificate should be revoked. If so, then:

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

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

Solutions 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.

Solutions' PKI equipment at the primary site (Sirar by stc's data center) have built-in hardware fault-tolerance and configured to be highly available with auto-failover switching. Solutions 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.

Solutions' 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 of Solutions' PKI 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.

Solutions' 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.

Solutions has developed recovery plans to mitigate the effects of any kind of natural, man-made or equipment failure related disaster.

Solutions has implemented an alternate recovery site as per industry standards to provide full recovery of critical PKI services in case of the disaster related events. Solutions' Business Continuity Policy includes further details .

5.8 CA TERMINATION

In the event that the STC Intermediary CA ceases operation, it must notify its Issuing 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 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 Issuing CAs of each unrevoked or unexpired Certificate issued by it 60 days' notice by sending an electronic mail to the Issuing CA relevant teams of its intention to cease acting as a CA;
4 ensure that discontinuing its operations causes minimal disruption to its Issuing 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 Intermediary CA CP

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

The 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 Solutions' PKI (Intermediary and Issuing CAs), the Hardware Security Modules (HSM's) used for key generation meet the requirements of FIPS 140-2 Level 3.

The 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 Intermediary CA management.

6.1.2 PRIVATE KEY DELIVERY TO END-ENTITIES

The Intermediary CA does not generate private keys to its end entities (Issuing 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 Issuing CA Public Key must be transferred to the Intermediary 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

The Intermediary CA Public Key shall be delivered to the Relying Parties by making it available as set forth in section 2.2.1.

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.

Issuing CAs keys is 4096-bit RSA while the OCSP responders keys is 2048-bit RSA. 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 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
4) OCSP Key Pair: 2048 bits RSA

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

The Intermediary CA shall generate public keys in accordance with industry standards such as FIPS 186-4 and check public key parameters for their validity.

6.1.7 KEY USAGE PURPOSES

Public keys that are bound with the Issuing CAs certificates shall be certified for use in Certificate and CRL signing. The use of a specific key is determined by the key usage extension in the X.509 certificate. The Intermediary CA key is used for Certificate and CRL signing.

6.2 PRIVATE KEY PROTECTION AND CRYPTO-MODULE ENGINEERING CONTROLS

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

Cryptographic modules employed for private key protection for the Intermediary CA and the OCSP Responder shall comply with FIPS-PUB 140-2 “Security Requirements for Cryptographic Modules”, Level 3 and above.

6.2.2 CA PRIVATE KEY MULTI-PERSON CONTROL

Multi-person control of the Intermediary CA private key is achieved using an “m-of-n” split key knowledge scheme. 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.

The OCSP Responder private key may not be under multi-person control.

6.2.3 PRIVATE KEY ESCROW

The Intermediary CA does not escrow the Issuing CAs’ Private keys.

6.2.4 PRIVATE KEY BACKUP

Solutions uses the mechanisms provided by the HSM’s to backup the Intermediary and Issuing CAs are backed up and held stored safely in exclusive safes maintained in the most inner security zones of the primary PKI facilities. Backup operations are executed as part of the CA key generation ceremonies.
The DR keys are backed up under the same dual control and split knowledge as the primary keys. The DR keys are kept at the backup location identified as disaster recovery location.
Procedures for backing up the CAs Keys are specified as part of Solutions’ key ceremony procedures.

6.2.5 PRIVATE KEY ARCHIVAL

The Intermediary CA does not archive Private Keys.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

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

6.2.10 METHODS OF DESTROYING PRIVATE KEYS

The STSC Intermediary CA and Issuing CAs under the PKI hierarchy Private keys shall be destroyed as per Solutions' Cryptographic Devices Lifecycle Management Policy and Procedure, which shall be consistent with section 6.2.2 of the 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 Intermediary CA certificate (which contains the public key) is backed up and archived as part of the Intermediary CA and Sirar by stc's 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
OCSP Signing Key	2048	36 months

6.4 ACTIVATION DATA

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

The Intermediary CA and the Issuing 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 Sirar by stc's data centre.

