Policy CA 11 V3.2 Certificate Practice Statement

Public Key Operations

Standard Bank of South Africa

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

, , Version Error! Unknown document property name.**2** Error! Unknown document property name.

Based on *RFC 3647 Certificate Policy and Certificate Practices Framework, Chokhani and Ford, November 2003*

Prepared by **Moris Halevi**

Thursday, 26 April 2018 - 11:18:20 AM

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

, , Version Error! Unknown document property name.**2** Error! Unknown document property name.

Based on	*RFC 3647 Certificate Policy and Certificate Practices Framework, Chokhani and Ford, November 2003*
Prepared by	**Moris Halevi**
	Thursday, 26 April 2018 - 11:18:20 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
11th June 2015	Moris Halevi	3.1	Reviewer added
10th December 2017	Londani Mulaudzi	3.2	Removed WEBTRUST Reference, CA version infrastructure update and update for RFC 3647

Reviewers

Name	Version approved	Position	Date
Lynette Schulz	3.0	Head: Cryptography Services	2015/06/11
Londani Mulaudzi	3.1	Specialist: Cryptography	28 April 2017
Zukiswa Mahlawe	3.2	Specialist: Cryptography	09th January 2018

Table of Contents

Tables

1. INTRODUCTION

1.1. Overview

The main goal of the Standard Bank Policy Certification Authority is to offer a common policy repository for all Certificate type that has common ground 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 its own 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 Policy CA 11 Certification Authority in issuing and managing digital certificates for its Issuing CA's that are for Standard Bank internal use only. The Issuing CA's that get certified by the Policy CA 11, issue certificates to Standard bank employees, full time contractors and equipment that is part of Standard Bank's asset register.

The purposes of this document are to:

1. Guarantee that 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, is not compromised by introduction of the Policy CA 11 into the Standard Bank Trust Hierarchy.
2. Describe how the Standard Bank Policy CA 11 meets the requirements of each Certificate Policies under which certificates are issued to the different Issuing CA's in the Standard Bank PKO.
3. Set out the minimal requirements for its Issuing CA's for the management and administrative practices used to protect the trustworthiness of the Issuing CA and the whole Standard Bank PKO.
4. Act as an input to audit activities. One audit activity is to validate that the Policy CA 11 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 [RFC2527]. 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 Policy CA 11 issues certificates in accordance with this CPS dated “2018-04-26”, that certifies the Standard Bank Issuing CA’s and establishes the ***“TRUST chain”*** to Standard Bank’s ROOT CA.

CPS Name: Standard Bank Policy CA 11 Certificate Practice Statement OID: 1.3.6.1.4.1.16543.401.11.2.2.1

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
Policy CA 11	11
CPS	2
Version	2.1

Table 1 – Standard Bank PKO POLICY CA 11 CPS OID

1.3. COMMUNITY AND APPLICABILITY

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

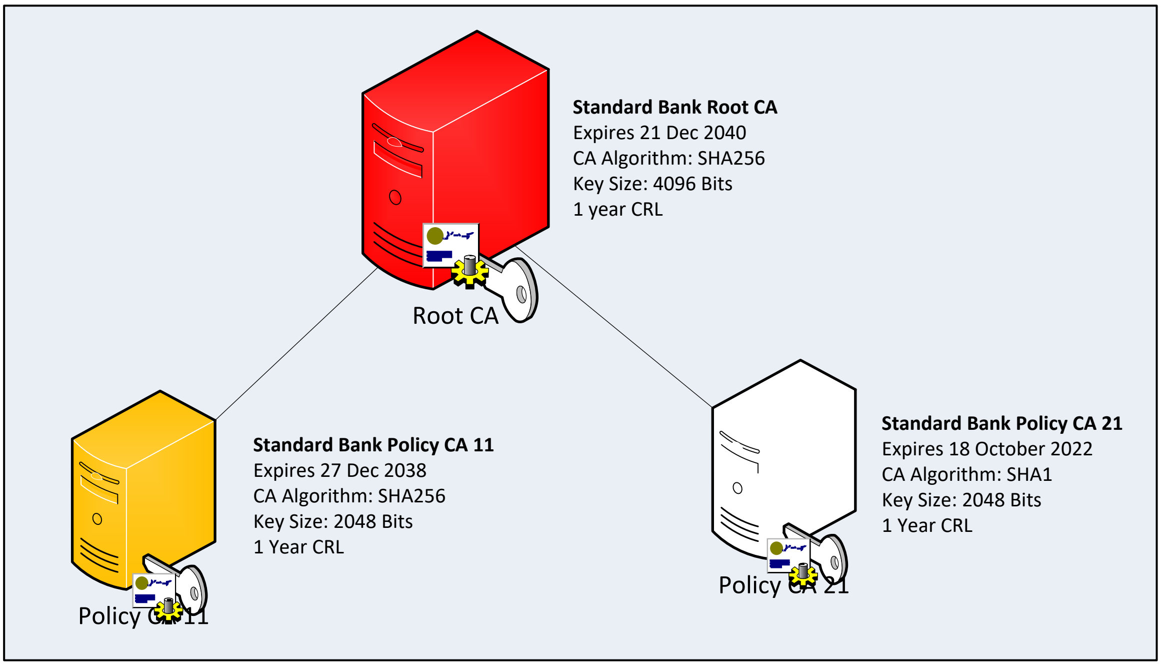

Table 2 – Standard Bank PKO High-Level Architecture

1.3.1. Certificataion 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 Policy CA 11 the description of its ROOT & Issuing CA's are included for better understanding of this CPS.

