

SAUDI NATIONAL PKI POLICY

January 13 2009

Version 1.31

Document Classification:

Public

Document Reference

Item	Description
Document Title:	Saudi National PKI Policy
Department:	Policies , Rules & Regulations Department
Version No.:	1.31
Status:	Final
File Name:	Saudi_National_PKI_Policyv1.31.doc
Type:	MS Word Document
Author(s)	Dr. Deoraj B. M.
	Policies , Rules & Regulations Department Signature/Date
Reviewed by	Naif Alotaibi
	Policies , Rules & Regulations Department Signature/Date
Approved by	Dr. Fahad A. AlHoymany
	NPA Chairperson/ NCDC Director Signature/Date

Document Revision History

Version	Date	Author(s)	Revision Notes
1.0	25/10/2008	Dr Deoraj	First Draft
1.1	24/11/2008	Dr Deoraj	Document scope, Saudi PKI Diagram , Certificate assurance, Certificate life cycle management, key management, audit scope, Incorporated comments of Mohammed
1.2	25/11/2008	Dr Deoraj	Incorporated comments from Dr Fahad and Mohammed
1.3	13/01/2009	Dr Deoraj	Incorporated Figure approved by Dr Fahad
1.31	17/01/2009	Dr Deoraj	Copyright statement added

Document Control

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

Copies of this document will be held by:

- 1 Policies, Rules & Regulations Department
- 2 NPA Department

Table of Contents

1	Saudi PKI Framework	5
2	Scope	6
3	Introduction	7
4	Publication and Repository Responsibilities	8
5	Identification and Authentication	9
6	Certificate Life-Cycle Operational Requirements	9
7	Facility, Management, and Operational Controls.....	10
8	Technical Security Controls.....	12
9	Certificate, CRL, and OCSP Profiles.....	13
10	Compliance Audit and Other Assessments.....	13
11	Other Business and Legal Matters.....	14

1 Saudi PKI Framework

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, managed through the National Center for Digital Certification (NCDC). The NCDC is created by an act of law and its mandate is stipulated in the Saudi e-transactions law, articles 19 & 20

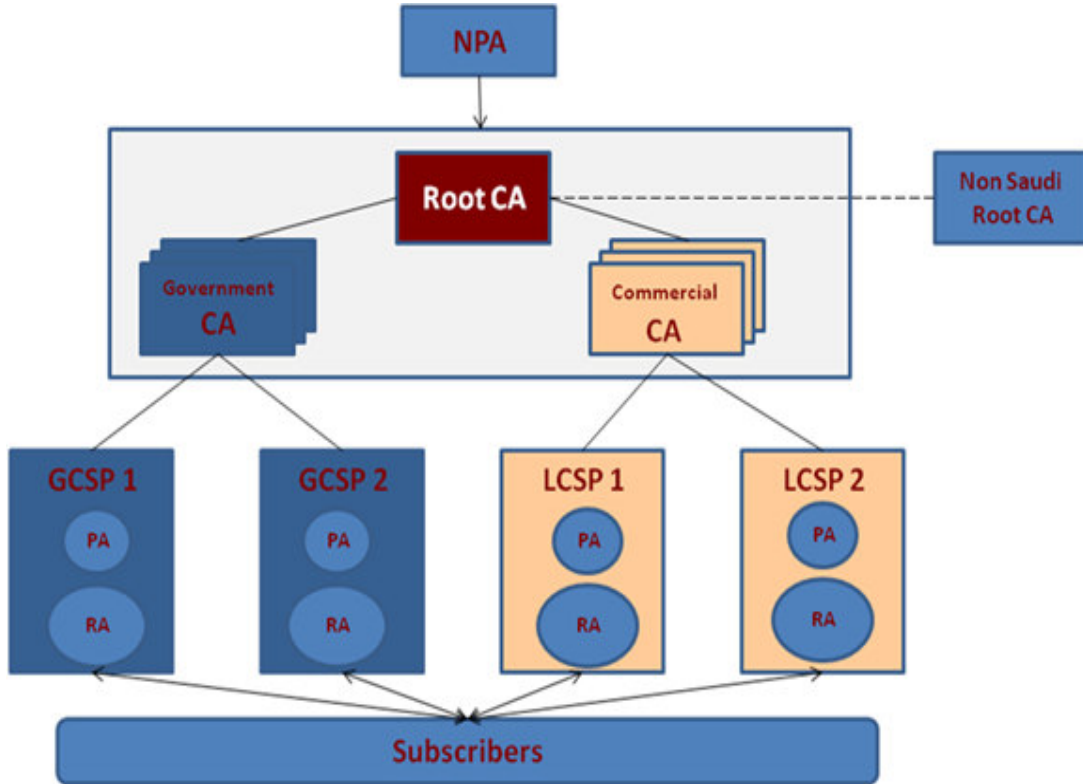
NCDC provides trust services to secure the exchange of information between key stakeholders. Participants include:

- Government
- Citizens
- Business

The NCDC operates as a closed business system model. It utilizes Digital Certificates issued by Certification Authorities (CAs) meeting rules established by the NCDC's policy committee, the National Policy Authority (NPA). NCDC's Digital Certificates support Authentication, Digital Signature, Encryption and non-repudiation services for access and processing of electronic information, documents and transactions.