In addition, the activation data shall be secured at the same level as the cryptographic data for the Intermediary CA and Issuing 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 Intermediary CA servers hosted in Sirar by stc's 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.

Sirar by stc's data centre has implemented layered security approach to ensure the security and integrity of the computers used to run the Intermediary CA software. The following controls ensure the security of Sirar by stc's 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

Solutions employs the following System Development controls:

- Solutions may use standard software from product vendors for version control. Where Solutions 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;
- Solutions 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 Solution' 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 Intermediary CA system as well as any modifications and upgrades must be documented and controlled in accordance with Solutions' 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

Any of the Intermediary CA or the Issuing CAs IT systems or components that are replaced are taken out of operation according to Solutions' change management and the other relevant operational procedures.

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.

Sirar by stc's 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 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.

Sirar by stc's data centre network security controls are designed to protect Solutions' 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 Issuing CA Certificates;
- Revocation of Issuing CA Certificates;
- Posting of CRL updates;

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

QUCA certificate profile:

Field / x.509 extension	Value or Value Constant	Critical
Version	2 (Version 3)	V1 Field
SerialNumber	At least 64 bits of entropy validated on duplicates.	V1 Field
Signature	SHA256 with RSA Encryption	V1 Field
Issuer	CN = STCS Intermediary CA O = STCS C = SA	V1 Field
NotBefore	Certificate generation process date/time.	V1 Field
NotAfter	Certificate generation process date/time + Up to 120 months (10 years)	V1 Field
Subject	CN = STCS QUCA O = STCS C = SA	V1 Field
SubjectPublic KeyInfo	Public Key Key length: 4096 (RSA)	V1 Field
CRL Distribution Points	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.stcs.com.sa/CRL/stcs_intca_crlfile.crl	NO
Authority Key Identifier	<subjectKeyIdentifier of STCS Intermediary CA>	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=CA Path Length Constraint=0	YES
Certificate Policies	[1]Certificate Policy: Policy Identifier=<2.16.682.1.101.5000.1.4.1.2.1.2> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.stcs.com.sa/repository	NO
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://crl.stcs.com.sa/certs/stcs_intca.crt [2]Authority Info Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.stcs.com.sa	NO
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing	YES

IDCA certificate profile:

Field / x.509 extension	Value or Value Constant	Critical
Version	2 (Version 3)	V1 Field
SerialNumber	At least 64 bits of entropy validated on duplicates.	V1 Field
Signature	SHA256 with RSA Encryption	V1 Field
Issuer	CN = STCS Intermediary CA O = STCS C = SA	V1 Field
NotBefore	Certificate generation process date/time.	V1 Field
NotAfter	Certificate generation process date/time + Up to 120 months (10 years)	V1 Field
Subject	CN = STCS IDCA O = STCS C = SA	V1 Field
SubjectPublic KeyInfo	Public Key Key length: 4096 (RSA)	V1 Field
CRL Distribution Points	e.g. [1]CRL Distribution Point Distribution Point Name: Full Name: URL= http://crl.stcs.com.sa/CRL/stcs_intca_crlfile.crl	NO
Authority Key Identifier	<subjectKeyIdentifier of STCS Intermediary CA>	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).	NO
Basic Constraints	Subject Type=CA Path Length Constraint=0	YES
Certificate Policies	[1]Certificate Policy: Policy Identifier=<2.16.682.1.101.5000.1.4.1.2.1.2> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.stcs.com.sa/repository	NO
Authority Information Access	[1]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://crl.stcs.com.sa/certs/stcs_intca.crt [2]Authority Info Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL= http://ocsp.stcs.com.sa	NO
Key Usage	Certificate Signing, Off-line CRL Signing, CRL Signing	YES

7.1.1 VERSION NUMBERS

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

7.1.2 CERTIFICATE EXTENSIONS

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

The Issuing certificates may include any extensions as specified by RFC 5280 in a certificate, but must include those extensions required by 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

The Intermediary CA shall sign the Issuing CA 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).