1.3.2. 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

1.3.3. 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 **<u>Internal Policy CA *"PCA 1x"*:</u>** This(these) PCA(s) certifies the Standard Bank internal use Issuing CA's which in turn certify employees, contractors 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 Business Unit or Country level.

2 **<u>Internal Policy CA "PCA 2x":</u>** 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 provide secure communications and authenticated message delivery between the Business Units and their clients.

The Policy CA 11 is certified by the Root CA to perform certificate services only to certify subordinate Issuing CA's. The Standard Bank Root CA Certificate Policies and the Policy CA 11 certification agreements ensure that the Policy CA 11 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.

1.3.4. Registration authorities

The primary purpose of a RA is to register End Entities, on behalf of its parent CA. The registration of subordinate Issuing CA's is a complex but manual process executed under scrutiny of an independent observer, therefore Standard Bank Policy CA 11 will not deploy a RA.

The practices used for registration and certification of End Entities are documented in the CPS of the Issuing CA's. This CPS must be approved by the Standard Bank PKO Authority ***("PA")*** prior to the certification of the Policy CA 11, and accredited by an independent assessor.

1.3.5. End entities

The Standard Bank Policy CA 11 will only certify subordinate Issuing CA's; there are no End Entities. The Policy CA 11 may issue certificates to the operational staff of the Subordinate Issuing CA's for strong authentication, since these certificates are not usable outside the Policy CA 11 environment they are not considered as End-Entities certificates.

1.3.6. Relying Parties

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

1.3.7. 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 Policy CA 11 are supported by this CPS. The Certificate Policies supported by the Standard Bank Policy CA 11 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 of this CPS.

1.3.8. Suitable Applications

- Certification of Issuing CA's that will issue certificates for internal use and primarily to support Microsoft integrated services such as Secure email, Encrypted File System, device authentication (Computers, CISCO equipment) but not limited to those only. Individual policies will be added as they become necessary
- Being the LINK to the Anchor of Standard Bank TRUST Hierarchy.

1.3.8.1 Restricted Applications

No stipulation

1.3.8.2. Prohibited Applications

Standard Bank Policy 11 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 Operation Crypto Services
Standard Bank
5 Simmonds St
2000 Marshaltown
South Africa

E-mail: ITS Certificate Management ITSCertificateManagement@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 Policy CA 11 will operate in a contractually closed environment. Therefore contractual agreements are assumed to be in place between all the Subordinate Issuing CA's and the Policy CA 11 in the Standard Bank PKO.

2.1.1. CA obligations

2.1.2. Policy CA 11 Obligations

The Policy CA 11 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 Subordinate Issuing CA's, that comply with X.509 standards and are suitable for the purpose required and certifying no other entities

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 the Issuing 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.

2.1.3. Issuing CA y11 Obligations

Issuing CA's operating under this Policy CA 11 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 Policy CA 11 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 Policy CA 11 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 ***("in this instance into Standard Bank Active Directory defined in the bank's forest")***

4 Provide revocation status services for certificates it issues and publishing Certificate status information in a CRL to a nominated directory. ***("see point (3) above ")***

2.1.2. RA obligations

No stipulation - Policy CA 11 does not depend or implement RA for signing subordinate Issuing CA's.

2.1.3. Subscriber obligations

The subscriber of Policy CA 11 certificate services is a set of subordinate Issuing CA's see 0, this CPS does limit PCA and ICA relationship to CA Certificate Services by PCA for the ICA's. Therefore there are no obligations by the ICA's.

2.1.4. Relying party obligations

Relying Parties fulfil their obligations under this CPS by:

1 Obtaining a trustworthy copy of the Policy CA 11's certificate signed by the ROOT CA.

  - 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 Policy CA 11 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 Policy CA 11 makes no other warranties or promises and have no further obligations to the subordinate Issuing 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 Policy CA 11 disclaims all other warranties, promises and other obligations.

In no event shall Standard Bank Policy CA 11 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 Policy CA 11 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 Issuing CA's subordinate to this Policy CA.

2.2.4. Other exclusions

Standard Bank Policy CA 11 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 Policy CA 11
- 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 Policy CA 11
- 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 Policy CA 11 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 Policy CA 11 an agent, fiduciary, trustee, or other representative of the Subordinate Issuing 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 Policy CA 11.

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 interprets consistently inline with what is commercially reasonable and in good faith under the circumstances.

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

2.5. FEES

Certificate issuance or renewal fees

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

Certificate access fees

No stipulation

Revocation or status information access fees

No stipulation

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.

Refund policy

No stipulation.

2.6. PUBLICATION AND REPOSITORY

2.6.1. Publication of Root CA information

The following information is available in a repository to all parties that use Standard Bank Policy CA 11 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 majeur. Standard Bank will make its best effort to limit the unavailability of the repository.

2.6.2. Frequency of publication

CPS and CP publication are in accordance with section 8. Certificates are 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 are appropriate access controls to oversee 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 Policy CA 11, to verify if the Subordinate Issuing CA's comply 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 Policy CA 11.
- At any other time that it deems warranted, and at least annually

The PA has the right to require audits on Subordinate Issuing CA's in order to detect non-compliance with obligations imposed by this CPS the applicable CP or Policy CA 11 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 Policy CA 11 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 Policy CA 11 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 Issuing 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.

The Certificate Policy states requirements for naming of the Issuing CA's serviced under this 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 the Subordinate Issuing 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 Policy CA 11 will assure uniqueness of all the Subordinate Issuing 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 Subordinate Issuing CA's operated by Business Units of the Standard Bank entering the Standard Bank PKO. The authentication of the Standard Bank organisational unit, applying for a Subordinate Issuing 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

Issuing 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 application in writing
- and a visit a described in ***(“Policy CA 11 Operations Guide”)*** to the Policy CA 11

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 IT Security PKO Authority the owner of the Policy CA 11 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 11 delivers the required level of trustworthiness. If this validation yields a satisfactory result the PA will subordinate the Issuing CA

Upon receipt of the subordination the PA will set a date on which the creation of the Issuing CA can occur and appoint a team from the PA and an independent observer as a witness for the creation.