A new service delivery model has been created whereby a shared National PKI Center has been created. The National Center for Digital Certification - Shared Services Center (NCDC-SSC) will consolidate and manage CSP's CAs and related operations for outsourced CA's joining the Saudi PKI.

The NCDC owns and operates the Root Certificate Authority of the Kingdom of Saudi Arabia. The CAs wishing to set up CA operations need to complete certain pre defined requirements laid down by the NPA. Approved CAs shall be issuers of NCDC Digital Certificates through Certificate Service Providers (CSPs) to Subscribers, Relying parties, Registration Authorities, and if expressly approved by the NPA. Together all of these components and participants form the "Saudi PKI." For any CA seeking accreditation, through cross certification the NPA ensures that a trusted chain is built up to the Saudi National Root CA.



2 Scope

This document is intended for use by the Certification Authority (CA) wishing to set up operations under the Saudi National Root CA. The aim of this document is to introduce requirements for such CAs and to ensure that such CAs can fit into the Saudi PKI framework.

3 Introduction

- This section identifies and introduces the set of provisions and indicates types of entities and applications for which the prospective CA going to issue certificates. This section can also be used to provide synopsis of the CA PKI business. A CA must have Certificate Policy (CP), PKI Disclosure Statement and a Certification Practice Statement (CPS) confirming to the CP. The Certification Authority Certificate Policy and Certification Practice Statement shall adhere to RFC-3647 with relevant supportive administrative, technical and operational documents. The CP shall be a public document published by the CA describing the conditions that are attached to use and application of the certificates it issues. The CPS shall be a controlled document describing the practices followed by the CA in managing the certificates it issues.
- The CA shall post a Public Disclosure Statement summaries the key points of the Certificate Policy for the benefit of Subscribers and Relying Parties
 - Every CA will obtain OID from NPA under the OID scheme set up for the Saudi PKI. OIDs shall be utilized from the OID arc allocated by the Saudi Arabian Standards Organisation.

<http://www.oid-info.com/cgi-bin/display?oid=2.16.682.1.101.5000&submit=Tree+display>

CAs can seek guidance from NCDC for OID allocation for the certificates types it is going to support.

- The CAs may issue certificates supporting different levels of assurance. For different levels of assurance, the CA shall assign separate OID for each certificate type and describe appropriate policies and practices followed specific to each qualified certificate type. The description covers following at a minimum but not limited to
 - certificate Subject
 - Assurance Level
 - Policy OID
 - Policy Name
 - Certificate Profile
 - Application Usage
 - Verification Process
 - Key Pair Generation & Installation
 - Certificate Issuance Process
 - Key usage
 - Private Key Protection
 - Certificate Life-time
 - Key Backup
 - Asymmetric Key Length
 - Certificate Re-key/Renewal

- Obligations
 - Liability
 - Fees
 - Warranties
 - External Auditing
 - Record maintenance
-
- The CA may issue different levels of assurance it supports for issuing certificates. In case of different levels of assurance, the CA shall describe appropriate applications or types of applications that are appropriate or inappropriate for different levels of assurance.

4 Publication and Repository Responsibilities

This section will define the provisions regarding the Certification Authority's obligations to publish information regarding its practices, certificates and current status of the certificates. This will also describe the access control on the published information such as Certificate Policy, certificates status and CRLs with the frequency of publication.

- Each CA shall have a repository for its issued certificates and CRLs. The CA repository must be available on a 24x7 basis and replicates the certificates issued.
- Repositories shall be fault tolerant and online with high availability provisions.
- Digital Certificate issued under the Saudi PKI must be X.509 in accordance to the RFC 3280 otherwise approved by the NPA.
- The CAs shall implement access restrictions for directory to prevent misuse and unauthorized harvesting of subscriber information.
- Repository information is stored using technology that supports the following industry standards and schema:
 - LDAP v3 operations
 - LDAP search filters
 - LDAP v3 intelligent referral
 - Relevant LDAP v3 RFCs
 - DSML (Directory Service Markup Language) v2
 - X.509 digital certificates
 - HTTP

5 Identification and Authentication

This section will describe procedures used by Certification Authority to authenticate a subscriber prior to certificate issuance. This will contain the naming practices adopted by the Certification Authority from name recognition, recognition to name dispute resolution. It will also describe how parties requesting re-key or revocation are authenticated.