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 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 Intermediary CA CRL Profile is shown below:

7.2.1 STCS INTERMEDIARY CA CRL PROFILE

Field	Content	Comment
Version	1 (Version 2)	
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	The intermediary CA's Subject Key Identifier	
CRL number	<number>	

7.2.2 VERSION NUMBERS

The 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

OCSP requests and responses shall be in accordance with RFC 6960.

The OCSP response signing certificate profile is as follows:

Field / x.509 extension	Value or Value Constant	Critical
Version	2 (Version 3)	V1 Field
SerialNumber	At least 64 bits of entropy validated on duplicates.	V1 Field
Signature	SHA256 with RSA Encryption	V1 Field
Issuer	CN = STCS Intermediary CA O = STCS C = SA	V1 Field
NotBefore	Certificate generation process date/time.	V1 Field
NotAfter	Certificate generation process date/time + Up to 36 months (3 years)	V1 Field
Subject	CN = STCS Intermediary CA OCSP Service O = STCS	V1 Field

Field / x.509 extension	Value or Value Constant	Critical
	C = SA	
SubjectPublicKeyInfo	Public Key Key length: 2048 (RSA)	V1 Field
Authority Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey of the **STCS INTERMEDIARY CA** (excluding the tag, length, and number of unused bits).	NO
Subject Key Identifier	keyIdentifier encoded in compliance to RFC 5280 The keyIdentifier should be composed of the 160-bit SHA-1 hash of the value of the BIT STRING **subjectPublicKey** (excluding the tag, length, and number of unused bits).	NO
Certificate Policies	[1]Certificate Policy: Policy Identifier=<**2.16.682.1.101.5000.1.4.1.2.1.2**> [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: https://www.stcs.com.sa/repository [2]Certificate Policy: Policy Identifier=<**2.16.682.1.101.5000.1.4.1.2.1.1.5**>	NO
OCSP No Revocation Checking (id-pkix-ocsp-nocheck)		NO
Key Usage	digitalSignature, nonRepudiation	YES
Extended keyUsage	Id-kp-OCSPSigning	NO

7.3.1 VERSION NUMBER

The version number for request and OCSP responses shall be v1.

7.3.2 OCSP EXTENSIONS

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The PKI Committee shall ensure that the requirements of the Intermediary CA CP and CPS and the provisions of applicable Agreements with NCDC are implemented and enforced. Intermediary CA shall undergo annual audits whose results shall be submitted to NCDC.

The PKI Committee shall ensure adherence of the Issuing CAs to this CPS, 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 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.

Further, the PKI Committee also performs an internal audit at least on a quarterly basis against a randomly selected sample for monitoring adherence and service quality.

The Subordinate Issuing CAs shall also follow the same audit frequency to ensure compliance against defined requirements.

8.2 IDENTITY AND QUALIFICATIONS OF ASSESSOR

The annual audit of the 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 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 Solutions' PKI operations environment is in compliance with the applicable CP, CPS and supporting operational policies and procedures. The term Solutions' 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 PKI Committee 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 (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 the PKI Committee, 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; 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 PKI Committee and/or NCDC as applicable.

The 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

Solutions 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

Solutions may charge access fees at its discretion to any database which stores issued certificates.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEE

Solutions does not charge fees to access certificate status information via the CRL nor the OCSP responder.

9.1.4 FEES FOR OTHER SERVICES

Solutions may charge fees for other services such as timestamping.

9.1.5 REFUND POLICY

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

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

9.2.1 INSURANCE COVERAGE

Solutions shall hold insurance cover in lieu of its performance and obligations under the following guidelines or that which is deemed sufficient by the 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

Solutions 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 Intermediary CA may be made publicly available at the discretion of NCDC and/or the PKI Committee. Specific confidentiality requirements for business information are defined in Solutions' 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 corporate or personal information held by NCDC or 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 Intermediary CA CP, and in accordance with Solutions Privacy Policy.

9.3.1.2 Certificate Information

The reasons for a certificate being revoked is considered confidential information, with the sole exception of the revocation of the Saudi National Root-CA or the 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 Intermediary CA in which case prior disclosure of the termination may be given.

9.3.1.3 PKI Documentation

Solutions' 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 Intermediary CA CP; 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 Solutions' PKI participants shall be responsible for protecting the confidential information they possess in accordance with Solutions' Privacy Policy and applicable laws and Agreements.

