Standard Bank Root CA CPS

Public Key Operations

Standard Bank of South Africa

Standard Bank

Inspired. Motivated. Involved.

The information contained in this document represents the current view of Standard Bank on the Public Key Operations as of the date of publication. Because Standard Bank must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Standard Bank, and Standard Bank cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Standard Bank MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Disclaimer:

The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, places, or events is intended or should be inferred.

The information contained in this document represents a Guideline to implement Public Key Operations in Standard Bank

Root CA CPS, Public Key Operations, Version 3.1 Release

Based on	*RFC 3647 Certificate Policy and Certificate Practices Framework, Chokhani and Ford, November 2003*
Prepared by	**Moris Halevi**
	Wednesday, 2 January 2019 - 8:27:40 AM

Revision and Signoff Sheet

Change Record

Date	Author	Version	Change reference
4th August 2006	Moris Halevi	1.1	Document converted to Standard Bank Design
22nd August 2006	Moris Halevi	1.2	Standard Format & Typo corrections
1st September 2006	Moris Halevi	1.4	Final Draft
5th October 2006	Moris Halevi	1.6	Updates for compliance with WEBTRUST & RFC 2527 Framework
9th October 2006	Moris Halevi	2.0	Final Draft Initial Release
13th October 2006	Moris Halevi	2.1	Final Draft Corrections for recommendations 1.3
21st April 2015	Moris Halevi	3.0	Removed Confidential & Minor Corrections
10th December 2017	Londani Mulaudzi	3.1	Removed WEBTRUST Reference, CA version infrastructure update and update for RFC 3647
02nd January 2019	Londani Mulaudzi	3.1	Remove confidential information

Reviewers

Name	Version approved	Position	Date
Londani Mulaudzi	3.0	Specialist: Cryptography	28 April 2017
Zukiswa Mahlawe	3.1	Specialist: Cryptography	09th January 2018

Table of Contents

Tables

x

1 INTRODUCTION

1.1 Overview

The main goal of the Standard Bank Root Certification Authority is to offer a common “Trust Anchor” for all PKO initiatives within the Standard Bank group. The Standard Bank certification services will be designed to support security services to satisfy the business needs for digital signatures and other security services for its employees, partners, supplies and clients. The Standard Bank certification services will be offered to its employees, partners, supplies and clients by means of a hierarchical set of Policy CA’s, which each will fulfil the requirements of its particular community.

Each Policy CA will operate under the Root CPS. Before a Policy CA can participate in the Standard Bank PKO, the Standard Bank PKO Authority will review and approve its CPS to ensure that a minimal level of trust is maintained within the Standard Bank PKO. An overview of the current hierarchy can be found in section 1.3

This Certification Practice Statement (CPS) describes the practices of the Standard Bank Root Certification Authority in issuing and managing digital certificates for its Policy CA’s.

The purposes of this document are to:

1. Provide evidence of the trustworthiness of the Standard Bank Root CA as “Trust Anchor” within the Standard Bank PKO hierarchy, including the technology, operational processes and physical infrastructure.
2. Describe how the Standard Bank Root CA meets the requirements of each Certificate Policies under which certificates are issued to the different Policy CA’s entities in the Standard Bank PKO.
3. Set out the minimal requirements for its Policy CA’s for the management and administrative practices used to protect the trustworthiness of the Policy CA and the whole Standard Bank PKO.
4. Act as an input to audit activities. One audit activity is to validate that the Root CA is operated in accordance with the practices described in this document. A second audit activity is to determine, given the purposes for which certificates are used (as described in the Certificate Policy documents), that the practices in this CPS are sufficient to effectively manage security risks.

The structure of this CPS is based on the Internet X.509 Public Key Infrastructure Certificate policy and Certification Practices Framework [RFC3647]. For consistency with that document’s format, as well as for adaptability, all sections of the framework are included, with appropriate section headings. When no stipulation has been made for a section with regard to this CPS, "No Stipulation" is indicated below the related section heading.

1.2 IDENTIFICATION

The ROOT CA issues certificates in accordance with this CPS dated “2019-01-02”, that certifies the Standard Bank Policy CA’s and establishes the ***“TRUST Anchor for”*** Standard Bank.

CPS Name: Standard Bank Root CA Certificate Practice Statement OID: 1.3.6.1.4.1.16543.401.1.2.2.1

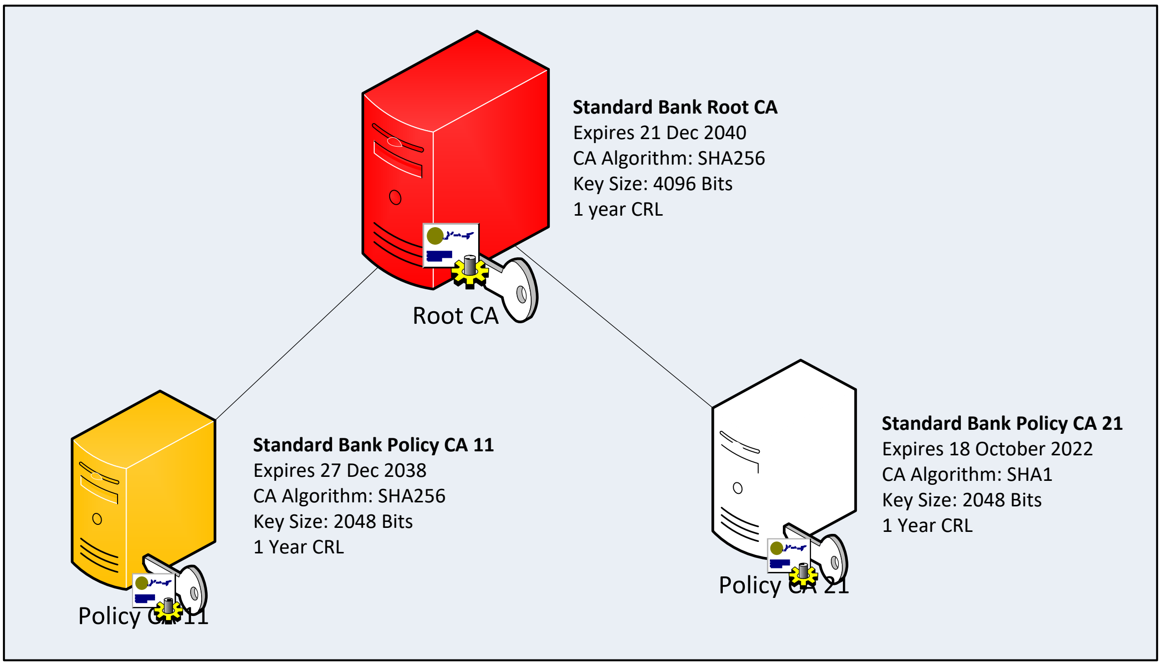
The following parts compose the OID:

ISO assigned	1
Organization acknowledged by ISO	3
US Department of Defence	6
Internet	1
Private	4
IANA registered private enterprise	1
Standard Bank	16543
Production environment	401
Root CA	1
CPS	2
Version	2.1

Table 1 – Standard Bank PKO ROOT CA CPS OID

1.3 COMMUNITY AND APPLICABILITY

A high level diagram of the Standard Bank PKO is shown below.



Standard Bank Root CA
Expires 21 Dec 2040
CA Algorithm: SHA256
Key Size: 4096 Bits
1 year CRL

Standard Bank Policy CA 11
Expires 27 Dec 2038
CA Algorithm: SHA256
Key Size: 2048 Bits
1 Year CRL

Standard Bank Policy CA 21
Expires 18 October 2022
CA Algorithm: SHA1
Key Size: 2048 Bits
1 Year CRL

Table 2 – Standard Bank PKO High-Level Architecture

1.3.1.1 Certification authorities

The purpose of a Certification Authority (CA) is to attest to the binding between an entity and a public key. Although this CPS is only applicable to the Root CA the description of its Policy CA is included for better understanding of this CPS.

1.3.1.2 Root Certification Authority (RCA)

The Root CA is the highest point of trust within the PKO hierarchy. It acts as the ‘Trust Anchor’ in the PKO – it is directly trusted by all parties that use the PKO. In order to trust the Root CA, a party requires the Root CA’s self-signed certificate, which must be obtained from a trusted source. All other entities in the PKO may be trusted by establishing a trust chain (a chain of digital certificates extending from the Root CA)

The primary purpose of the Root CA is to certify Policy Certification Authorities (PCA), by digitally signing their Certificates. The Root CA may also cross-certify with other trust providers, as business needs dictate. The establishment of such cross-certification relationships is under the control of the Standard Bank PKO Authority.

The Root CA is kept off-line and the Root CA's private key is generated and used in a tamper-proof hardware security module. When not in use the Root CA’s private key is split in pieces and stored in safes at a different location

1.3.1.3 Policy Certification Authorities (PCA)

In the current implementation there are 2 types of Policy CA’s, which are all Policies of the Root CA. They are described below:

1 **Internal Policy CA *“PCA 1x”*:** This(these) PCA(s) certifies the Standard Bank internal use Issuing CA’s which in turn certify employees, and Standard Bank owned entities. The policy allows implementation of multiple internal PCA’s should there be a need for grouping Issuing CA’s at Bank BU or Country.

2 **Internal Policy CA “PCA 2x”:** T This(these) PCA(s) certifies the Standard Bank external use Issuing CA’s which in turn certify Standard Bank Clients, Business Partners and where needed Standard Bank Business Units that need to provide secure communications and authenticated message delivery between the Business Units and their clients

Each of the Policy CA’s is certified by the Root CA to perform certain certificate services in a prescribed manner. The Standard Bank Root CA Certificate Policies and Policy CA certification agreements ensure that the Policy CA agrees to execute practices, including the issuance and management of certificates, in a manner that will maintain the level of trust required within the Standard Bank PKO.

1.3.1.4 Registration authorities

The primary purpose of a RA is to register End Entities, on behalf of its parent CA. The registration of Policy CA’s is a complex but manual process executed under scrutiny of an independent observer, therefore Standard Bank Root CA will not deploy a RA.