4.2. CERTIFICATE ISSUANCE

On the agreed date the observer appointed by the PA will be present during the Issuing 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 Issuing CA's private key and a self-signed certificate request.

The certificate request file will be stored in a tamperproof media containing the signatures of the ceremony master and the team appointed by the PA this until the issuance by the Policy CA 11.

At the Policy CA 11 the certificate will be issued only if:

- The media 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 Policy CA 11 indicates a complete and final approval of the certificate application by the Policy CA 11.

The issued certificate will be handed over to the Issuing CA administrator. The Policy CA 11 will wait with the publication of the issued certificate in the repository, until a confirmation of the successful completion of the Issuing CA installation has been received.

Detailed process and team protocols are described in ***("Policy CA 11 Operations Guide")***

4.3. CERTIFICATE ACCEPTANCE

Upon reception of the certificate the Issuing CA will complete the second part of the creation ceremony. The Issuing 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 Policy CA 11 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 Policy CA 11 will be notified of the successful installation and a copy of the creation ceremony will be sent to the Policy CA 11.

By accepting a certificate, the Issuing CA agrees:

- to be bound by the continuing responsibilities, obligations and duties imposed on him by this PCA, the CP and this CPS
- no unauthorised person has ever had access to the Issuing CA's private key.
- all information given by the Issuing CA to the Policy CA 11 and included in the certificate is true

4.4. CERTIFICATE SUSPENSION AND REVOCATION

The Policy CA 11 is responsible for issuing and publishing CRL's. The Policy CA 11 shall update its CRL to reflect changes in revocation status and must issue timely CRL's.

4.4.1. Circumstances for revocation

Certificates are 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 Issuing CA has no longer use for the certificate
- The Issuing CA can be shown to have violated the stipulations of the CP, this CPS or the subordination principles
- An authenticated revocation request is received from the Issuing CA
- A validated revocation request is received from a third party
- The Issuing CA private key is suspected of compromise :
- Unauthorised access or suspected unauthorised access to the private key
- Lost or stolen key
- Destroyed key
- The Policy CA 11 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

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

The Issuing CA must immediately notify the Policy CA 11 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
- and a visit to the Policy CA 11

In writing Authentication of the revocation request shall meet the requirements in 3.4 The Policy CA 11 shall archive all revocation requests, the cause for revocation, the means of authenticating the request and the resulting actions taken by the Policy CA 11. To process a revocation request:

1 The Policy CA 11 authenticates the revocation request

2 The Policy CA 11 makes the arrangements for the key-holders attendance

3 The Policy CA 11 revokes the Certificate.

4 The Policy CA 11 submits an updated CRL to the repository, including the revoked certificate.

5 The Policy CA 11 notifies the Issuing 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 Issuing CA 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 Policy CA 11 issues a CRL reporting the revocation status of all the Subordinate Issuing CA’s at intervals not exceeding 1 year. In the event that a Subordinate Issuing CA’s certificate needs to be revoked, the Policy CA 11 will immediately issue and publish a replacement CRL. The previous CRL will be deleted from the directory.

Policy CA 11 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 are stored locally however before use; each such certificate is 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 Policy CA 11 system and software components which may affect the outcome of the certificate issuing processes and the CRL.

Cryptographic tokens used in the Policy CA 11 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 Policy CA 11 system shall log, for audit purposes:

- All physical access to Policy CA 11 Strong Room
- POLICY CA 11 server start-up, shutdown and take-down
- POLICY CA 11 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 POLICY CA 11 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 are processed each time the CA system is removed from the safe and brought operational and analyzed for evidence of unauthorised or inappropriate behaviour.

4.5.3. Retention period for audit log

Audit logs are 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, are 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 Policy CA 11 which includes CA application audit log, operating system generated logs and essential configuration files are written to CD-ROM before the Policy CA 11 is returned to its safe.

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

4.5.5. Audit log backup procedures

Two copies of the consolidated logs are 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 Policy CA 11's possession including:

- Configuration files of the Policy CA 11 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 Policy CA 11.
- 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 are 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 Policy CA 11 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 Policy CA 11 shall make documentation available that demonstrates the Policy CA 11's compliance with section 2.7 of this CPS.

The Policy CA 11 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 Policy CA 11 key changeover procedures in the "Policy CA 11 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 Policy CA 11 will be suspended and the Policy CA 11 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 POLICY CA 11 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 POLICY CA 11 irrespective if the CA was used or not in the last 12 months. ***("see Physical Security Protocols in the PKI Design document for details")***

PKO operations have the responsibility of bringing up the POLICY CA 11 within 3 month from notice or disaster. In worst case scenario as stipulated in deployment guidelines POLICY CA 11 can be re-build from scratch on newly ordered hardware. There is no need for redundant hardware.

DR scenario for POLICY CA 11 entails re-start-up of the physical server from scratch as would be in the case of the initial commissioning of the POLICY CA 11 and The HSM will be re-loaded from the Admin & Operator Smartcards. The process is detailed in ***("Deployment and Operations Guides")*** for the POLICY CA 11.

4.8.2. Entity Public Key is revoked

In the event of the need for revocation of the Policy CA 11's public key, the CA must:

- immediately notify the PA
- Inform its Subordinate Issuing CA's.
- The Policy CA 11 certificate must be removed from all relying parties trust lists

The Policy CA 11 will be brought down and a new Policy CA 11 key generation process will occur. Certificates issued prior to the revocation are re-signed.