9.4 PRIVACY OF PERSONAL INFORMATION

Any personal identifying information collected by Solutions shall be protected in accordance with Solutions' Privacy Policy. 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 Solutions' 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 the Issuing Certificates such as the organization name, and public key will not be deemed private. Solutions' 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

Solutions' employees, suppliers and contractors handle personal information in strict confidence under the Solutions' contractual obligations that at least as protective as the terms specified in section 9.4.1.

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 Solutions' Privacy Policy.

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL/ADMINISTRATIVE PROCESS

Any disclosure shall be handled in accordance with Solutions' Privacy Policy.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

Any disclosure shall be handled in accordance with Solutions' Privacy Policy.

9.5 INTELLECTUAL PROPERTY RIGHTS

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

Solutions retains exclusive rights to any products or information developed under or pursuant to Intermediary CA CP.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA REPRESENTATIONS AND WARRANTIES

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

- Providing the operational infrastructure and certification services;
- Making reasonable efforts to ensure it conducts an efficient and trustworthy operation. "Reasonable efforts" include but are not limited to operating in compliance with:
  - Documented CP and CPS;
  - Documented Solutions Operations Policies and Procedures; and
  - Within applicable agreements, Saudi Law and regulations.
- At the time of Certificate issuance; 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 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 Solutions' 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

Solutions warrant that it performs registration functions as per the stipulations specified in this CPS and the CP.

9.6.3 RELYING PARTIES REPRESENTATIONS AND WARRANTIES

Relying Parties who rely upon the certificates issued under the Intermediary CA shall:

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

Determining that such Certificate provides adequate assurances for its intended use.

9.6.4 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

No stipulation.

9.7 DISCLAIMERS OF WARRANTIES

Solutions, 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.

Solutions 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 Intermediary CA or for the legal validity, acceptance or any other type of recognition of its own certificates, those issued by it through its Issuing CAs, any digital signature backed by such certificates, and any products provided by Solutions. Solutions 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:

- Solutions will not incur any liability to any person to the extent that such liability results from their negligence, fraud or willful misconduct;
- Solutions 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 Solutions from and against any such liability and costs and claims arising there from;
- Solutions 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;
- Solutions denies any financial or any other kind of responsibility for damages or impairments resulting from its CA operation.

9.9 INDEMNITIES

Notwithstanding any limitations on its liability to its Sub-CAs and Relying Parties, Solutions understands and acknowledges that the Application Software Suppliers who have supplied the CA software in use by the STCS Intermediary CA do not assume any obligation or potential liability of Solutions 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, Solutions 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 Intermediary 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 Intermediary 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).

Solutions shall indemnify, defend and hold harmless the following parties:

- Its directors, officers, employees, agents, consultants, and subsidiaries from any and all claims, damages, costs (including, without limitation, attorney's fees), judgments, awards or liability;
- Any parties relying on the STCS Intermediary CA 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 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 Intermediary CA CPS can be found at: https://solutions.com.sa/repository/.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

Upon termination of this CPS, all 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 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 CAs' Certificate assurance level.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

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

Intermediary CA reserves the right to change this CPS from time to time. 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 PKI Committee 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 PKI Committee shall provide their comments to the PKI Committee in accordance with NCDC rules.

The PKI Committee'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 Solutions.

9.13 DISPUTE RESOLUTION PROCEDURES

Any dispute arising out of or related to the digital certificates issued by the 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 Solutions' Dispute Resolution Policy.

DISPUTE RESOLUTION COMMITTEE

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

DISPUTE RESOLUTION POLICY

Solutions' Dispute Resolution Policy is applicable to all participants of the Solutions' 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 Intermediary CA CPS, without the prior written consent of Solutions.

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 Intermediary CA will be treated according to the laws of the Kingdom of Saudi Arabia.

9.16.5 FORCE MAJEURE

The 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 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 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 Solutions, 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 Solutions 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 Solutions.

9.17.2 ADMINISTRATIVE PROCESSES

As specified in Solutions' Operations Policies and applicable Agreements.