Each RA within the Standard Bank PKO hierarchy is Policy to a nominated CA; this is a function of the operating hierarchy. The practices used for registration and certification of End Entities are documented in the CPS of the Policy CA. That CPS must be approved by the Standard Bank PKO Authority prior to the certification of the Policy CA

1.3.1.5 End entities

The Standard Bank Root CA will only certify Policy CA’s; there are no End Entities. The Root CA may issue certificates to the operational staff of the Policy CA’s for strong authentication, since these certificates are not usable outside the Root CA environment they are not considered as End-Entities certificates.

1.3.1.6 Relying Parties

The Relying Parties in the scope of this CPS are parties which relies on the Root CA certificate, the certificates issued to the Policy CA’s, including the certificate status and the repository.

1.3.1.7 Applicability

Certificate Policies that are applicable to the practices described in this document are listed at Appendix A.

All Certificates issued by the Standard Bank Root CA are supported by this CPS. The Certificate Policies supported by the Standard Bank Root CA and covered by this CPS identify the suitable uses for those Certificates.

This CPS is not intended to support the use of Certificates which are issued by a CA outside the hierarchy of

CA’s described in section 1.3.1.1 of this CPS.

1.3.2 Suitable Applications

- Certification of Policy CA’s
- Being the Source and Anchor of Standard Bank TRUST Hierarchy.

1.3.2.1 Restricted Applications

No stipulation

1.3.2.2 Prohibited Applications

Standard Bank Root certification services and all other certification services within the Standard Bank PKO are not intended, designed, or authorised for use beyond the financial industry interface and processes.

1.4 CONTACT DETAILS

1.4.1 Specification administration organization

This CPS is administered by the Standard Bank PKO Authority. The PKO Authority’s responsibilities are to:

- Instigate drafting of policies for new trust entities entering the PKO.
- Ensure that existing policies are effectively maintained and implemented.
- Review and approve all policies within the scope of the PKO.
- Endorse the operations and processes undertaken in support of the policies approved by the PKO Authority.
- Ensure that policies are published to the appropriate community of interest.

1.4.2 Contact person

Questions concerning this CPS should be addressed to:

IT Security Public Key Operation Services
Standard Bank
5 Simmonds St
2000 Marshalltown
South Africa

E-mail: info.PKO@StandardBank.co.za, KeyManagementTeam@StandardBank.co.za
Phone: +27 (0) 11 636 9111 (switchboard)

1.4.3 Person determining CPS suitability for the policy

Same as 1.4.2

2 GENERAL PROVISIONS

This section contains provisions relating to the respective obligations of Root CA and Policy CA’s and relying parties, and other issues pertaining to law and dispute resolution.

2.1 OBLIGATIONS

The Standard Bank Root CA will operate in a contractually closed environment. Therefore contractual agreements will be in place between all Policy CA’s and the ROOT CA in the Standard Bank PKO.

2.1.1 CA obligations

2.1.1.1 Root CA Obligations

The Root CA meets its obligations under this CPS by:

1 Adhering to the practices described within this CPS.
2 Publishing its self-signed CA Certificate for relying parties.
3 Maintain records required demonstrating trustworthy operations and compliance with this CPS.
4 Issuing Certificates to authorised Policy CA’s, that comply with X.509 standards and are suitable for the purpose required.
5 Publishing issued Certificates in a nominated directory.
6 Ensuring that Certificates it issues are factually correct from the information known to it at the time of issue, and that are free from data entry errors.
7 Provide revocation status services for Policy CA certificates and publishing Certificate status information in a CRL to a nominated directory.
8 Publish updates to this CPS and applicable CP as soon as a new version is available.

2.1.1.2 Policy CA Obligations

Policy CA’s operating under the Root CA fulfils their obligations under this CPS by:

As a subscriber:

1 Comply with the practices and obligations set out in this CPS
2 Provide the required proofs to meet registration or Certificate renewal requirements as defined in the relevant CP.
3 Requesting acceptance of a self-generated key-pair.
4 Prove possession of and the right to use the self-generated key-pair.
5 Immediately notifying the Root CA of any error or defect in the Certificate or of any subsequent changes in the information detailed in the Certificate.
6 Reading the applicable CP and if required this CPS before using the key pair.
7 Using the key pair only in accordance with the relevant CP.
8 Ensuring the security and integrity of the private key, including:
9 Controlling access to the Hardware Security Module holding the private key
10 Protecting Pin’s and Pass-phrases used to access the private key
11 Immediately notifying the Root CA of any instance in which a key pair is compromised or in which they have reason to believe a key pair may have become compromised.
12 Agree to be bound by the provisions of limitations of liability as described in section 2.2 of this CPS

As a Policy CA:

1 Publish a CPS detailing its practices.
2 Ensuring that Certificates it issues are factually correct from the information known to it at the time of issue, and that are free from data entry errors.
3 Publishing issued Certificates in a nominated directory.
4 Provide revocation status services for certificates it issues and publishing Certificate status information in a CRL to a nominated directory.

2.1.2 RA obligations

No stipulation. ROOT CA does not depend or implement RA for signing subordinate Policy CA's

2.1.3 Subscriber obligations

The subscriber of Root CA certificate services is the Policy CA see 2.1.1

2.1.4 Relying party obligations

Relying Parties fulfil their obligations under this CPS by:

1 Obtaining a trustworthy copy of the Root CA's self-signed certificate.
   - Exercising reasonable judgement before deciding to rely on a certificate based service, as well as:
     - Performing a Certificate Path Validation
     - Obtaining Certificate revocation status using a CRL
     - Only trusting and relying on a Certificate that has not expired, or been revoked or been suspended and if a proper chain of trust can be established.

2 Agree to be bound by the provisions of limitations of liability as described in section 2.2 of this CPS.

2.1.5 Repository Obligations

The Repository, as managed by the CA, shall:

- Publish and maintain certificate information
- Publish the CPS, the applicable CP's and the CRL
- Use its best efforts to keep the Repository available 24 hours per day, 7 days a week
- Update the CPS as soon as a new version becomes available

2.2 LIABILITY

2.2.1 Warranties and Limitations on Warranties

The Standard Bank Root CA warrants and promises to:

- Provide certification and repository services consistent with the relevant Certificate Policies and with this CPS
- Perform authentication and identification procedures in accordance with the relevant Certificate Policies and within section 3 of this CPS
- Provide key management services including Certificate issuance, publication and revocation in accordance with the relevant Certificate Policies and with the CPS

The Standard Bank Root CA make no other warranties or promises and have no further obligations to Policy CA's or Relying Parties, except as set forth under this CPS.

2.2.2 Disclaimers

Except for express warranties stated in this CPS, Standard Bank Root CA disclaims all other warranties, promises and other obligations.

In no event shall Standard Bank Root CA be liable for any indirect, consequential, incidental, special or punitive damages, or for any loss of profits, loss of data, or other indirect or consequential damages arising from or in connection with the use, delivery, license, availability or non-availability, performance or non-performance of Certificates, digital signatures, the repository, or any other transactions or services offered or contemplated by this CPS, even if Standard Bank Root CA has been advised of the possibility of such damages.

2.2.3 Loss Limitations

This issue will be handled in the Subscriber Agreements stipulating the terms and conditions of the Policy CA.

2.2.4 Other exclusions

Standard Bank Root CA is not liable for any loss:

- Due to war, natural disasters or other uncontrollable forces
- Due to unauthorised use of Certificates issued by Standard Bank Root CA
- Use of Certificates beyond the prescribed use defined by the relevant Certificate Policy and this CPS
- Arising from the negligent or fraudulent use of Certificates or CRL's issued by Standard Bank Root CA
- Arising from any use of Certificates and CRL's issued by Policy CA's
- Due to disclosure or use of information in the Certificate and CRL

2.3 FINANCIAL RESPONSIBILITY

2.3.1 Indemnification by relying parties

Standard Bank Root CA assumes no financial responsibility for improperly used certificates

2.3.2 Fiduciary relationships

Issuance of certificates in accordance with this CPS does not make the Root CA an agent, fiduciary, trustee, or other representative of the Policy CA or relying parties.

2.3.3 Administrative processes

No stipulation.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 Governing law

South African laws shall govern the enforceability, construction, interpretation and validity of this CPS and related CP's.

2.4.2 Severability, survival, merger, notice

Standard Bank shall ensure the continuity and stability of the Standard Bank Root CA.

If any provision of this CPS is found to be unenforceable, the remaining provisions are interpreted to best carry out the reasonable intent of the parties.

This CPS is interpreted consistently with what is commercially reasonable in good faith under the circumstances.

Severance or merger may result in changes to the scope, management and /or operations the ROOT CA. In such an event, this CPS will require modification to reflect those changes. Changes to the operations will be consistent with the ROOT CA's disclosed management processes and will be detailed in ROOT CA's Operations Guide accordingly.

2.4.3 Dispute resolution procedures

2.4.3.1 Hierarchy of Certificate Policy

When the subject of the dispute is between this CPS and:

1 A CP, the CP shall prevail.
2 A Policy CA agreement or statement of Policy CA obligations, the Policy CA agreement/obligation shall prevail.
3 Any other policy, procedure or any other operational or practices documentation whatsoever, this CPS shall prevail.

2.4.3.2 Process

In the event of any dispute involving services or provisions covered by this CPS, the aggrieved party shall first notify the Standard Bank PKO Authority and all other relevant parties regarding the dispute.

If the dispute cannot be resolved by negotiations it will be settled by arbitration or in South African court.

2.5 FEES

2.5.1 Certificate issuance or renewal fees

No fees will be charged for the issuance and use of the certificates issued under this CPS.

2.5.2 Certificate access fees

No stipulation

2.5.3 Revocation or status information access fees

No stipulation

2.5.4 Fees for other services such as policy information

No fees, other than those covering reasonable media reproduction and distribution costs, may be charged for supplying physical media copies of this CPS or for supplying physical copies of a certificate policy.

2.5.5 Refund policy

No stipulation.