4.8.3. Entity Key is compromised

If an incident occurs resulting in the Policy CA 11 private key being compromised, the Policy CA 11 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 Policy CA 11 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 Policy CA 11 to protect their operations.

For detailed description of security architecture please refer to ***"PKI Design"*** and for security access protocols please refer to ***"Policy CA 11 Deployment Guide".***

All the processes and protocols are also defined in specific worksheets that act as route maps to deploy then use the POLICY CA 11. 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 POLICY CA 11.

5.1. PHYSICAL SECURITY CONTROLS

Physical security controls are implemented to control access to the Policy CA 11'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 Policy CA 11 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 Policy CA 11 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 Policy CA 11 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.

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

Off site storage is used for the storage and retention of backup software and data. The off site storage is referred as the cold storage and is managed by a third party contracted to offer OFF-Site storage 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 more lower in the case of a Policy CA, a health check is prescribed for all the OFFLINE & POWERED-OFF CA's at least once 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 Policy CA 11 system need to be attended by multiple roles and individuals. Each account on the Policy CA 11 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 Policy CA 11 equipment according to defined rules
- Generating, distributing, and otherwise managing CRL’s
- Administrative functions associated with maintaining the Policy CA 11 database and assisting in compromise investigations.

System Administrator (SA)

- Retrieving Policy CA 11 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 Policy CA 11'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 Policy CA 11 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 Policy CA 11 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 Policy CA 11'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.

6.2.1. Key pair generation

The Policy CA 11 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 Policy CA 11 to undertake adequate measures to ensure that all public keys are unique within its domain before certificate binding takes place.

6.2.2. Private Key delivery to entity

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

6.2.3. Public Key delivery to certificate issuer

The Issuing CA's public keys will be delivered on diskette to the (offline) Policy CA 11 Key pairs of trusted roles are created in the protected environment of the Policy CA 11.

6.2.4. Policy CA 11 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 & Policy Certificate will be installed using integrated Active Directory Synchronisation processes.

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

6.2.5. Key sizes

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

6.2.6. 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.

6.2.7. Parameter quality checking

No stipulation.

6.2.8. Hardware/software key generation

The Policy CA 11 and all other PKO entity keys are generated in Hardware Security Modules (HSMs).

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

No stipulation, this is defined in the Key Life Cycle document.

6.3. PRIVATE KEY PROTECTION

6.3.1. Standards for Cryptographic Module

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

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

The HSM that stores the Policy CA 11 private keys is cleared of all keys after each use. The Policy CA 11 private key is stored on multiple smartcard(s) protected by a key encryption key (KEK) and encrypted key-parts stored on KMDATA. Furthermore the Private 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 Policy CA 11 key, the custodian of KM DATA and at least three out of these nine persons need to convene at the CA'S to reconstruct the KEK and to restore the Policy CA 11 key. This means that no three persons shall possess the means required to activate the Policy CA 11 key.

6.3.3. Private Key escrow

There is no key escrow.

6.3.4. Private Key backup

The Policy CA 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.

6.3.5. Private Key archival

The Policy 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.

6.3.6. Private Key entry into cryptographic module

All private keys are generated in a HSM and disseminated to smartcards, they are stored in such way that they can be used inside the token but never be retrieved from the token.

The Policy CA 11 private key is never persistent in the HSM as described in 6.2.2.

6.3.7. Private Key activation

The Standard Bank Policy CA 11 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.

6.3.8. 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, trough an interface command or by shutting down the software-interface. Furthermore the Private Key can only be used when the last Operator Card is still in the HSM, as part of Takedown the Operator Card is un-slotted from the HSM and locked in the Vault Safe.

"THIS IS PART OF THE TAKE-DOWN PROCESS"

6.3.9. 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"

6.4. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.4.1. Public key archival

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

6.4.2. Usage periods for the public and private keys

The POLICY CA 11 private issuing keys shall not be valid for more then 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 then 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.

6.5. ACTIVATION DATA

Activation Data for the Policy CA 11 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.

6.6. COMPUTER SECURITY CONTROLS

6.6.1. 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.

6.7. LIFE CYCLE TECHNICAL CONTROLS

6.7.1. 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 Policy CA 11 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.

6.7.2. 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

6.7.3. Life cycle security ratings

No stipulation.

6.8. NETWORK SECURITY CONTROLS

The Policy CA 11 is never connected to a network.

6.9. 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. There is an automated process defined in the nCipher netHSM that creates & manages unique numbers for the certificates issued by the Policy CA. The details of the certificate fields are described in Appendix - 9.1. Standard Bank Policy CA 11 Certificate **& Certificate Policies**

7.1.2. Certificate Extensions

The PKO supports Certificate extensions. Certificate extensions consist of three fields:

Type	this field indicates the type of data in the value field
Criticality	this indicates the importance of the information contained in the value field
Value	this field contains the additional Certificate information

The PKO supports Certificate extensions to provide additional information about, or restrict usage of, a Certificate as prescribed within a relevant CP.

Key Usage fields in all Certificates issued within the PKO have a criticality value of “true”. The purpose and meaning of Certificate extensions are explained in the associated CP.

7.1.3. Algorithm Object Identifiers

No Stipulation. The details of the certificate fields are described in Appendix - 9.1. Standard Bank Policy CA 11 Certificate **& Certificate Policies**

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 PKO.

