



Subject	Specification
Project Name	Appointment of the Service Provider to implement a modernised Trust Centre.
Reference	RFP22/23/42/Modernised Trust Centre PKI/MM

Contents

1	INTRODUCTION	1
1.1	Background.....	1
1.2	Terminology	1
2	OBJECTIVE	2
3	PROPOSED BUSINESS PROCESS.....	2
3.1	Customer Registration	2
3.2	Key Activation Process	2
3.3	Key Re-issue Process.....	2
4	BIDDER SCOPE OF WORK	2
4.1	Cloud Hosting Facility	3
4.2	PKI Software Configuration, Implementation and Support.....	3
4.2.1	Installation.....	3
4.2.2	Maintenance and Support.....	3
4.2.3	Reporting	3
4.2.4	Data Ownership and Management	3
4.2.5	Training.....	4
4.2.6	Integration.....	4
4.2.7	Handover	4
4.3	Compliance.....	4
4.4	Audit.....	4
5	FUNCTIONAL SPECIFICATIONS.....	5
5.1	User Interface	5
5.1.1	Customer Interface	5
5.1.2	User Interface	5
5.1.3	Administrator Interface.....	5
5.2	SAPO Customer Functionality	5
5.2.1	Digital Certificate Request	5
5.2.2	Documentation Submission	5
5.2.3	Validity Checks	5
5.3	Accredited Registration Authorities Functionality	5
5.3.1	Online Verification.....	5
5.3.2	Document Capture.....	5
5.3.3	Certificate Verification	5
5.4	Certification/Issuing Authority (CA) Functionality	6
5.4.1	Application Approval	6
5.4.2	Digital Certificates Creation	6
5.4.3	Digital Certificate Signing.....	6
5.4.4	Digital Certificate Revocation.....	6
5.4.5	Digital Certificate Verification	6
5.4.6	Digital Certificate Lifecycle Management	6
5.4.7	Key Recovery	6
5.5	Validation Authority	6
5.5.1	Certificate Validation	6

5.6	Certificate Use Cases	6
5.7	Trust Centre Security	7
5.7.1	Physical Security.....	7
5.7.2	Network Segmentation.....	7
5.7.3	Environment Lockdown.....	7
5.7.4	Access Control.....	7
5.8	Types of certificates	7
5.9	Integration.....	7
5.10	Protocols.....	8
5.11	Hierarchy	8

1 Introduction

The South African Post Office (SAPO) is a State Owned Company that offers a national Public Key Infrastructure (PKI) facility known as the Trust Centre. The Trust Centre provides citizens and corporate entities with encryption services to secure digital transactions through digital identity and authentication products and services to meet business and security requirements. The SA Post Office Trust Centre technology is the first South African-developed PKI platform that has been accredited by the South African Accreditation Authority (SAAA) as per the Electronic Communications and Transaction Act of 2002 as a Preferred Authentication Service Provider.

SAPO, in terms of this accreditation, is designated as a Certification Authority (CA).

1.1 Background

SAPO seeks to appoint a service provider to implement a modernised trust centre to be hosted in the Cloud within the borders of the country for a period of 5 years.

1.2 Terminology

Terminology	Description
PKI	Public Key Infrastructure
CA	Certificate Authority
RA	Registration Authority
VA	Validation Authority
HSM	Hardware Security Module
CRL	Certificate Revocation List
OCSP	Online Certificate Status Protocol, RFC2560
CMP	Certificate Management Protocol, RFC4210
SCEP	Simple Certificate Enrolment Protocol
Subscriber	The person or customer in whose name the Electronic Signature Certificate is issued
RTO	Recovery Time Objective
RPO	Recovery Point Objective
Trust Centre / PKI	Trust centre is the name given to the operation managing the PKI.

2 Objective

The appointed service provider shall provide a cloud based PKI service inclusive of the supply, installation, setup, configuration, integration, training and support on a negotiable revenue split basis for a period of five (5) years.

The project shall be self-funded therefore SAPO shall not incur any costs in the provisioning of the solution. The suppliers pricing shall include all the expenditure for the provisioning of a cloud based PKI services.

3 Proposed Business Process

The following diagram depicts the business process that are supported by the proposed PKI solution:

3.1 Customer Registration

The customer registration process is triggered by a request for a customer seeking a digital certificate. The customer submits documentation that is required to identify the customer/entity. The documents are then captured in the system and the customer is identified by the personnel involved in the provision of the services.