2.6 PUBLICATION AND REPOSITORY

2.6.1 Publication of Root CA information

The following information will be made available in a repository to all parties that use Standard Bank Root CA services:

- This CPS
- The applicable CP’s under which certificates are issued
- Revocation status information for all issued certificates
- All Policy CA certificates

The Standard Bank Active Directory and WEB Site at URL https://PKO.StandardBank.co.za are the repository of the above information and they will be available all day 24/24 hours except in Case of force majeure. Standard Bank will make its best effort to limit the unavailability of the repository.

2.6.2 Frequency of publication

CPS and CP publication will be in accordance with section 8. Certificates will be published as soon as they are issued. Published CRL’s (Certificate Revocation Lists) shall have a finite validity period. Publication of a new CRL will be done before expiration of the subsequent CRL.

The lifetime of a CRL will be in accordance with section 4.4.9 of this CPS.

2.6.3 Access controls

Each certificate has a pointer to the relevant Certificate Policy. No access controls will be imposed on threading of these documents or on this CPS. Access controls on certificates or CRL’s will be based on the need to know need to have principle. There will be appropriate access controls controlling who can write or modify items in the repository.

2.6.4 Repositories

The CPS, CP’s, CRL, ROOT & Policy CA certificates are available at:

https://PKO.Standard Bank.co.za

2.7 COMPLIANCE AUDIT

The purpose of the audit is to verify the quality of the services provided by the Standard Bank Root CA, to verify if the Root CA complies with all the requirements of this CPS, and to verify if the CPS is consistent with the requirements of the supported Certificate Policies.

2.7.1 Frequency of entity compliance audit

The PKO Authority reserves the right to conduct a comprehensive compliance audit of the practices documented in this CPS:

- Within one year of the commencement of operations of the Root CA.
- At any other time that it deems warranted, and at least annually

The PA has the right to require audits on Policy CA’s in order to detect non-compliance with obligations imposed by this CPS the applicable CP or Policy CA agreements

The IT Security Officer of each entity (DBB, DBIL, and DCL) has the right to require periodic or non-periodic inspections and audits on the components and operations within their entity.

2.7.2 Identity/qualifications of auditor

The initial audit will be performed by an independent and reputable public auditor.

For later audits the auditing team will be assigned by the PA, and recruited from the security departments of Standard Bank.

The team will consist of members representing applications, infrastructures and policy/management activities.

2.7.3 Auditor's relationship to audited party

As stated in 2.7.2

2.7.4 Topics covered by audit

The topics covered by a compliance audit will include but nor be limited to:

- Security policy and planning
- Physical security
- Technology evaluation
- Procedural documentation
- CA service administration
- Personnel vetting
- Relevant CP and CPS
- Contracts
- Data protection and privacy considerations
- Business continuity planning documents

2.7.5 Actions taken as a result of deficiency

The decision regarding which actions to take will be based on previous response to problems, the severity of the irregularities, and the recommendations of the auditor. The forthcoming amendments/corrections will be implemented with sixty (60) days of formal notification.

2.7.6 Communication of results

Audit results are considered to be sensitive information and are therefore not available for external parties. The audit results will be distributed to the audited CA and the IT Security Officers.

2.8 CONFIDENTIALITY

2.8.1 Types of information to be kept confidential

Any personal or corporate information held by the Root CA that is not appearing on issued certificates is considered confidential and must not be released, unless required otherwise by law.

All private and secret keys used and handled within the Root CA operation under this policy are to be kept confidential.

Audit logs and records shall not be made available in their totality, except when required by law. Only records of individual transactions can be released according to section 4.6.6. In providing PKO services, Standard Bank complies with all relevant data protection legislation.

Access to confidential information by operational staff is on a need-to-know basis. Paper based documentation containing confidential information is kept in secure and locked containers or filing systems, separate from all other records.

2.8.2 Types of information not considered confidential

Information included in certificates and CRL's is not considered confidential.

2.8.3 Disclosure of certificate revocation/suspension information

When a certificate is revoked, a reason code will be included in the CRL entry. This reason code is not considered confidential (see 2.8.2), however no other details concerning the revocation are as a standard disclosed

When a certificate is suspended, no reason code will be included in the CRL entry.

2.8.4 Release to law enforcement officials

The Standard Bank CA shall comply with legal requirements to provide information to law enforcement officials. The evaluation of such requests and the decision to provide information is at the discretion of Standard Bank's legal department.

2.8.5 Release as part of civil discovery

No stipulation.

2.8.6 Disclosure upon owner's request

The subject of a registration record has full access to that record, and is empowered to authorize release of that record to another person.

No release of information is permitted without formal authorization. Formal authorization may take two forms:

- A digital signed e-mail.
- By application in writing.

2.8.7 Other information release circumstances

No stipulation.

2.9 INTELLECTUAL PROPERTY RIGHTS

The certificates issued through the Standard Bank PKO and all related documents, including the CP and this CPS, are the property of Standard Bank and are protected by intellectual property rights.

3 IDENTIFICATION AND AUTHENTICATION

This section contains the practices and procedures to be followed in identifying and authenticating Policy CA certificate request during a certification process.

3.1 INITIAL REGISTRATION

3.1.1 Types of names

All Certificates require a distinguished name that is in compliance with the X.500 standard for Distinguished Names.

Each Certificate Policy states requirements for naming of a Policy CA issued with certificates under that policy.

The Policy CA proposes and the PA approves the distinguished name.

3.1.2 Need for names to be meaningful

In all Cases, names of Policy CA’s must be meaningful. Generally the Common Name of a CA will indicate its community of interest.

3.1.3 Rules for interpreting various name forms

Guidance how naming information in certificates should be interpreted may be found in the Certificate Policy referenced by a certificate.

3.1.4 Uniqueness of names

The Root CA will assure uniqueness of all Policy CA’s distinguished names.

3.1.5 Name claim dispute resolution procedure

Any dispute regarding a Distinguished Name is resolved in terms of section 2.4.3 - Dispute resolution procedures

3.1.6 Recognition, authentication and role of trademarks in I&A

No stipulation

3.1.7 Method to prove possession of private key

The Policy CA’s generate and store their private key in FIPS 140-2 Level 3 certified Hardware Security Modules and perform a digital signature operation on the certificate request (self signed request). The Root CA verifies the signature with the public key listed in the request for certification.

3.1.8 Authentication of organization identity

This CPS supports only Policy CA’s operated only by Business Units of the Standard Bank entering the Standard Bank PKO. The authentication of the Standard Bank organisational unit, applying for a Policy CA Certificate, and their right to use the Standard Bank name in the certificate will be done during the review by the PA of the supplied documentation providing evidence of compliance with minimal Trust levels required by the PA.

3.1.9 Authentication of individual identity

There are no stipulations for the ROOT or Policy CA’s, while Issuing CA’s have detailed individual identity specifications.

3.2 ROUTINE REKEY

Policy CA's may request Certificate renewal (with re-key, i.e. change of key) provided that:

- The request is made prior to the expiry of their current Certificates.
- Material Certificate information as contained in registration records has not changed.
- Their current Certificates have not been revoked. Authentication of the request will be performed according section 3.1

3.3 REKEY AFTER REVOCATION

Re--key is not permitted after Certificate revocation.

3.4 REVOCATION REQUEST

A request to revoke a Certificate, if authenticated as being from the certificate holder, constitutes a valid and enforceable revocation request.

Parties other than the certificate holder may request revocation, but such parties must be reliably identified and authenticated before the certificate is revoked.

Possible Authentication mechanisms are:

- A signed e-mail
- A visit in person to the Root CA
- A application in writing

4 OPERATIONAL REQUIREMENTS

This section is used to specify the operating requirements upon entities involved in the certification and certificate revocation process.

4.1 CERTIFICATE APPLICATION

The Standard Bank organisational unit owning the Policy CA is responsible to create the following documents and submit them to the PA:

- A CPS describing its community and practices used
- The supported CP's
- A creation and configuration document describing the logical and physical security applied to the Policy CA (hardware and software components used and their configuration details, key generation, storage and backup, ...)

The PA will validate these documents to check if the Policy CA delivers the required level of trustworthiness. If this validation yields a satisfactory result the PA will send a subscriber agreement to the Policy CA

Upon receipt of the signed subscriber agreement the PA will settle a date on which the creation of the Policy CA can occur and appoint a member of the PA or a person performing a trusted Root CA role as a witness for the creation.

4.2 CERTIFICATE ISSUANCE

On the agreed date the person appointed by the PA will be present during the Policy CA creation ceremony and verify that the CA is created according to the validated documents.

The first phase of the creation ceremony will end with the creation of the Policy CA's private key and a self-signed certificate request.

The certificate request file will be stored in a tamperproof envelope containing the signatures of the ceremony master and the person appointed by the PA this until the issuance by the Root CA.

At the Root CA the certificate will be issued only if:

- The envelope does not have any sign of tamper and the signatures on the envelope can be verified.
- A successful verification of the self-signed request with the public key listed in the request can be done
- The content in the certificate request (DN, ...) is in accordance with the validated documents.

The issuance of a certificate by the Root CA indicates a complete and final approval of the certificate application by the Root CA.

The issued certificate will be handed over to the Policy CA administrator. The Root CA will wait with the publication of the issued certificate in the repository, until a confirmation of the successful completion of the Policy CA installation has been received.

4.3 CERTIFICATE ACCEPTANCE

Upon reception of the certificate the Policy CA will complete the second part of the creation ceremony. The Policy CA is responsible to check the correctness of the content of the certificate if any inconsistencies are found between the content in the certificate and the information submitted during certificate request he must inform the Root CA immediately.

After the successful ending of the ceremony all persons present will sign off the ceremony document, this constitutes a final acceptance of the certificate. The Root CA will be notified of the successful installation and a copy of the creation ceremony will be sent to the Root CA.

By accepting a certificate, the Policy CA agrees:

- to be bound by the continuing responsibilities, obligations and duties imposed on him by the subscriber agreement, the CP and this CPS
- no unauthorised person has ever had access to the Policy CA's private key.
- all information given by the Policy CA to the Root CA and included in the certificate is true

4.4 CERTIFICATE SUSPENSION AND REVOCATION

The Root CA is responsible for issuing and publishing CRL's. The Root CA shall update its CRL to reflect changes in revocation status and must issue timely CRL's.