- CSPs shall setup Registration processes based on the certificate type and assurance level for subscribers prior to issue them with certificates.
- The CSP may request to CA for specific type of certificate based on the requirement of their user community.
- The CA PA shall take up this with the NPA and based on approval grant permission for any changes in the current certificate or new certificates types.
- The registration request shall be supported with valid identity documentation.
- The CSPs may designate specific RAs to perform the Subscriber's Identification and Authentication and Certificate request and revocation functions defined in the respective CA-CP and other relevant documents.
- The RA is obligated to perform certain functions pursuant to an RA Agreement. An RA who performs registration functions represents and warrants that it shall comply with the stipulations of applicable CP, and the associated CPS.
- Where a Subscriber has already undergone an in-person identity and authentication process by a CSP to receive a certificate, the Subscriber can use that certificate and may obtain further NCDC-issued certificates without having to undertake another face-to-face registration based upon understanding between CSPs.

6 Certificate Life-Cycle Operational Requirements

This section will specify requirements imposed upon the Certifying Authority or subscribers regarding various operational activities with respect to Certificate life cycle management e.g. Certificate application, issuance, acceptance, suspension and revocation.

- The prospective CA must submit application to National Policy Authority for setting up Certification Authority business. In addition, for commercial CAs, a license must be obtained from the CITC after an application is approved by the NCDC NPA.
- All key backup functionalities shall be governed by CMP protocol in accordance with RFC 4210 and certification request syntax shall be in accordance with PKCS #10.

- CA private keys shall be encrypted and stored in a FIPS 140-2 Level 3 validated HSM.
- The CA signing keys shall be backed up under the same multi-person control as the original signature keys.
- Access to the CA's private key shall require multiple authorizations and tight security measures.
- The RA's/LRA's private keys shall be encrypted and stored in at least FIPS 140-2 Level 2 validated Smartcards or USB Tokens.
- Smart Cards or USB Tokens used to generate and store end-user certificates shall be at least FIPS 140-2 Level 2 validated.
- The maximum period for which a Certificate can be suspended shall not exceed ninety (90) days.
- The CAs issuing confidentiality certificates must provide key back up and support escrow mechanism for the end users decryption keys.
- When an authorized party requires access to encrypted data without the consent of the Subscriber who encrypted the data, a request to recover that data shall be sent to the escrow agent. The escrow agent, after securing proper authorizations, shall forward a request to fetch the Subscriber's private decryption key to the CA. The CA will then authorize access to the key from Backup or Archive, depending whether it is a current key or an expired/revoked certificate. The escrow agent shall then decrypt the message using that private key, and only return the decrypted message to the requesting authorized party.
- An independent Key Escrow service shall be established upon approval of the NPA for CSP's CAs that issue confidentiality certificates. Escrowed private keys shall be stored in encrypted form at an Independent Third-Party Escrow Agent (EA).
- A CA shall not back up Subscriber's private signing keys.
- The NPA reserves right to revoke any certificate if deem necessary.

7 Facility, Management, and Operational Controls

This section will describe the measures relating to non-technical security control to provide reasonable assurance that physical access to the Certifying Authority is limited to authorized trusted individuals with proper background checks. This section will indicate the level of security required to ensure that CA remains trusted and safe for its user communities and those with which it interoperates. The CA systems shall be hosted in a secured facility and protected from environmental hazards.

- A Threat Risk Assessment shall be performed before establishing the CA facility and operations.

- The CSP shall visit RA facility and review procedures with a contemplation of environmental factors, technological and operational infrastructures, and the security infrastructure as it relates to the services being offered as per the RA agreement.
- The CAs must perform third party vulnerability assessment at least once a year.
- The CAs shall retain all system generated (electronic) and manual audit records for a period not less than twelve months from the date of creation.
- The minimum retention period for archive data is ten years.
- All logs must be time stamped and CA must use GPS time synchronization.
- Time Servers shall be used to synchronize time for all CA-side components. The time servers shall operate as NTP servers in accordance to RFC 1305 and accommodative to SNTP in accordance to RFC 4330
- Multiple time servers shall be located in multiple security zones.
- The servers shall synchronize with a predefined set of reliable atomic clock time servers on the internet/using GPS which are secured and governed by a well known independent authority
- The CAs shall establish an appropriate separation of duties between key roles.
- All persons filling trusted roles shall be selected on the basis of skills, loyalty, trustworthiness, integrity and must be citizens of the Kingdom of Saudi Arabia. A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be extraordinarily responsible or the integrity of the PKI is weakened. Examples of such trusted roles for a CA operation are:
 - CA Master User
 - CA First Officer,
 - CA Administrator
 - CA Operator
 - CA Auditor,
- The CAs must ensure that contingency plans are prepared, tested and regularly updated to address business continuity of operations.