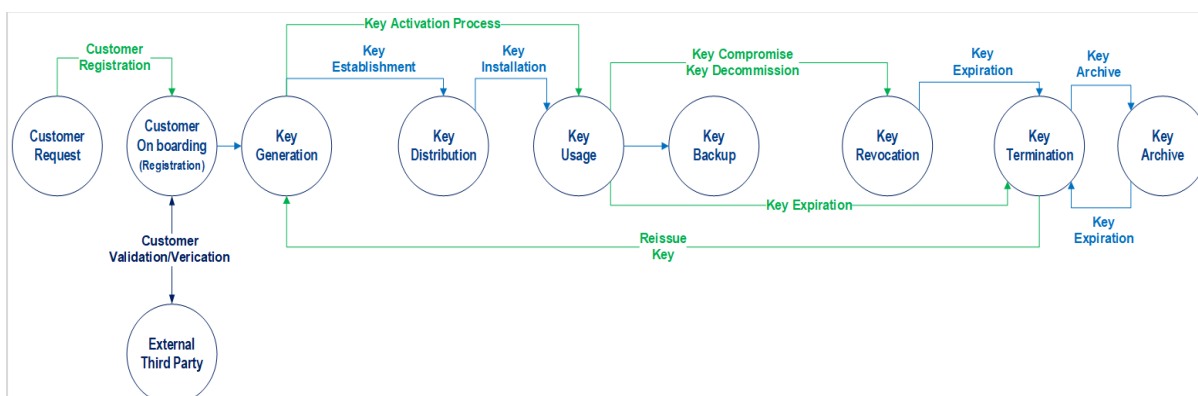
3.2 Key Activation Process

The key activation process is triggered by a completion of the customer registration process. The Trust Centre personnel will generate the key, link the key to the customer data, distribute the key for installation.

3.3 Key Re-issue Process

The key re-issue process is triggered when the customer request a key after the expiration of the key. The following sub-processes are executed:

- Key generation
- Key distribution
- Key Installation



4 Bidder Scope of Work

The South Africa Post Office is looking for a service provider that is going to provide the trust centre services that will comply with the web-trust compliance standards and be in

the position to provide an environment enabling SAPO to issue the digital certificates as follows:

4.1 Cloud Hosting Facility

- Provide a Software as a Service (SaaS) offering required for the Trust centre that will provide minimum hardware and software required to host Trust Centre services that are compliant with relevant WebTrust Principles and Criteria for Certification Authorities as published by the Chartered Professional Accountants of Canada.
- Proposed solution shall include the primary and testing environments.
- In the proposed solution, the primary and disaster recovery environments shall operate on an Active-Active basis.
- The solution shall subscribe to a Recovery Time Objective (RTO) of 2 hours for business continuity and maintain a 99.9% up time.
- Provide the necessary backup services required.
- The proposed PKI solution shall be hosted within the borders of the Republic of South Africa.
- The proposed PKI solution shall be hosted in a facility that complies with the relevant WebTrust Principles and Criteria for Certification Authorities.
- The appointed service provider should provide a 3 months project implementation plan.

4.2 PKI Software Configuration, Implementation and Support

4.2.1 Installation

Supply, installation and commissioning of all required hardware and software for the implementation of a working PKI solution.

4.2.2 Maintenance and Support

Maintenance and support of the implemented Public Key Infrastructure solution to meet the required operational SLA for a period of five years.

4.2.3 Reporting

Developing and providing reporting to meet the required operational SLA for a period of five years.

4.2.4 Data Ownership and Management

Customer data and data related to digital certificates will remain the property of SAPO and is to be handed over in the requested format as and when required by SAPO. The service provider shall:

- Store SAPO data in an industry standard format.

-
- Maintain real time replication link between the primary and disaster recovery sites.
 - Incorporate existing certification data into the new solution.

4.2.5 Training

The service provider shall provide SAPO employees with the required training to operate the software provided as well as any training related to updates during the agreement lifetime.

4.2.6 Integration

- Configure integration with identified SAPO systems as per integration specification documents that will be supplied at implementation stage.
- Integration of existing certification data.
- Configure integration to the Department of Home Affairs National Identification System (HANIS) web service.

4.2.7 Handover

- Hand over all data and backups to SAPO at termination of the agreement.
- The solution provider shall not retain any copies of the data belonging to SAPO.

4.3 Compliance

- The Trust Centre shall comply with the ISO 21188 standard.
- The Trust Centre shall comply with the Electronic Communications and Transaction Act of 2002.
- The Trust Centre shall comply with the Protection of Personal Information Act of 2013.
- The Trust Centre shall comply with the relevant WebTrust Principles and Criteria for Certification Authorities

4.4 Audit

- The service provider shall allow SAPO Internal Auditors to audit the Trust Centre on an ongoing annual basis.
- The service provider shall permit external independent auditors accredited by SAAA to conduct an annual compliance audit in the Trust centre.
- The service provider shall provide proof of corrective actions taken with regard to the audit findings that are relevant to the service provider.
- Key ceremonies shall be required as and when recommended by the auditors, therefore the service provider shall permit SAPO and external auditors to participate in the key ceremony in the Trust centre.