4.4.1 Circumstances for revocation

Certificates will be revoked when any of the information in a certificate is known or suspected to be inaccurate or when the private key associated with the certificate is compromised or suspected to be compromised.

Examples are:

- An improper or faulty issue of a Certificate is discovered.
- Material Certificate information becomes inaccurate
- The Policy CA has no longer use for the certificate
- The Policy CA can be shown to have violated the stipulations of the CP, this CPS or the subscriber agreement
- An authenticated revocation request is received from the Policy CA
- A validated revocation request is received from a third party
- The Policy CA private key is suspected of compromise :
- Unauthorised access or suspected unauthorised access to the private key
- Lost or stolen key
- Destroyed key
- The Root CA private key is suspected of compromise

4.4.2 Who can request revocation

Certificate revocation can be requested by:

- The Administrator of Standard Bank PKO
- Persons performing trusted roles for the Policy CA
- The PA
- Any other party that has evidence that the circumstances described in section 4.4.1 have occurred.

4.4.3 Procedure for revocation request

Revocations are requested promptly after detection of a compromise or any other event giving cause for revocation.

The Policy CA must immediately notify the Root CA when a compromise investigation has been started.

A revocation request may be generated in the following ways:

- Electronically by a digitally signed message to the PA
- By a visit to the Root CA

In writing Authentication of the revocation request shall meet the requirements in 3.4 The Root A shall archive all revocation requests, the cause for revocation, the means of authenticating the request and the resulting actions taken by the Root CA. To process a revocation request:

1 The Root CA authenticates the revocation request
2 The Root CA makes the arrangements for the key-holders attendance
3 The Root CA revokes the Certificate.
4 The Root CA submits an updated CRL to the repository, including the revoked certificate.
5 The Root CA notifies the Policy CA of the date and time of revocation.

Independent of the circumstances prompting the request, approval or denial of the request and the actual revocation has to be done within a maximum period of 2 working days. The PolicyCA owning a revoked certificate must securely destroy all instances of the private key.

4.4.4 Revocation request grace period

No stipulation.

4.4.5 Circumstances for suspension

No stipulation.

4.4.6 Who can request suspension

No stipulation.

4.4.7 Procedure for suspension request

No stipulation.

4.4.8 Limits on suspension period

No stipulation.

4.4.9 CRL issuance frequency

The Root CA issues a CRL reporting the revocation status of Policy CA’s at intervals not exceeding 367 days. When the certificate of a Policy CA is revoked, the Root CA will immediately issue and publish a replacement CRL. The previous CRL will be deleted from the directory.

Policy CA’s will issue a CRL at intervals not exceeding 367 days. Typically the Policy CA’s will update the CRL every time a subordinate Issuing CA’s status changes

CA’s will ensure that a CRL is issued prior to the expiry of the previous CRL, to ensure that there is always a current available CRL, even in the event of delays in CRL’s propagating through to relying parties.

4.4.10 CRL checking requirements

Checking certificates for revocation is the responsibility of the relying party. The certified content of a certificate cannot be fully trusted unless the relying party follows proper revocation checking procedures as stated below.

- A relying party that downloads a CRL from a repository shall verify the authenticity of the CRL by checking its digital signature and the associated certification path.
- The relying party shall check the validity period of the CRL to make sure that the information in the CRL is up to date.
- The relying party is allowed to cache the CRL during its validity period, the decision whether to use a cached CRL or the latest CRL available is left to the relying party's discretion.
- Certificates may be stored locally on a relying party's system but, before use, each such certificate will be validated through a check on current revocation status.
- If no valid revocation checking information can be obtained, due to system failure or service, no certificates should be accepted. Any acceptance of a certificate without conformance to this requirement is done at the relying party’s own risk.

4.4.11 On-line revocation/status checking availability

No stipulation.

4.4.12 On-line revocation checking requirements

No stipulation.

4.4.13 Other forms of revocation advertisements available

No stipulation.

4.4.14 Checking requirements for other forms of revocation ads

No stipulation.

4.4.15 Special requirements regarding key compromise

No stipulation.

4.5 SECURITY AUDIT PROCEDURES

The security audit procedures in this section are valid for the Root CA system and software components which may affect the outcome of the certificate issuing processes and the CRL.

Cryptographic tokens used in the Root CA-system are not covered in this section. They are regulated separately in section 6.2.1.

4.5.1 Types of event recorded

The security audit functions related to the Root CA system shall log, for audit purposes:

- All physical access to Root CA Strong Room
- ROOT CA server start-up, shutdown and take-down
- ROOT CA application start-up & close-down
- Failures & Anomalies – Hardware & Application
- Attempts to create, remove, set passwords or change the system privileges of operational personnel for the ROOT CA Server and Physical Access Card/PIN to the strong room.
- Changes to CA details and/or keys
- Changes to certificate creation profiles
- Login and logoff attempts
- Unauthorised attempts to access system files
- Installation of new software or software updates
- All system events recorded as part of Windows process will be transferred in to permanent logs, that reflect date, time and details of the event
- Certificate lifecycle management-related events – described in Deployment & OP's Guides
  - Certificate Applications
  - Certificate Issuance
  - Certificate Renewal
  - Certificate Revocation
  - Certification Process, Steps & Results (issued, failed, rejected)
  - Certificate Revocation List Process, Steps & Results
- Key lifecycle management-related events – described in Deployment & OP's Guides
  - KeyPair Generation
  - KeyPair Backup
  - KeyPair Archival
  - KeyPair Recovery
  - KeyPair Storage
  - KeyPair Destruction
- Hardware Security Module management-related events – described in Deployment & OP's Guides
  - Initial Installation
  - Secure World definition & Admin Smart Card issuance
  - KeyPair Generation and Operation Smart Card Issuance
  - Take down process & steps

4.5.2 Frequency of processing audit log

The logs will be processed each time the CA system is removed from the safe and brought operational and analysed for evidence of unauthorised or inappropriate behaviour.

4.5.3 Retention period for audit log

Audit logs will be retained for the standard archival period as defined in 4.6.2

4.5.4 Protection of audit log

The CA application audit log, which contains all certificate lifecycle related events, will be digitally signed and time-stamped by the CA system. After signing, the audit log will only be open for read access and no longer for modification by whatever system or person, including the CA Administrator.

The configuration of the offline Root CA which includes CA application audit log, operating system generated logs and essential configuration files are written to CD-ROM before the Root CA is returned to its safe.

Audit logs will be verified and consolidated at least annually. At least two people in SA or ISSO roles will be present for such verification and consolidation.

4.5.5 Audit log backup procedures

Two copies of the consolidated logs will be made on a WORM media and stored in separate physically secured locations.

4.5.6 Audit collection system (internal vs. external)

No stipulation.

4.5.7 Notification to event-causing subject

No stipulation

4.5.8 Vulnerability assessments

No stipulation

4.6 RECORDS ARCHIVAL

4.6.1 Types of event recorded

The records shall include all relevant evidence in the Root CA's possession including:

- Configuration files of the Root CA system.
- Contents of issued certificates.
- Revocation requests and all recorded messages exchanged with the originator of the request.
- CRL's posted to the directory and other relevant revocation checking information released by the Root CA.
- Audit journals including records of auditing of CA's.
- Current and preceding implemented certificate policy documents and their related CPS.

Records may be kept in the form of either computer-based messages or paper-based documents, provided their indexing, storage, preservation, and reproduction are accurate and complete.

4.6.2 Retention period for archive

Archives will be retained and protected against modification or destruction for at least 30 years from the date of archival, unless applicable law or regulations require a longer period.

4.6.3 Protection of archive

No person, including the CA Administrator, is allowed to modify, manipulate or delete an archived record. To ensure continuity, archived records may be moved or copied to another medium. Under no circumstances shall the contents of the archive be released as a whole, except as required by law.

The CA will store all archival records in a secure storage facility

4.6.4 Archive backup procedures

Archive backup procedures are established to ensure and enable complete restoration of current service or verification in the event of a disaster situation.

Long term storage of records is accomplished on WORM media.

4.6.5 Requirements for time-stamping of records

All archive records contain the date and time of the audit event.

4.6.6 Archive collection system (internal or external)

Internal

4.6.7 Procedures to obtain and verify archive information

The Root CA shall act in compliance with requirements regarding confidentiality stated in 2.8

Records of individual transactions may be released upon request by any of the entities involved in the transaction.

On request, the Root CA shall make documentation available that demonstrates the Root CA's compliance with section 2.7 of this CPS.

The Root CA shall ensure availability of the archive and that archived information is stored in a readable format during its retention period.

4.7 KEY CHANGEOVER

The Standard Bank PKO will ensure continuity and disclose the Root CA key changeover procedures in the ***"ROOT CA Operations Guide"*** and the changes will be reflected in amendments of this CPS.

4.8 COMPROMISE AND DISASTER RECOVERY

4.8.1 Computing Resource, Software, and/or Data are Corrupted

In the event computing resources or software and/or data are corrupted the operation of the Root CA will be suspended and the Root CA will be reinstalled from original media and data will be restored from the last backup taken. The event will be recorded and the failure reason will be investigated and finding will be notified to PKO management and logged.

There is a detailed disaster recovery process. ***("see Deployment and Operations Guides for details")***.

Due to fact that the ROOT CA is an off-line CA (non network connected) and also switched off with components segregated, two level backup is taken of the CA each time the CA server is used and then taken-down. Furthermore every 12 month a health check is performed on the ROOT CA irrespective if the CA was used or not in the last 12 months. ***("see Physical Security Protocols in PKI Design document for details")***

PKO operations have the responsibility of bringing up the ROOT CA within 3 month from notice or disaster. In worst case scenario as stipulated in deployment guidelines ROOT CA can be re-build from scratch on newly ordered hardware. There is no need for redundant hardware.

DR scenario for ROOT CA entails re-start-up of the physical server from scratch as would be in the case of the initial commissioning of the ROOT CA and The HSM will be re-loaded from the Admin & Operator Smartcards. The process is detailed in ***("Deployment and Operations Guides")*** for the ROOT CA.