8 Technical Security Controls

This section will define the security measures taken by the issuing Certifying Authority to protect its cryptographic keys and activation data (e.g. PINs, password). Secure key management is critical component for any PKI and the issuing Certifying Authority shall ensure that all keys and activation data are protected and used by authorized personnel only. Also this section defines technical controls implemented by the Certifying Authority for performing functions such as certificate life cycle management, audit and archival. The technical security controls will include life-cycle security controls and operational security controls.

- The CA software shall be certified under the Common Criteria or ITSEC to a level equivalent to Common Criteria EAL 4.
- The CA's, Hardware Security Modules (HSM's) used for key generation shall meet the requirements of FIPS 140-2 Level 3, and/or Common Criteria EAL4+.
- Cryptographic hardware issued to Subscribers shall FIPS 140-2 Level 2 compliant.
- Multi-person control of CA private key shall be achieved using an "m-of-n" split key knowledge scheme.
- The CA signing keys shall be backed up under the same multi-person (m of n) control as the original signature keys.
- The CAs shall implement System Security Technical controls and set up procedures according to appropriate standards (e.g. BS ISO/IEC 17799:2005 or similar).
- According to the RFC 3280 the Key Identifiers used for CA Certificates shall comply to first option provided and should be as suggested below:
(1) The keyIdentifier is 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).
- The following algorithms and key lengths are recommended under the Saudi PKI framework:
 - Symmetric Key - triple-DES or AES (minimum 128 bit key strength)
 - Hashing Algorithms - Secure Hash Algorithm version 1 (SHA-1)
 - Asymmetric Key - RSA
 - Minimum Public Key sizes
 - CSP CA Key Pair 2048 bits
 - Subordinate CA Key pair 2048 bits
 - Subscriber Key Pairs 1024 bits
 - OCSP Key Pair 2048 bits
- The maximum certificate lifetime shall be :
 - CSP CA Signing Certificate - 120 months
 - Subordinate CA signing Certificate - 84 months

- End Entity signing Certificate - 36 months
- End Entity Encryption Certificate - 36 months

9 Certificate, CRL, and OCSP Profiles

This section will define X.509 certificate and CRL format including profile information, versions and extensions used.

- CA's shall be able to issue, update and sign CRLs as per RFC 3280. The CRL profile shall be compliant with X.509 CRL v2 profile and X.509 v3 CRL extensions which is specified by RFC 3280. OCSP requests and responses shall be in accordance with RFC 2560.
- The CA shall support complete certificate life cycle management comprise of following functions:
 - The Initialization is composed of the following functions: registration, key pair generation, certificate creation, certificate publication, and key/certificate delivery.
 - The Operation services can be summarized as following: Certificate Retrieval, Certificate Validation, Key Recovery, key/certificates Update/Renewal, Key History, and Key Escrow.
 - The termination service is composed of the following functions: Certificate Expiration, Certificates Suspension and Certificate Revocation

10 Compliance Audit and Other Assessments

This section will cover frequency of the compliance audit or other assessment, auditor qualification, auditor relationship with the entity being audited, scope of the audit and action taken on the deficiencies found during the audit.

- CAs shall be subjected to periodic compliance audits which are no less frequent than twelve months. However the NPA reserves right to conduct ad-hoc compliance audits of CAs operations.
- The compliance audits will verify whether the CA PKI operations environment is in compliance with the applicable CP, CPS and supporting operational policies and procedures. The term CA PKI Operations environment defines the total environment and includes, but is not limited to
 - 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),
- software and information.
- The CSP or an entity designated by it shall have the right to carry out annual as well as periodic audits and investigations in accordance with the contractual agreement, of the records, operations and services provision of the RA. The RA is also required in its contract with any LRA's and any relevant outsourced services, to provide equivalent access to auditors and investigators representing the CSP.
- The chosen auditor will be an independent third party and aside from the audit function, 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.
- An Audit Compliance Report, including identification of corrective measures taken or being taken by the audited party, shall be provided to the respective PA.

11 Other Business and Legal Matters

This section covers general business and legal matters. The subsections will cover provision relating to the fees charges by the CA and repositories for the various services provided and financial responsibility of the participants.

- The CAs shall cover the fees for the services and refund policy.
- The CAs shall cover provisions relating to Governing law, Severability, merger, survival and dispute resolution.
- The CA shall cover the confidentiality of business requirements in the Privacy Policy and the applicable agreements.
- The CA shall cover provisions regarding apportionment of liability for each type of entity, Insurance coverage ,warranties and limitation of warranties
- The CA shall describe the financial responsibilities of CA and repository