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, the Policy CA does not use any Certificate extension(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 30 days notice. Other changes will have a 60-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 will be received within 30 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 is given at least 30 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
- in electronic form via e-mail from ITSCertificateManagement@standardbank.co.za

APPENDICES

9. CP’s Supported Under this CPS

9.1. Standard Bank Policy CA 11 Certificate & Certificate Policies

Standard Bank Public Key Operations TRUST Hierarchy Anchor defines and implements the Bank’s ROOT Certificate Authority. The Policy CA’s joins the Bank’s Trust Chain as an off-line Stand-alone CA, who’s certificate is signed by the ROOT CA.

There are no Certificate Policy loaded into the Policy CA 11 except the standard Microsoft Window 2003 PKI standard Certificate template to sign subordinate CA’s ***(“Issuing CA’s in this case”)***

9.1.1. Standard Bank Policy CA 11 Certificate

OID: 1.3.6.1.4.1.16543.401.11.1.1.1

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
Policy CA 11	11
Certificate	1
Version	1.1

Table 3 – Standard Bank PKO Policy CA 11 Certificate OID

9.1.2. Certificate DUMP:

9.1.2.1. V0.0

```
X509 Certificate:
Version: 3
Serial Number: 610b8ebd000000000002
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: 10/18/2007 9:49 AM
 NotAfter: 10/18/2022 9:59 AM
```

```
Subject:
    CN=Standard Bank Policy CA 11
    OU=IT Security
    OU=PKO Services
    O=Standard Bank Group
    L=JNB
    S=GP
    C=ZA
  Name Hash(sha1): 9cdc86e5faa3185a4f630cd8b95c10ea5f68bd3b
  Name Hash(md5): f270fc2a2041808efaf84a6ea73611e5

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 e3 fc f4 9b b0 df b8
    0010  be cd 26 9b d2 15 a0 97  a8 ec 61 40 1e 8f 4c ac
    0020  35 81 da ce 88 b2 80 42  d3 45 b8 a6 de e2 5a 63
    0030  64 b5 cf 13 97 bc 45 ee  3c e5 06 8e 3d 1d d3 1b
    0040  9e a3 3f ae fa db e4 67  96 e4 c7 90 32 46 b4 55
    0050  e6 b4 2b 9e 7b 74 12 a8  ae c9 0d f0 71 d5 e9 52
    0060  01 c8 e8 d4 93 5b fd 05  cf 2b ed ed 34 30 88 bd
    0070  64 3d 8a bc f5 c0 7e 7d  1e ba 30 8b ca 65 bb 7e
    0080  47 17 c1 7d 13 a0 08 de  c6 97 25 66 23 9b b7 af
    0090  1a 3a 5d f7 e7 e5 61 21  d1 0e 5c 08 a3 cf bc c7
    00a0  00 38 aa 0f 74 d7 fc 3a  46 dc 5f 9b 6f ba 83 78
    00b0  e3 a4 f9 cc 04 6a c1 bd  ef 19 8b aa da 94 c3 9b
    00c0  13 6b d5 a2 a6 3e 7b 36  31 3d bb 68 83 25 bd 30
    00d0  b4 7c 06 57 45 7f b8 53  f4 6e ea b2 88 1b a3 f6
    00e0  c4 a4 22 fd d9 e1 f1 82  36 e1 36 a2 e8 20 66 fe
    00f0  cb 32 8e fe 27 ac b2 b5  00 93 a0 0f 2a d3 0b 25
    0100  72 06 1f 33 7d 13 6c 83  67 37 19 22 99 f3 be 83
    0110  56 d4 7e c3 51 4e fe 08  33 ff 4e 49 21 29 85 89
    0120  ba 59 db 6d 00 65 94 d6  d0 ab 37 fe ef b2 10 be
    0130  83 ee 26 ea 9b d9 f5 ac  02 c8 ae 43 b8 8a 02 3d
    0140  23 a9 ee b3 c3 bc bf 5a  7b f1 ed 34 cd 58 3c cb
    0150  e0 20 7b 31 17 c3 eb 4f  33 d0 88 99 55 86 89 7c
    0160  60 de 14 e7 c5 b3 54 e0  09 e4 7d 9d ba c1 c4 2d
    0170  40 c0 f5 c1 8c 0c 51 d3  4d e7 4c 0f 88 6f 3d 75
    0180  8f 2a 91 cb 77 22 7b 18  02 35 e3 22 d5 05 7e bf
    0190  33 88 57 7c 0a b5 f9 cd  49 ef 39 be 33 ba 16 e4
    01a0  d7 60 a9 76 20 ae 1e 06  c2 7d 96 15 11 79 24 10
    01b0  c7 1a c1 20 ee f5 58 66  89 b3 f7 9c da 17 f1 43
    01c0  27 fc 32 b8 9c 68 c3 d7  55 31 5e 9e 71 5c 8f 8f
    01d0  96 2c 1a e1 e1 cc 5c a6  7f 57 3b 9a 56 7f 02 77
    01e0  83 8e fe 42 0d c0 97 6b  0b ca a1 64 97 65 e1 5f
    01f0  85 06 8a 51 2f f9 5b 86  0d 7b 39 b2 f8 6a a1 87
    0200  53 8c 9d 09 1a 4e be c4  0d 02 03 01 00 01
Certificate Extensions: 9
    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
        36 d7 9c 61 11 ab a9 53 f9 ad 24 08 21 c6 41 34 67 30 68 7a

    2.5.29.15: Flags = 0, Length = 4
    Key Usage
        Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (86)