4.8.2 Entity Public Key is revoked

In the event of the need for revocation of the Root CA's public key, the CA must:

- immediately notify the PA
- Inform its Policy CA's.
- The Root certificate must be removed from all relying parties trust lists

The Root CA will be brought down and a new Root CA key generation process will occur. All the Certificates in the Trust Chain will have to be re-certified.

4.8.3 Entity Key is compromised

If an incident occurs resulting in the Root CA private key being compromised, the Root CA private key will be immediately revoked, after which the same steps as described in section 4.8.2. have to take place. In addition, the Root CA Administrator will thoroughly investigate the cause of the compromise. All certificates issued before the compromise are to be revoked and renewed in the shortest timeframe possible using the standard procedure

4.8.4 Secure facility after a Natural or Other Type of Disaster

Standard Bank has an alternative processing site; it has equivalent strength in physical and logical security as the primary processing facility. Such facility will be operational no more than 24 hours after the disaster.

4.9 CA TERMINATION

If it is decided by Standard Bank to terminate the Standard Bank PKO, all certificates will be revoked and are put on a final CRL. All material requirements in this CPS will survive CA termination, including but not limited to record archiving.

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

This section describes the physical, procedural, and personnel security controls required of the Root CA to protect their operations.

For detailed description of security architecture please refer to ***"Public Key Infrastructure Design"*** and for security access protocols please refer to ***"ROOT CA Deployment Guide".***

All the processes and protocols are also defined in specific worksheets that act as route maps to deploy then use the ROOT CA. These worksheets also serve as audit control map for the independent *(non-Bank employee)* observer to perform their task in each and every interaction with the ROOT CA.

5.1 PHYSICAL SECURITY CONTROLS

Physical security controls are implemented to control access to the Root CA's hardware, software, data and tokens.

The keys for signing certificates and CRL's are kept physically protected in such a way that they may never become exposed due to physical penetration.

The Standard Bank Root CA facility shall also have a place to store backup and distribution media in any manner sufficient to prevent loss, tampering, or unauthorised use of the stored information.

Backups are kept both for data recovery and for the archival of important information.

Backup media shall also be stored at a site different from where the CA system resides, to permit restoration in the event of a natural disaster to the primary facility.

5.1.1 Site location and construction

The site location of the Root CA and the Issuing CA's are in a secure location with physical security and access control procedures which meet or exceed financial industry standards.

5.1.2 Physical access

Only authorised personnel are granted physical access. The number of personnel authorised to enter the area is kept to a minimum and a log is maintained of all accesses.

Access to the safe storing the offline Root CA is limited to those personnel performing one of the roles described in Section 5.2.1

5.1.3 Power and air conditioning

The Standard Bank CA facility is equipped with a no-break power circuit and air conditioning systems to provide a suitable operating environment.

5.1.4 Water exposures

The Standard Bank CA facility has reasonable precautions taken to minimize the impact of water exposure.

5.1.5 Fire prevention and protection

Suitable fire notification & prevention infrastructure are maintained in the Standard Bank RiverClub Computer facility that implements, fire prevention methods which are designed to comply with local fire safety regulations and the Strong Room is an integral part of the RiverClub Computer Facility.

5.1.6 Media storage

All magnetic media containing PKO information, including backup media, are stored in containers, cabinets or safes with fire protection capabilities and are located either within the Standard Bank CA facility or its disaster facility.

5.1.7 Waste disposal

Paper documents, magnetic media or security tokens containing trusted elements of the PKO or commercially sensitive or confidential information are securely disposed of by:

1 In the case of magnetic media or security tokens:
   - physical damage to, or complete destruction of the asset
   - the use of an approved utility to wipe or overwrite magnetic media
   - tokens & smartcards are force erased

2 In the case of printed material, shredding, or destruction by an approved service.

3 In case equipment such as the server and hardware security module there is no need to destruct them, due to the fact that when powered off and taken-down to the same state that they were when received from the manufacturer, therefore they can be re-assigned.

5.1.8 Off-site backup

Offsite storage is used for the storage and retention of backup software and data. The offsite storage is referred as the cold storage and is managed under contract to Standard Bank, and it:

1 Is available to authorised personnel 24 hours per day seven days per week for the purpose of retrieving software and data;

2 Has an appropriate level of physical security in place.

5.1.9 Training

Due to the fact that probability of commissioning a new Issuing CA is very low and much lower in the case of a Policy CA, a health check is prescribed for all the OFFLINE & POWERED-OFF CA’s at least twice a year. In the ***“ROOT CA & Policy CA xx Operations Guide’s”*** there are specific processes which details the annual health check that is applied to ROOT CA and Policy CA’s. These processes serve in essence as on the job training for all the authorised responsibility holders of the Strong Room CA’s.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles for CA's

To ensure that one person acting alone cannot circumvent safeguards, responsibilities at a Root CA system need to be attended by multiple roles and individuals. Each account on the Root CA system shall have limited capabilities, commensurate with the role of the account holder.

CA Observer/Auditor (CAOA)

- Assigning security privileges and access controls of CAA. SA ISSO.
- Assigning passwords to all new accounts.
- Performing archive of required system records

CA Administrator (CAA)

- Certificate generation: Generating signed certificate to be processed and executed by the Root CA equipment according to defined rules
- Generating, distributing, and otherwise managing CRL's
- Administrative functions associated with maintaining the Root CA database and assisting in compromise investigations.

System Administrator (SA)

- Retrieving Root CA system from the safe
- Performing initial configuration of the system including secure boot start-up and shut down of the system
- Initial setup of all new accounts
- Setting the initial network configuration
- Creating emergency system restart media to recover from catastrophic system loss
- Performing system backups, software upgrades and recovery.
- Changing of the host name and/or network address.

Information System Security Officer (ISSO)

- Personally conducting or supervising an annual inventory of the Root CA's records.
- The secure storage and distribution of the backups to an off-site location
- Review of the audit log to detect CAA compliance with system security policy.
- Review of the audit log is done at least with each Root CA start-up

Note: that the ISSO, who is not directly involved in issuing certificates, performs an oversight function in examining system records or audit logs to ensure that other persons are acting within the realms of their responsibilities and within the stated security policy.

5.2.2 Number of Persons Required per Task

Separate individuals fill each of the roles described above. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over system operation.

5.2.3 Identification and Authentication for Each Role

Identification and authentication of CAA's, SA's and ISSO's are appropriate and consistent with practices, procedures and conditions stated in this policy.

5.3 PERSONNEL SECURITY CONTROLS

5.3.1 Background, qualifications, experience, and clearance requirements

The CAA role, which involves creating and managing certificate and key information, is a critical position security-wise. The individual assuming the CAA role should be of unquestionable loyalty, trustworthiness and integrity, and should have demonstrated a security consciousness and awareness in his or her daily activities.

All CA personnel in sensitive positions:

- not be assigned other duties that may conflict with their duties and responsibilities
- not as far known have been previously relieved of a past assignment for reasons of negligence or non-performance of duties
- have received proper training in the performance of their duties

5.3.2 Background check procedures

As stated in 5.3.1

5.3.3 Training requirements

PKO staff is typically trained in:

1 Basic PKO concepts
2 The use and operation of CA software
3 Documented CA procedures
4 Computer security awareness and procedures
5 The meaning and effect of relevant CP’s and this CPS.

5.3.4 Retraining frequency and requirements

PKO staff needs to refresh their knowledge annually and when they are assigned a job profile.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorised actions

Personnel performing unauthorised actions are subject to disciplinary actions consistent with existing Standard Bank human resource practices. In addition, the PA has the authority to temporarily suspend personnel from performing functions within the Root CA if deemed necessary for the security of the Standard Bank PKO.

5.3.7 Contracting personnel requirements

PKO staff may be contractors who are appointed in writing and given written notification of the terms and conditions of their position.

5.3.8 Documentation supplied to personnel

PKO staff has access to all relevant:

1 Hardware and software documentation
2 Application manuals
3 Policy documents, including relevant CP
4 Operational practice and procedural documents, including this CPS

6 TECHNICAL SECURITY CONTROLS

This section contains provisions of the public/private key pair management policy for the Root CA's and the corresponding technical controls.

6.1 KEY PAIR GENERATION AND INSTALLATION

All CA keys are generated only as part of pre-scheduled key protocol &ceremony processes.

6.1.1 Key pair generation

The Root CA generates his own key in hardware which is at least compliant to FIPS 140-1 level 3. Key pairs for trusted roles are generated on an IC card

It is the responsibility of the Root CA to undertake adequate measures to ensure that all public keys are unique within its domain before certificate binding takes place.

6.1.2 Private Key delivery to entity

All Policy CA's and trusted roles must generated their private keys, there is no key delivery.

6.1.3 Public Key delivery to certificate issuer

The Policy CA's public keys will be delivered on diskette to the (offline) Root CA Key pairs of trusted roles are created in the protected environment of the Root CA.

6.1.4 Root CA Public Key delivery to Users

The trusted CA is always the Root CA (rather than a Policy CA being directly trusted). The Certificate of the Root CA needs to be delivered to the End User for Certificate path validation. These may be distributed with the End User's own keys and certificates or may be downloaded by the End User from the Directory Services or from a Website.

For workstations under the control of the Standard Bank IT departments, the Root Certificate will be installed using remote software installation tools.

A hash of the issuing Root CA's public key will be available at a suitable location to allow an end user to verify its integrity and/or validity.

6.1.5 Key sizes

The keypairs for the Root CA and all Policy CA's have at least 2048 bits modulus for RSA

6.1.6 Public Key parameters generation

Key generation is accomplished by a random or pseudo-random number generator, compliant to ANSI X9.82. Key generation is accomplished using a prime number generator compliant to ANSI X9.80.

Key generation shall use an appropriate key generation algorithm for RSA, DSA or EC keys, compliant to the associated ANSI standards.

6.1.7 Parameter quality checking

No stipulation.

6.1.8 Hardware/software key generation

The Root CA and all other PKO entity keys are generated in Hardware Security Modules (HSMs).