5 Functional Specifications

5.1 User Interface

5.1.1 Customer Interface

The proposed PKI solution shall provide a customer interface that enables subscribers/customers to access various customer related functionality.

5.1.2 User Interface

The proposed PKI solution shall provide a user interface that permits SAPO employees to access various functionality related to the management of the full life cycle of the certificate.

5.1.3 Administrator Interface

The proposed PKI solution shall provide an administrator interface that permits system administrators to access various functionality related to the monitoring and management of the PKI solution.

5.2 SAPO Customer Functionality

5.2.1 Digital Certificate Request

The proposed PKI solution shall accept requests for digital certificates via the SAPO e-commerce website.

5.2.2 Documentation Submission

The proposed PKI solution shall permit potential subscribers/customers to submit the required documentation online where allowed by the Web Trust regulations.

5.2.3 Validity Checks

The proposed PKI solution shall permit customers to verify the validity of their digital certificates.

5.3 Accredited Registration Authorities Functionality

5.3.1 Online Verification

The proposed PKI solution shall permit SAPO to verify the identity of potential customers using online verification methods.

5.3.2 Document Capture

The proposed PKI solution shall provide Accredited Registration Authorities (RA) to capture mandatory documents related to applications for digital certificates.

5.3.3 Certificate Verification

The proposed PKI solution shall provide Accredited Registration Authorities the ability to verify the authenticity of digital certificates as and when required to do so.

5.4 Certification/Issuing Authority (CA) Functionality

5.4.1 Application Approval

The proposed PKI solution shall permit SAPO to approve the issuing of digital certificates after the verification process has been completed.

5.4.2 Digital Certificates Creation

The proposed PKI solution shall enable SAPO to issue digital certification to customers who have requested such digital certificates.

5.4.3 Digital Certificate Signing

The proposed PKI solution shall enable SAPO to digitally sign the digital certificate.

5.4.4 Digital Certificate Revocation

The proposed PKI solution shall enable SAPO to maintain Certificate Revocation Lists (CRL).

5.4.5 Digital Certificate Verification

The proposed PKI solution shall enable SAPO employees to verify the authenticity of digital certificates as and when requested to do so.

5.4.6 Digital Certificate Lifecycle Management

The proposed PKI solution shall enable SAPO to manage digital certificate through the complete life cycle, from registration up to and including revocation or expiration.

5.4.7 Key Recovery

The proposed PKI solution shall provide SAPO with the capability to recover keys.

5.5 Validation Authority

5.5.1 Certificate Validation

The proposed PKI solution shall provide the Validation Authority (VA) with the capability to verify the validity of digital certificates as per X.509 and Request for Comment (RFC) 5280 standard.

The proposed PKI solution shall have the capability to access the CRL information hosted by the CA.

5.6 Certificate Use Cases

The proposed PKI solution shall enable SAPO to issue digital certificates that can be used for, but not limited to, the following use cases:

- Message encryption,
- website identity,
- code signing,

-
- authentication of servers, organisations and individuals,
 - email signing,
 - document signing,
 - commissioner of oaths
 - secured digital post-box
 - electronic stamps
 - electronic registered mail
 - device certificates for Internet of Things etc.

5.7 Trust Centre Security

5.7.1 Physical Security

The physical security of the hosting site shall comply with the specifications set out in the SAAA, WebTrust Principles and Criteria for Certification Authorities.

5.7.2 Network Segmentation

The Trust centre's local area network (LAN) that hosts the PKI service shall be physically and logically segmented from the service provider's data centre network and shall not interface with any other service that is hosted in the data centre according to the WebTrust compliance standard.

5.7.3 Environment Lockdown

The PKI environment shall be locked down after installation with only SAPO employees having logical and physical access to the Trust Centre.

Any hardware and software changes by the service provider shall follow SAPO change request control process and will be done under SAPO supervision.

5.7.4 Access Control

The access control mechanism of the Trust centre shall be physically separated from the service provider's access control mechanism.

5.8 Types of certificates

The proposed PKI solution shall enable SAPO to provide the following hierarchy of certificates:

- Root certificates,
- Intermediate certificate,
- Leaf certificate or end-entity certificates.

5.9 Integration

- The proposed PKI solution shall integrate with various Hardware Security module appliances and applications.

-
- The proposed PKI solution shall expose a standard set of Application Programming Interfaces (API) to facilitate data sharing.
 - The proposed PKI solution shall expose a standard set of APIs to enable extensibility of the functionality of the solution.

5.10 Protocols

The proposed PKI solution shall comply with the following communications and related protocols:

- Online Certificate Status Protocol, **RFC 6960** (OCSP)
- Certificate Management Protocol, **RFC 4210** (CMP)
- Simple Certificate Enrolment Protocol (SCEP)

5.11 Hierarchy

The proposed PKI solution shall provide the capability to create a hierarchy that includes Root CA, Sub-Ordinate CA, RA, and VA.