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

    2.5.29.32: Flags = 0, Length = 54
    Certificate Policies
        [1]Certificate Policy:
             Policy Identifier=1.3.6.1.4.1.16543.401.11.2.2.1
             [1,1]Policy Qualifier Info:
                  Policy Qualifier Id=CPS
                  Qualifier:
                       http://pko.standardbank.co.za/PCA-11-CPSPage.htm

    1.3.6.1.4.1.311.20.2: Flags = 0, Length = c
    Certificate Template Name (Certificate Type)
        SubCA

    2.5.29.35: Flags = 0, Length = 18
    Authority Key Identifier
        KeyID=ff 5b 92 09 02 f7 b9 80 d7 e8 21 79 8e 8a 00 83 fd 1e cb a2

    2.5.29.31: Flags = 0, Length = 48
    CRL Distribution Points
        [1]CRL Distribution Point
             Distribution Point Name:
                  Full Name:
                       URL=http://pko.standardbank.co.za//Standard      Bank      ROOT      CA.crl
(http://pko.standardbank.co.za//Standard%20Bank%20ROOT%20CA.crl)

    1.3.6.1.5.5.7.1.1: Flags = 0, Length = 5e
    Authority Information Access
        [1]Authority Info Access
             Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
             Alternative Name:
                  URL=http://pko.standardbank.co.za//05766pkojnb0001_Standard   Bank   ROOT   CA.crt
(http://pko.standardbank.co.za//05766pkojnb0001_Standard%20Bank%2
0ROOT%20CA.crt)

Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
    Algorithm Parameters:
    05 00
Signature: UnusedBits=0
    0000  73 86 93 9c 82 99 46 da  89 29 2a 68 87 54 7e 02
    0010  28 18 ae 06 f8 6a f1 8c  ec 02 cb e0 a3 aa be 99
    0020  55 22 44 99 7e 02 2a 69  af e0 2d f6 01 2e 69 ce
    0030  4c d0 88 d5 1c af ed 89  37 16 32 b6 65 84 30 f5
    0040  d1 55 9e 19 37 ba 98 56  34 12 62 26 93 31 9a dc
    0050  c9 1d 1c d8 e2 11 03 48  d2 08 fa fd 41 88 22 3d
    0060  93 56 a3 eb 79 e7 ef c8  40 92 34 af 5f 10 ea de
    0070  ce 7e 25 6e 0f 41 6a 0a  52 21 4c 15 fa 69 ed ee
    0080  1a fd be 62 6a 9f 9c 41  00 5f 07 bf 28 22 30 30
    0090  b6 0c fa d0 a2 27 9a b8  2e fa 5a 39 aa 54 d6 f8
    00a0  e2 93 4c 22 24 b5 40 c7  01 75 04 fc 4e 5c 0f 25
    00b0  5b d0 2b 6e 85 97 42 76  d4 89 40 45 0b 58 f0 61
    00c0  69 8d e7 69 f9 e8 60 c5  f5 6f b0 04 15 0a 39 be
    00d0  44 0b e2 89 73 d0 5f b5  91 71 6b 5e a3 72 f3 54
    00e0  50 b3 b1 5c 24 21 2f 85  12 45 ef 8f 4e b8 1c 9a
    00f0  0c 2d 9e 49 6b 02 1c 46  f7 74 07 c3 31 fa 96 c5
    0100  90 72 2d b8 0d 89 af dc  15 d2 be 2d 25 c9 52 9b
    0110  94 4d a7 d9 b5 e2 84 83  20 e2 90 90 ee e6 56 bd
    0120  f2 07 f0 71 5a 42 b0 6d  8f 66 42 b8 65 f5 3f 31
    0130  4a af db 01 30 be ae 98  19 55 ef 7c 10 a4 ee 44
    0140  b3 80 ae 59 6c 7a 5b 8e  9e 81 31 31 db 85 5b a7
    0150  f6 8b d5 27 43 ae a7 51  02 1d c0 5e 5a d1 03 be
    0160  5a c3 bb ac d7 cd 7d 76  11 89 d9 4e ef 44 0f 46
    0170  16 c1 33 16 ca e3 1e 30  bb c2 f2 5c b3 86 d2 1a
    0180  4f 49 a0 93 a8 24 64 35  cc d0 0f 57 c2 d2 d0 16
    0190  ad 03 5a 38 c8 e4 6a d5  d5 18 9e 49 55 04 49 1b
    01a0  0a e0 65 dd 9a f1 03 f5  99 85 f5 2a 70 34 66 87
    01b0  80 35 db b6 3e 89 b4 9c  c7 5c 7f 9b df ad 70 15
    01c0  96 1a 9d bd ff 62 b0 3e  97 59 d6 62 35 9b a4 45
    01d0  ec 4f 93 fa e4 a6 79 79  fd 28 7c b9 dc f4 e2 d5
    01e0  87 de c2 5b 0c 8a f2 62  59 4c 4a eb bb 11 32 ae
    01f0  a5 09 d7 da 7a 8e 40 f7  58 31 48 bf 08 1e ea 99
Non-root Certificate
Key Id Hash(rfc-sha1): 9f c0 e8 69 ba 1d f3 f1 f4 a7 ea 52 1f 25 fd 09 74 91 c4 87
Key Id Hash(sha1): 36 d7 9c 61 11 ab a9 53 f9 ad 24 08 21 c6 41 34 67 30 68 7a
Key Id Hash(md5): 1ec48c6abe99f62d556d5479a39f21bd
Key Id Hash(sha256): 46006ec99aa324a209afe79c549985a8c82e139609db3c844199cacb2298f7f1
Cert Hash(md5): d7 0e df 5d 6d e2 87 a3 23 bb 17 d9 be cb 67 49
Cert Hash(sha1): 05 12 07 72 4f b8 96 2b 23 02 2f a0 a0 3d 8c a6 90 10 5c d4
Cert Hash(sha256): 472cfb65ba6c5c46b664ea94068e252cf52f05a940c690b08d41f6bb4287f5cc
Signature Hash: 0a83d780a7ab0bb46e5e71652ca4684a60df76fe
CertUtil: -dump command completed successfully.
```