6.1.9 Key usage purposes (As per X.509 v3)

No stipulation, this is standard process for subordinate Policy CA signing.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for Cryptographic Module

Cryptographic modules in use within the Standard Bank PKO comply with industry standards (e.g. FIPS 140-1)

6.2.2 Private Key (n out of m) multi-person control

The HSM that stores the Root CA private keys will be erased after each use. The Root CA private key is stored on a smartcard(s) protected by a key encryption key (KEK) this key is split into nine (9) segments. Each segment is stored on a different smart card, and different persons hold each a smart card. In order to reconstruct the Root CA key, at least three out of these nine persons need to convene at the CA'S to reconstruct the KEK and to restore the Root CA key. This means that no two persons shall possess the means required to activate the Root CA key.

6.2.3 Private Key escrow

There is no key escrow.

6.2.4 Private Key backup

The Root Private Key is backed up in the same manner as described in 6.2.2, three of the nine smartcards are stored in Backup location in segregated storage.

6.2.5 Private Key archival

The Root Private Key is archived up in the same manner as described in 6.2.2, three of the nine smartcards are stored at off-site cold-storage.

6.2.6 Private Key entry into cryptographic module

All private keys are generated in a HSM or on a smartcard, they are stored in such way that they can be used inside the token but never be retrieved from the token.

The Root CA private key is unloaded from the HSM as described in 6.2.2.

6.2.7 Private Key activation

The Standard Bank Root CA Private Key is not maintained online, it can be restored as described in 6.2.2. Once loaded, 3 people holding a SA role are required to activate the HSM.

6.2.8 Method of deactivating Private Key

Private keys stored in a HSM can be deactivated by either the HSM itself, through the self-protection mechanism, a reset, or by the CAA, through an interface command or by shutting down the software-interface.

"THIS IS PART OF THE TAKE-DOWN PROCESS"

6.2.9 Method of destroying Private Key

Private keys stored in a HSM can only be destroyed by resetting the cryptographic module and destroying or erasing more than three of the smart cards described in section 6.2.2.

Secret shares stored on smart cards can be destroyed by destroying or erasing the smart card, or by overwriting the secret share stored on the smartcard with a new one.

"THIS IS PART OF THE TAKE-DOWN PROCESS"

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public key archival

All public keys are published as certificates and archived from AD regularly.

6.3.2 Usage periods for the public and private keys

The ROOT CA private issuing keys shall not be valid for more than 20 years and shall not be used before or after its validity period for any purpose.

Private keys associated with a trusted role within the CA or RA (CAA, SA or ISSO) shall not be valid for more than 5 years. During the certificate validity period the CA shall provide adequate revocation services.

This implies that:

- A certificate may be used to verify a signature after the expiration of the certificate or after the certificate has been revoked as long as it can be determined that the signature was created before the time of revocation or before the certificate expiration date. This will normally require that the signed message has been time stamped (or logged) by a trusted service as well as access to associated certificates and CRL's, valid at the time when the signature was created.

6.4 ACTIVATION DATA

Activation Data for the Root CA are maintained in secret shares as defined in section 6.2.2 and used as multi-factor authentication process.

Passphrases serving as activation data for smartcards of the trusted roles shall consist of at least eight characters.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific computer security technical requirements

The Certification Authority System (CAS) shall provide sufficient computer security controls for the separation of roles described in Section 5.2 to be enforced.

The security controls shall provide access control and traceability down to an individual level on all transactions and functions affecting the use of the CA private keys.

Initialization of the system operating CA private keys shall require co-operation of at least two operators, both of which are securely identified by the system.

Activation of private CA-keys shall meet requirements stated in 6.2.2

In all cases, the configuration of Standard Bank PKO components will meet the security compliance requirements of Standard Bank's Information Security Department.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System development controls

The executable code that makes up the CA system software is vital to the correct functioning of the system. All executable code must be installed from the original software distribution media. The configuration of the Root CA system as well as any modification must be documented and controlled.

In all cases, the configuration of Standard Bank PKO components will meet the requirements of Standard Bank's Information Security Department.

6.6.2 Security management controls

System security management is controlled by the privileges assigned to operating system accounts, and by the trusted roles described in section 5.2

6.6.3 Life cycle security ratings

No stipulation.

6.7 NETWORK SECURITY CONTROLS

The Root CA is never connected to a network.

6.8 CRYPTO ENGINEERING CONTROLS

In general, Standard Bank does not engineer its own Cryptographic Modules. It utilizes commercially available modules either in hardware or software form to implement this PKO. The cryptographic tokens used shall meet the standards stated in 6.2.1

7 CERTIFICATE AND CRL PROFILES

This section contains rules and guidelines regarding the use of particular X.509 certificate and CRL fields and extensions.

7.1 CERTIFICATE PROFILES

7.1.1 Version number(s)

The PKO supports and uses X.509 Version 3 Certificates. The version field of the Certificates issued under this CPS shall then be set to 2, indicating that the version is v3.

7.1.2 Certificate Extensions

No stipulation, there are no Certificate extensions defined for subordinate CA signing.

7.1.3 Algorithm Object Identifiers

No Stipulation.

7.1.4 Name Forms

See 3.1.1

7.1.5 Name Constraints

There are no name constraints applicable to the certificate issued under this CPS.

7.1.6 Certificate Policy Object Identifier

CP OID’s are carried in the standard extension field of PKO X.509 certificates and published in the relevant CP.

7.1.7 Usage of Policy Constraints Extension

Policy Constraints extensions are not implemented in the ROOT CA

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation, this is left to the Issuing CA

7.1.9 Processing semantics for the critical certificate policy extension

No stipulation, there are no Certificate extensions defined for signing subordinate CA’s.

7.2 CRL PROFILE

7.2.1 Version number(s)

The PKO supports and uses X.509 Version 2 Certificate Revocation Lists (CRL’s).

7.2.2 CRL and CRL Entry Extensions

The PKO implements CRL entry extensions. Details of these extensions are included in the Certificate Profile section of the relevant CP.

8 SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

8.1.1 Items that can change without notification

The only changes that may be made to this specification without notification are editorial or typographical corrections, or changes to the contact details.

8.1.2 Changes with notification

Changes to items which, in the judgment of the PKO Authority (PA), will not materially impact a substantial majority of the subscribers or relying parties using this CPS may be changed with 90 days notice. Other changes will have a 120-day notice.

All proposed changes that may materially impact users of this policy will be notified by e-mail

Impacted users may file comments with the PA; comments have to be received within 60 days of original notice. Any action taken as a result of comments is at the sole discretion of the PA.

If the proposed change is modified as a result of comments, notice of the modified proposed change will be given at least 45 days prior to the change taking effect.

If a CPS change is determined by the PA to have a material impact on a significant number of users of the policy, PA may, at its sole discretion, assign a new Object Identifier to the modified CPS.

8.2 PUBLICATION AND NOTIFICATION POLICIES

8.2.1 Items not published in the CPS

No stipulation

8.2.2 Distribution of certificate policy definition and CPS

This CPS can be obtained from:

- In electronic form on the Intranet site: http://PKO.StandardBank.co.za/RCA_CPS.htm
- in electronic form via e-mail from info.PKO@StandardBank.co.za

APPENDICES

A CP's Supported Under this CPS

A.1 Standard Bank ROOT CA Certificate & Policy

Standard Bank Public Key Operations TRUST Hierarchy Anchor defines and implements the Bank's ROOT Certificate Authority.

There are no Certificate Policy loaded into the ROOT CA except the standard Microsoft Window 2003 PKI standard Certificate template to sign subordinate CA's ***("Policy CA's in this case")***

A.1.1 Standard Bank Root CA Certificate

OID: 1.3.6.1.4.1.16543.401.1.1.1.1

The following parts compose the OID:

ISO assigned	1
Organization acknowledged by ISO	3
US Department of Defence	6
Internet	1
Private	4
IANA registered private enterprise	1
Standard Bank	16543
Production environment	401
Root CA	1
CPS	2
Version	2.1

Table 3 – Standard Bank PKO ROOT CA Certificate OID

Certificate 0.0 DUMP:

```
E:\PKO\Trust Anchor>certutil -dump RCA.cer
X509 Certificate:
Version: 3
Serial Number: 060cd9c6e686448b4f7343e85ddbc856
Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
    Algorithm Parameters:
    05 00
Issuer:
    CN=Standard Bank ROOT CA
    O=Standard Bank Group
    OU=IT Security
    OU=PKO Services
    C=ZA
    S=GP
    L=JNB
  Name Hash(sha1): 4e85d97983cfc404906f66ebc3337a597b490e63
  Name Hash(md5): 00303dbf2c24f608461b869b0c0a63a8

 NotBefore: 10/9/2007 3:05 PM
 NotAfter: 10/9/2027 3:10 PM

Subject:
    CN=Standard Bank ROOT CA
    O=Standard Bank Group
    OU=IT Security
    OU=PKO Services
    C=ZA
    S=GP
    L=JNB
  Name Hash(sha1): 4e85d97983cfc404906f66ebc3337a597b490e63
  Name Hash(md5): 00303dbf2c24f608461b869b0c0a63a8

Public Key Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA
    Algorithm Parameters:
    05 00
Public Key Length: 4096 bits
Public Key: UnusedBits = 0
    0000  30 82 02 0a 02 82 02 01  00 b7 95 43 ad 3e d7 bc
    0010  8f 48 33 aa 96 c1 da 06  cf 3e 6c b2 1f 6f 17 74
    0020  fc 1b a1 5b 22 82 87 32  2b 9c 9a 20 15 13 01 e7
    0030  9e 50 c4 67 5c 5c 4c fc  4b f4 14 1e 15 db b4 27
    0040  db 99 10 fc ae 0e b3 c1  bb f9 57 15 3e ba f6 54
    0050  b4 0f 29 c0 be 3d 16 e4  c2 fe f5 1d 90 7e cd 91
    0060  38 b8 0a a5 45 2f 86 82  95 45 29 7a 58 17 28 5d
    0070  fc 8b a8 cb 52 a5 c0 a2  7d aa ab c2 ad 7b f8 b6
    0080  a3 1b 07 71 30 a3 11 3d  b3 5a 14 94 b0 37 15 e0
    0090  11 40 63 00 86 a6 4c 5f  ac d2 cf 0e a4 b0 02 06
    00a0  ed 7c 94 a5 e3 8d b1 b1  04 72 8a 4e 6a e4 7e 9a
    00b0  0e 3b 91 fb b7 45 6b 11  f0 54 e0 1c 35 38 26 af
    00c0  68 ce d9 37 a2 58 cd 51  1a 0a 7d a7 72 bc 02 c5
    00d0  d1 cc 6a c0 2f d0 c1 bd  5e f4 9e a7 16 cf b2 dd
    00e0  81 69 d3 95 1e a9 26 a9  2b 54 dc 6b 47 2c f7 ec
    00f0  b2 0e d2 e2 36 dd 21 f8  3a ef de 76 7f 70 c7 7f
    0100  b6 86 de 6b 8f 3e c2 d7  62 40 eb df 9d 1a 85 50
    0110  12 17 43 ad fe ad cd 2c  8d 20 0e 02 45 c5 fb 9a
    0120  4f 34 30 2f ec 9f 07 2c  40 85 61 14 14 0d 1f 8c
    0130  a4 e6 7e d6 19 f3 dd 54  12 8c 4c c1 60 b2 71 00
    0140  80 f8 be 8a 03 6a 17 63  65 72 09 14 8c 4d c8 54
    0150  22 4d 29 72 cf b1 a5 e3  82 6e a8 49 d4 89 e8 ce
    0160  d9 d6 81 f6 38 21 7a df  73 ea 0e 2a e5 5c 35 72
    0170  a9 55 e0 57 0e 4a 7d 1e  5c 43 51 76 c8 1a 10 7d
    0180  f1 35 16 69 93 e9 97 0b  a4 1c e0 e8 5e 5e b2 7f
    0190  e0 93 01 8a df 46 57 be  63 61 4a 4d 3a ef 98 d5
    01a0  bb 31 1f b1 4e 90 c2 4d  76 c4 1b 50 4f bb 04 60
    01b0  a1 f1 eb 77 a1 2c f2 b1  ab 48 b8 da af c6 7c 7f
    01c0  46 8e ae ad a6 88 ff 3c  d1 3d fa 36 0c 19 1e 24
    01d0  da 10 4d bc 71 65 cb f5  aa d8 04 8f 06 11 c9 a3
    01e0  cb 83 e4 47 7a 7f f6 1d  8f f0 e6 b0 20 cb bb 31
    01f0  d8 f6 28 ca 21 0f bc 25  4b 24 e5 f6 27 c3 f6 a1
    0200  de 97 52 02 2a 63 03 af  c1 02 03 01 00 01
Certificate Extensions: 5
    2.5.29.15: Flags = 0, Length = 4
    Key Usage
        Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

    2.5.29.19: Flags = 1(Critical), Length = 5
    Basic Constraints
        Subject Type=CA
        Path Length Constraint=None

    2.5.29.14: Flags = 0, Length = 16
    Subject Key Identifier
        ff 5b 92 09 02 f7 b9 80 d7 e8 21 79 8e 8a 00 83 fd 1e cb a2

    1.3.6.1.4.1.311.21.1: Flags = 0, Length = 3
    CA Version
        V0.0

    2.5.29.32: Flags = 0, Length = 51
    Certificate Policies
        [1]Certificate Policy:
             Policy Identifier=1.3.6.1.4.1.16543.401.1.2.2.1
             [1,1]Policy Qualifier Info:
                  Policy Qualifier Id=CPS
                  Qualifier:
                       http://pko.standardbank.co.za/RCA-CPSPage.htm

Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
    Algorithm Parameters:
    05 00
Signature: UnusedBits=0
    0000  59 ca bc a8 c5 bd 0e 4b  e6 cc 81 8e 03 b8 0f d7
    0010  a2 ff 0c cb c6 44 68 8f  9b 88 07 1b 17 f5 14 0d
    0020  63 bb 5a 42 28 ca 31 56  38 92 3a 2f 5f 95 b3 e1
    0030  4e fe f3 2a a3 c9 53 ab  1e 86 7b ac 64 d6 3d b7
    0040  71 f2 ed 47 cc 9a 82 2b  7c ee 54 c9 2e 59 4d 8b
    0050  b9 86 7a 9a 9b 08 ba 92  c2 d7 76 df 1a de b9 43
    0060  f2 24 06 a0 75 d8 1e 49  d9 66 fe 67 36 7d f4 e2
    0070  9e f9 09 41 37 6c 55 5f  af 8e 3b 5f 18 a4 ba f4
    0080  5a 79 6c 7a 41 a3 0b e3  05 0c 3c 81 f8 2e 27 fe
    0090  57 65 59 e7 18 f7 77 5b  a0 36 17 a1 9b e5 fe cf
    00a0  27 ce d2 17 bf 6a 6d 72  95 f5 62 11 b8 06 e3 6e
    00b0  a4 19 01 64 6b 3b 86 68  ae 62 86 78 0a bb 5c 77
    00c0  60 f0 de 30 73 b1 64 5b  b9 7e ba 84 b9 69 66 a9
    00d0  b9 d0 80 78 f8 46 c8 33  74 21 1d 04 42 f4 b3 a9
    00e0  f5 2a 02 3e c9 25 7c 4a  92 49 59 df fe 0a 3a 10
    00f0  be 8a 7a ca 00 d9 24 29  8c 81 87 d4 f9 81 4d f2
    0100  5b bd 44 31 8f 6d 2d 15  53 2e 25 03 2d ae 6c e9
    0110  cf d2 e6 9f c8 03 64 8b  a1 be f5 5d 4a 86 14 ec
    0120  e3 bf ab 5d 13 a0 59 1a  20 0c 45 5d a7 c1 5c 9f
    0130  a6 3b 41 84 d2 7e 1f d6  40 34 8d 84 f0 81 a3 6a
    0140  65 4d 28 6f bb 1c 89 1c  5c 67 19 c2 38 95 c6 2b
    0150  63 76 ea 5f 46 fc 6d 94  16 4d 04 98 5d 06 d1 79
    0160  28 75 43 ea 18 1e 1f 2a  f5 23 35 1f a8 5e 91 05
    0170  6f c1 c9 10 3d c0 87 e6  05 96 46 c2 c6 ba 71 4c
    0180  40 5a dc ee 79 83 c1 44  8d 40 ff a3 b8 91 47 e0
    0190  f2 61 05 00 e4 96 7b c2  74 76 79 10 f1 35 28 41
    01a0  b4 1d 7b e5 79 ac 4d dd  5f d6 75 b0 69 27 8e 49
    01b0  bb 82 4d 38 e2 83 7a 7c  69 11 bf 45 25 bc fe 61
    01c0  ea 2a f4 62 5b 74 56 3e  3e 01 77 a8 63 db 12 a1
    01d0  e7 ce 2f b2 2a bd 31 ed  6d a9 0d 58 0c 4a fd 6b
    01e0  50 c3 03 0d ac b4 2f ae  f8 dc e4 20 37 09 03 c1
    01f0  57 00 2b 76 2c 7e b2 ce  bc 93 08 b8 71 fc d6 95
```

```
Signature matches Public Key
Root Certificate: Subject matches Issuer
Key Id Hash(rfc-sha1): e3 9c 75 e0 cc e8 b6 0a e4 07 93 ed 89 1e 94 d0 46 5f 29 f5
Key Id Hash(sha1): ff 5b 92 09 02 f7 b9 80 d7 e8 21 79 8e 8a 00 83 fd 1e cb a2
Key Id Hash(md5): 8863e8c62aedaf51bf5b154ad06f8723
Key Id Hash(sha256): 93b9cb134980075241909c470ea6e2fe431a803229b77b6fe60aa52f2cc3149b
Cert Hash(md5): 17 8c f4 62 d4 bc 9b a6 c4 41 ae 11 bf f0 b3 37
Cert Hash(sha1): 00 bb 43 05 95 75 b7 c8 1a 7b dd 4b a6 c1 48 05 19 8c 10 e2
Cert Hash(sha256): c2a8b80657496c995787104eb7c7f3fd2b34e013c58433404fb8c283156cf64f
Signature Hash: e0c814d080e0646c741a64f5ab6e97f58cc5fd37
CertUtil: -dump command completed successfully.
```