9.1.2.2. V1.0

```
X509 Certificate:
Version: 3
Serial Number: 57000000058d1c55e8247398b0000100000005
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: 2016/12/27 01:16 PM
 NotAfter: 2038/12/27 01:26 PM

Subject:
    CN=Standard Bank Policy CA 11
    OU=IT Security
    OU=PKO Services
    O=Standard Bank Group
    L=JNB
    S=GP
    C=ZA

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 e3 fc f4 9b b0 df b8
    0010  be cd 26 9b d2 15 a0 97  a8 ec 61 40 1e 8f 4c ac
    0020  35 81 da ce 88 b2 80 42  d3 45 b8 a6 de e2 5a 63
    0030  64 b5 cf 13 97 bc 45 ee  3c e5 06 8e 3d 1d d3 1b
    0040  9e a3 3f ae fa db e4 67  96 e4 c7 90 32 46 b4 55
    0050  e6 b4 2b 9e 7b 74 12 a8  ae c9 0d f0 71 d5 e9 52
    0060  01 c8 e8 d4 93 5b fd 05  cf 2b ed ed 34 30 88 bd
    0070  64 3d 8a bc f5 c0 7e 7d  1e ba 30 8b ca 65 bb 7e
    0080  47 17 c1 7d 13 a0 08 de  c6 97 25 66 23 9b b7 af
    0090  1a 3a 5d f7 e7 e5 61 21  d1 0e 5c 08 a3 cf bc c7
    00a0  00 38 aa 0f 74 d7 fc 3a  46 dc 5f 9b 6f ba 83 78
    00b0  e3 a4 f9 cc 04 6a c1 bd  ef 19 8b aa da 94 c3 9b
    00c0  13 6b d5 a2 a6 3e 7b 36  31 3d bb 68 83 25 bd 30
    00d0  b4 7c 06 57 45 7f b8 53  f4 6e ea b2 88 1b a3 f6
    00e0  c4 a4 22 fd d9 e1 f1 82  36 e1 36 a2 e8 20 66 fe
    00f0  cb 32 8e fe 27 ac b2 b5  00 93 a0 0f 2a d3 0b 25
    0100  72 06 1f 33 7d 13 6c 83  67 37 19 22 99 f3 be 83
    0110  56 d4 7e c3 51 4e fe 08  33 ff 4e 49 21 29 85 89
    0120  ba 59 db 6d 00 65 94 d6  d0 ab 37 fe ef b2 10 be
    0130  83 ee 26 ea 9b d9 f5 ac  02 c8 ae 43 b8 8a 02 3d
    0140  23 a9 ee b3 c3 bc bf 5a  7b f1 ed 34 cd 58 3c cb
    0150  e0 20 7b 31 17 c3 eb 4f  33 d0 88 99 55 86 89 7c
    0160  60 de 14 e7 c5 b3 54 e0  09 e4 7d 9d ba c1 c4 2d
    0170  40 c0 f5 c1 8c 0c 51 d3  4d e7 4c 0f 88 6f 3d 75
    0180  8f 2a 91 cb 77 22 7b 18  02 35 e3 22 d5 05 7e bf
    0190  33 88 57 7c 0a b5 f9 cd  49 ef 39 be 33 ba 16 e4
    01a0  d7 60 a9 76 20 ae 1e 06  c2 7d 96 15 11 79 24 10
    01b0  c7 1a c1 20 ee f5 58 66  89 b3 f7 9c da 17 f1 43
    01c0  27 fc 32 b8 9c 68 c3 d7  55 31 5e 9e 71 5c 8f 8f
    01d0  96 2c 1a e1 e1 cc 5c a6  7f 57 3b 9a 56 7f 02 77
    01e0  83 8e fe 42 0d c0 97 6b  0b ca a1 64 97 65 e1 5f
    01f0  85 06 8a 51 2f f9 5b 86  0d 7b 39 b2 f8 6a a1 87
    0200  53 8c 9d 09 1a 4e be c4  0d 02 03 01 00 01
Certificate Extensions: 10
    1.3.6.1.4.1.311.21.1: Flags = 0, Length = 3
    CA Version
        V1.0

    1.3.6.1.4.1.311.21.2: Flags = 0, Length = 16
    Previous CA Certificate Hash
        05 12 07 72 4f b8 96 2b 23 02 2f a0 a0 3d 8c a6 90 10 5c d4

    2.5.29.14: Flags = 0, Length = 16
    Subject Key Identifier
        36 d7 9c 61 11 ab a9 53 f9 ad 24 08 21 c6 41 34 67 30 68 7a

    2.5.29.32: Flags = 0, Length = 55
    Certificate Policies
        [1]Certificate Policy:
             Policy Identifier=1.3.6.1.4.1.16543.401.11.2.2.2
             [1,1]Policy Qualifier Info:
                  Policy Qualifier Id=CPS
                  Qualifier:
                       http://pko.standardbank.co.za/PCA-11-CPSPage.htm

    1.3.6.1.4.1.311.20.2: Flags = 0, Length = c
    Certificate Template Name (Certificate Type)
        SubCA

    2.5.29.15: Flags = 0, Length = 4
    Key Usage
        Digital Signature, Certificate Signing, Off-line CRL Signing, CRL Signing (

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

    2.5.29.35: Flags = 0, Length = 18
    Authority Key Identifier
        KeyID=ff 5b 92 09 02 f7 b9 80 d7 e8 21 79 8e 8a 00 83 fd 1e cb a2

    2.5.29.31: Flags = 0, Length = 48
    CRL Distribution Points
        [1]CRL Distribution Point
```

```
             Distribution Point Name:
                  Full Name:
                       URL=http://pko.standardbank.co.za//Standard%20Bank%20ROOT%20

    1.3.6.1.5.5.7.1.1: Flags = 0, Length = 5e
    Authority Information Access
        [1]Authority Info Access
             Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
             Alternative Name:
                  URL=http://pko.standardbank.co.za//05766PKOJNB0001_Standard%20Ban
rt

Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.11 sha256RSA
    Algorithm Parameters:
    05 00
Signature: UnusedBits=0
    0000  5a 27 fc 5d 9f ae a8 26  01 08 fb 97 23 d1 79 de
    0010  79 35 49 12 3f 96 97 3d  da d6 af bb 0d 47 9a 8f
    0020  68 7f 2d fb aa 90 ae 0d  7e 7d 2e 35 3f 7f 20 b8
    0030  3e e1 44 d1 01 ba e6 d2  c1 6c ea cc 5d bb 3e 8f
    0040  e8 7c 9c 82 af 62 9b e0  62 e4 2e 41 77 8a 8c c3
    0050  16 1f 25 7d cc 4d 9d 8a  e3 ad b2 87 67 c8 26 89
    0060  30 8c b9 61 9f 6b 1f 8e  cb c4 0f 6e 6a 80 fe cd
    0070  1b 24 d2 9f 72 74 a5 1b  d4 27 b2 f6 cd 1f f6 5d
    0080  6f 30 06 d6 7c 91 40 1a  51 7e 9f 9b 7b 90 80 5a
    0090  fe a1 9a c7 86 1b 72 48  6e 9c 7d fe 45 11 c2 b3
    00a0  61 88 00 a9 30 70 bb da  c5 a8 e0 32 a5 c0 20 1b
    00b0  c2 0a 55 0c 86 29 1b 5c  a0 3f 4c 6f 22 e6 3f ad
    00c0  1a f9 87 5f 62 31 eb 59  5a 93 dc 46 ba f6 e9 c8
    00d0  20 ac 01 2e 5c 42 fc 7e  ee 79 7a 5e 3c e3 47 e7
    00e0  37 d9 7f c1 3c 5a e3 05  db b3 c0 77 41 44 c4 5a
    00f0  4b bb 65 63 2d 85 b0 65  2d 60 bd 21 52 be db 28
    0100  54 7f 5f f8 0f f9 b9 c0  2e c1 0d 2c 69 b0 32 df
    0110  e8 a7 53 d9 61 44 ed 44  8e 61 c9 d5 47 2e 66 56
    0120  03 12 43 ac f3 fd 79 d7  88 e8 d1 c1 99 1c e9 39
    0130  81 7b 96 da 5a 13 a2 a9  92 2f 9e 49 97 2e a9 15
    0140  35 69 43 10 27 1c 65 6d  18 6d 47 7d 16 e2 3e 6c
    0150  e2 19 20 41 34 d6 d9 db  64 d5 85 19 d9 92 cc 84
    0160  22 01 96 db 98 75 8d f1  1f bf 45 25 25 c8 3a 6f
    0170  53 ec e7 ff ea b2 67 52  58 4d fe 54 c2 7b 10 35
    0180  69 1d b1 8c d6 c4 21 d0  16 12 e6 09 ea 4f 41 df
    0190  c7 25 a7 73 c9 06 91 7a  ca 3e 4a 1d e6 15 63 b9
    01a0  ed 55 2d 37 04 23 2c d7  17 12 3a 6f 43 3c 65 92
    01b0  68 9e 93 e1 29 e7 fc 89  45 98 a8 81 b0 55 bb 8c
    01c0  a4 3a 97 76 e5 8d a1 f5  c7 6c 7c 35 65 6e 13 7d
    01d0  e5 f6 86 d0 7e 2e 8b 72  59 e3 f3 36 d4 e7 5c 57
    01e0  10 31 b3 94 ae b0 6e 20  32 aa 80 0c 7e 30 de 03
    01f0  88 50 eb 84 eb 42 da 02  c3 ba d8 d2 12 63 52 2f
Non-root Certificate
Key Id Hash(rfc-sha1): 9f c0 e8 69 ba 1d f3 f1 f4 a7 ea 52 1f 25 fd 09 74 91 c4 87
Key Id Hash(sha1): 36 d7 9c 61 11 ab a9 53 f9 ad 24 08 21 c6 41 34 67 30 68 7a
Cert Hash(md5): 57 ad c9 1e e8 68 a1 27 e7 23 64 c9 d6 7e 20 00
Cert Hash(sha1): 34 10 9b 84 e6 33 39 c8 44 11 fd ec 27 d7 25 fc 13 2f 65 24
CertUtil: -dump command completed successfully.
```

9.2. Standard Bank Policy CA 11 Configuration

Root Certificate Authority	
NetBIOS Name	05766PKOJNB0011
CA Unique Name	Standard Bank Policy CA 11
Version Type	2012 Certificate Server (Standalone SubordinateCA)
Current Certificate Version	1.0
	Install certificate from a PKCS#7 text file from the Standard Bank Root CA
CA Lifetime	22 Years
CA Key Length	2048
CRL Validity Interval	367 Days
CRL Publishing Interval	365 Days
CSP	nCipher Enhanced Cryptographic Provider
CSP PKI Algorithm	RSA
CSP HASH Algorithm	SHA-256
CRL Locations:	LDAP to Active Directory and HTTP
Operating System	Windows Server 2012 Standard Edition R2
Workgroup	SBICPKO

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

10. GLOSSARY

10.1. 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

10.1. 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.)

10.2. 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