Certificate 1.0 Dump:

```
X509 Certificate:
Version: 3
Serial Number: 474b89082917dfae49897ed257f80e01
Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.11 sha256RSA
    Algorithm Parameters:
    05 00
Issuer:
    CN=Standard Bank ROOT CA
    O=Standard Bank Group
    OU=IT Security
    OU=PKO Services
    C=ZA
    S=GP
    L=JNB

 NotBefore: 2007/10/09 03:05 PM
 NotAfter: 2040/12/21 06:56 PM

Subject:
    CN=Standard Bank ROOT CA
    O=Standard Bank Group
    OU=IT Security
    OU=PKO Services
    C=ZA
    S=GP
    L=JNB

Public Key Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.1 RSA
    Algorithm Parameters:
    05 00
Public Key Length: 4096 bits
Public Key: UnusedBits = 0
    0000  30 82 02 0a 02 82 02 01  00 b7 95 43 ad 3e d7 bc
    0010  8f 48 33 aa 96 c1 da 06  cf 3e 6c b2 1f 6f 17 74
    0020  fc 1b a1 5b 22 82 87 32  2b 9c 9a 20 15 13 01 e7
    0030  9e 50 c4 67 5c 5c 4c fc  4b f4 14 1e 15 db b4 27
    0040  db 99 10 fc ae 0e b3 c1  bb f9 57 15 3e ba f6 54
    0050  b4 0f 29 c0 be 3d 16 e4  c2 fe f5 1d 90 7e cd 91
    0060  38 b8 0a a5 45 2f 86 82  95 45 29 7a 58 17 28 5d
    0070  fc 8b a8 cb 52 a5 c0 a2  7d aa ab c2 ad 7b f8 b6
    0080  a3 1b 07 71 30 a3 11 3d  b3 5a 14 94 b0 37 15 e0
    0090  11 40 63 00 86 a6 4c 5f  ac d2 cf 0e a4 b0 02 06
    00a0  ed 7c 94 a5 e3 8d b1 b1  04 72 8a 4e 6a e4 7e 9a
    00b0  0e 3b 91 fb b7 45 6b 11  f0 54 e0 1c 35 38 26 af
    00c0  68 ce d9 37 a2 58 cd 51  1a 0a 7d a7 72 bc 02 c5
    00d0  d1 cc 6a c0 2f d0 c1 bd  5e f4 9e a7 16 cf b2 dd
    00e0  81 69 d3 95 1e a9 26 a9  2b 54 dc 6b 47 2c f7 ec
    00f0  b2 0e d2 e2 36 dd 21 f8  3a ef de 76 7f 70 c7 7f
    0100  b6 86 de 6b 8f 3e c2 d7  62 40 eb df 9d 1a 85 50
    0110  12 17 43 ad fe ad cd 2c  8d 20 0e 02 45 c5 fb 9a
    0120  4f 34 30 2f ec 9f 07 2c  40 85 61 14 14 0d 1f 8c
    0130  a4 e6 7e d6 19 f3 dd 54  12 8c 4c c1 60 b2 71 00
    0140  80 f8 be 8a 03 6a 17 63  65 72 09 14 8c 4d c8 54
    0150  22 4d 29 72 cf b1 a5 e3  82 6e a8 49 d4 89 e8 ce
    0160  d9 d6 81 f6 38 21 7a df  73 ea 0e 2a e5 5c 35 72
    0170  a9 55 e0 57 0e 4a 7d 1e  5c 43 51 76 c8 1a 10 7d
    0180  f1 35 16 69 93 e9 97 0b  a4 1c e0 e8 5e 5e b2 7f
    0190  e0 93 01 8a df 46 57 be  63 61 4a 4d 3a ef 98 d5
    01a0  bb 31 1f b1 4e 90 c2 4d  76 c4 1b 50 4f bb 04 60
    01b0  a1 f1 eb 77 a1 2c f2 b1  ab 48 b8 da af c6 7c 7f
    01c0  46 8e ae ad a6 88 ff 3c  d1 3d fa 36 0c 19 1e 24
    01d0  da 10 4d bc 71 65 cb f5  aa d8 04 8f 06 11 c9 a3
    01e0  cb 83 e4 47 7a 7f f6 1d  8f f0 e6 b0 20 cb bb 31
    01f0  d8 f6 28 ca 21 0f bc 25  4b 24 e5 f6 27 c3 f6 a1
    0200  de 97 52 02 2a 63 03 af  c1 02 03 01 00 01
Certificate Extensions: 6
    2.5.29.15: Flags = 0, Length = 4
    Key Usage
        Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

    2.5.29.19: Flags = 1(Critical), Length = 5
    Basic Constraints
        Subject Type=CA
        Path Length Constraint=None

    2.5.29.14: Flags = 0, Length = 16
    Subject Key Identifier
        ff 5b 92 09 02 f7 b9 80 d7 e8 21 79 8e 8a 00 83 fd 1e cb a2

    1.3.6.1.4.1.311.21.1: Flags = 0, Length = 3
    CA Version
        V1.0

    2.5.29.32: Flags = 0, Length = 52
    Certificate Policies
        [1]Certificate Policy:
             Policy Identifier=1.3.6.1.4.1.16543.401.1.2.2.1
             [1,1]Policy Qualifier Info:
                  Policy Qualifier Id=CPS
                  Qualifier:
                       http://pko.standardbank.co.za/RCA-CPSPage.htm

    1.3.6.1.4.1.311.21.2: Flags = 0, Length = 16
    Previous CA Certificate Hash
```

```
        00 bb 43 05 95 75 b7 c8 1a 7b dd 4b a6 c1 48 05 19 8c 10 e2

Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.11 sha256RSA
    Algorithm Parameters:
    05 00
Signature: UnusedBits=0
    0000  ff 8c 43 eb 49 68 3c bd  f3 66 fe df ef b4 7a 31
    0010  88 35 f7 71 2e c4 9e f5  a4 36 77 85 be dc af 9f
    0020  7a ff 86 6f bb ec fd 75  3b 41 3c 76 ff 00 05 68
    0030  e2 91 ea 1d af 19 4a c5  19 85 7e d7 94 07 84 25
    0040  b0 50 82 c4 32 1f 94 60  39 df b0 e3 89 ae 89 f9
    0050  5d 5f 94 4d 99 19 92 f4  8f 74 09 78 b1 43 70 0a
    0060  fe 1e a5 30 81 dc 29 3b  f4 81 ca f9 b1 77 2d f4
    0070  04 7d f2 ad 05 48 ea 58  34 cd c5 c0 85 13 51 be
    0080  15 86 77 c7 26 2a 0e 12  5e d4 54 69 12 c5 5c 6e
    0090  07 a8 20 64 2c e5 33 b5  8e 89 1a bf e4 5e 12 ce
    00a0  57 dd fd da 70 73 e4 ea  49 d3 e7 d6 0d 2e b7 bb
    00b0  d6 de 18 c4 db 67 36 82  90 a1 7d 76 e8 41 ca 63
    00c0  d3 82 3c 84 8e c8 20 08  1e b6 c3 6c 95 01 f9 ac
    00d0  e5 d9 c9 a8 bd 9b ff bc  50 a9 d2 a3 98 7c 1a a9
    00e0  8c 0f ba fb 2f 87 28 02  93 cf a1 bd c9 b6 34 eb
    00f0  04 d5 9c 64 e8 5b 27 8e  44 5c 71 af 42 8e 12 f1
    0100  e5 cb 65 4c 2a 4e e1 16  4b 89 fd 86 a0 1d 6f c7
    0110  82 81 f8 36 7b 8f c8 1e  41 8e fd 66 80 47 06 26
    0120  35 fe e3 12 01 06 45 79  bf da 39 f8 23 b3 04 ef
    0130  b0 7c 8c 3e fc f3 77 c9  45 c7 43 57 55 34 0e d6
    0140  58 c1 68 08 b8 a7 7c bc  c4 d7 c4 de 1b 88 c5 d4
    0150  da 3e ef 55 b0 f1 48 e4  66 3d 6d 30 0d b1 4c d4
    0160  7e 42 c0 27 86 0e e8 d6  dd e8 1a 7c 22 90 6e 28
    0170  0c 86 4a bb 76 1b 8b 87  da ba 36 e6 4d 83 8d bb
    0180  a8 5e 42 28 b7 30 7b df  02 32 61 6e ab 58 a1 18
    0190  3e c2 84 51 c8 d7 22 ba  5a 10 92 c3 52 b2 9c c1
    01a0  df 2f f4 65 a7 0f 5d 1b  39 34 c1 c7 03 00 37 69
    01b0  d0 7b fb da 2d 1b 97 1f  64 62 84 8c 42 28 eb a2
    01c0  2a 5b b8 4a 3d ea 00 95  a3 e6 32 0b 42 b3 47 4c
    01d0  4a 53 d1 a1 40 64 54 60  e8 59 2d 76 01 36 e2 52
    01e0  de 92 73 93 36 cb 3a 77  5d 87 48 36 32 e5 ee 6e
    01f0  8d 73 f5 e4 33 24 c2 19  6b 16 20 5c 85 92 fc 4c
Signature matches Public Key
Root Certificate: Subject matches Issuer
Key Id Hash(rfc-sha1): e3 9c 75 e0 cc e8 b6 0a e4 07 93 ed 89 1e 94 d0 46 5f 29 f5
Key Id Hash(sha1): ff 5b 92 09 02 f7 b9 80 d7 e8 21 79 8e 8a 00 83 fd 1e cb a2
Cert Hash(md5): cc 1c fb a4 24 67 3d c5 33 82 a7 fa 6d 39 2b bb
Cert Hash(sha1): 83 7d 9c f1 14 7a cf 12 07 3f 05 74 74 6d 2a 7b 6c 1f 7c ab
CertUtil: -dump command completed successfully.
```

A.2 Standard Bank Root CA Configuration

Root Certificate Authority	
CA Unique Name	Standard Bank Root CA
Version Type	V3
Current Certificate Version	3
	Self-Signed
CA Lifetime	33 Years
CA Key Length	4096
CRL Validity Interval	367 Days
CRL Publishing Interval	365 Days
CSP PKI Algorithm	RSA
CSP HASH Algorithm	SHA-256
CRL Locations:	LDAP to Active Directory and HTTP

Subject DN	O = Standard Bank Group
	OU = IT Security Services
	C = ZA
	L = JHB
	ST = GP

A.3 Glossary

A.3.1 Terms

Certification Authority (CA) - An authority trusted by one or more users to create and assign public key certificates. Optionally the CA may create the user's keys. It is important to note that the CA is responsible for the public key certificates during their whole lifetime, not just for issuing them.

CA-certificate - A certificate for one CA's public key issued by another CA.

Certificate policy (CP) - A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certification path - An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path. Certification Practice Statement (CPS) - A statement of the practices which a certification authority employs in issuing certificates.

Certificate revocation list (CRL) - A CRL is a time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.

Issuing certification authority (issuing CA) - In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).

Public Key Certificate (PKC) - A data structure containing the public key of an end entity and some other information, which is digitally signed with the private key of the CA which issued it.

Public Key Infrastructure (PKI) - The set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke PKCs based on public-key cryptography.

Registration authority (RA) - An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA). [Note: The term Local Registration Authority (LRA) is used elsewhere for the same concept.]

Relying party (RP) - A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Subject certification authority (subject CA) - In the context of a particular CA certificate, the subject CA is the CA whose public key is certified in the certificate

IPR – Intellectual Property Rights

A.3.2 Key words for use in RFC’s to Indicate Requirement Levels

According to RFC 2119 [2] —Key words for use in RFC’s to Indicate Requirement Levels“, we specify how the main keywords used in RFC’s should be interpreted.

Authors who follow these guidelines should incorporate this phrase near the beginning of their document: The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHAL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

MUST This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

MUST NOT This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
SHOULD This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

SHOULD NOT This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.

MAY This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

A.3.3 References

Request for Comments: 3647, Orion Security Solutions, Inc., Obsoletes: 2527, W. Ford, VeriSign, Inc., R. Sabett, Cooley Godward LLP, C. Merrill, McCarter & English, LLP, S. Wu, Infoliance, Inc., November 2003