CA 113/4 Certificate Practice Statement

Public Key Operations

Standard Bank of South Africa

Standard Bank

Inspired. Motivated. Involved.

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

CA 113/4 V4.1 Certificate Practice Statement, Public Key Operations, Version 1.2 Draft

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

Prepared by **Moris Halevi**

Wednesday, 2 January 2019 - 8:18:03 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
5th October 2006	Moris Halevi	1.2	Updates for compliance with WEBTRUST & RFC 2527 Framework
18th October 2006	Moris Halevi	1.7	Revised Draft work in progress
13th April 2007	Moris Halevi	2.0	Working Draft R2
20th April 2007	Moris Halevi	2.1	Proof-reading Final Draft 1st Pass
23th April 2007	Moris Halevi	2.1	Proof-reading Final Draft 2nd Pass
31st January 2014	Moris Halevi	3.0	PKO 2013 Migration - refresh
21st April 2015	Moris Halevi	4.0	PKO 2015 Updates & Removed Confidential
11th June 2015	Moris Halevi	4.1	Reviewer added
10th December 2017	Londani Mulaudzi	4.2	Removed WEBTRUST Reference, CA version infrastructure update and update for RFC 3647
02nd January 2018	Londani Mulaudzi	4.2	Remove confidential information

Reviewers

Name	Version approved	Position	Date
Lynette Schulz	4.0	Head: Cryptography Services	11th July 2015
Zukiswa Mahlawe	4.2	Specialist: Cryptography	8th January 2018

Table of Contents

Tables

1 INTRODUCTION

1.1 Overview

The main goal of the Standard Bank Certification Authority is to offer a common policy repository for all Certificate type(s) that has common ground within the Standard Bank. The Standard Bank certification services is 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 CA's, which each will fulfil the requirements of its particular community.

Each CA will operate under its own CPS. Before a 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 Certification Authority 111 in issuing and managing digital certificates for its end-user entities that are for Standard Bank internal use only. The CA 113/4 is certified by the Policy CA 11, issues 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" and Standard Bank Policy CA 11 as link to the "Trust Anchor" within the Standard Bank PKO hierarchy, including the technology, operational processes and physical infrastructure, is not compromised by introduction of the Standard Bank CA 113/4 into the Standard Bank Trust Hierarchy.
2. Describe how the Standard Bank Issuing CA 113/4 meets the requirements of each Certificate Policy under which certificates are issued to the various internal entities by the Standard Bank PKO.
3. Set out the minimal requirements for its end-user entities for the management and administrative practices used to protect the trustworthiness of the issued certificates and the whole Standard Bank PKO.
4. Act as an input to audit activities. One audit activity is to validate that the Issuing CA 113/4 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 [1]. 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 Issuing CA 113/4 issues certificate in accordance with this CPS dated “2019-01-02” to its end-users and establishes the ***“TRUST chain”*** to Standard Bank’s ROOT CA through Standard Bank’s Policy CA 11.

CPS Name: Standard Bank Issuing CA 113/4 Certificate Practice Statement OID: 1.3.6.1.4.1.16543.401.113.2.1.7 and 1.3.6.1.4.1.16543.401.114.2.1.7

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
Issuing CA 111	113 or 114
CPS	2
Version	2.1

Table 1 – Standard Bank PKO ISSUING CA 113-4 CPS OID

1.3 COMMUNITY AND APPLICABILITY

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

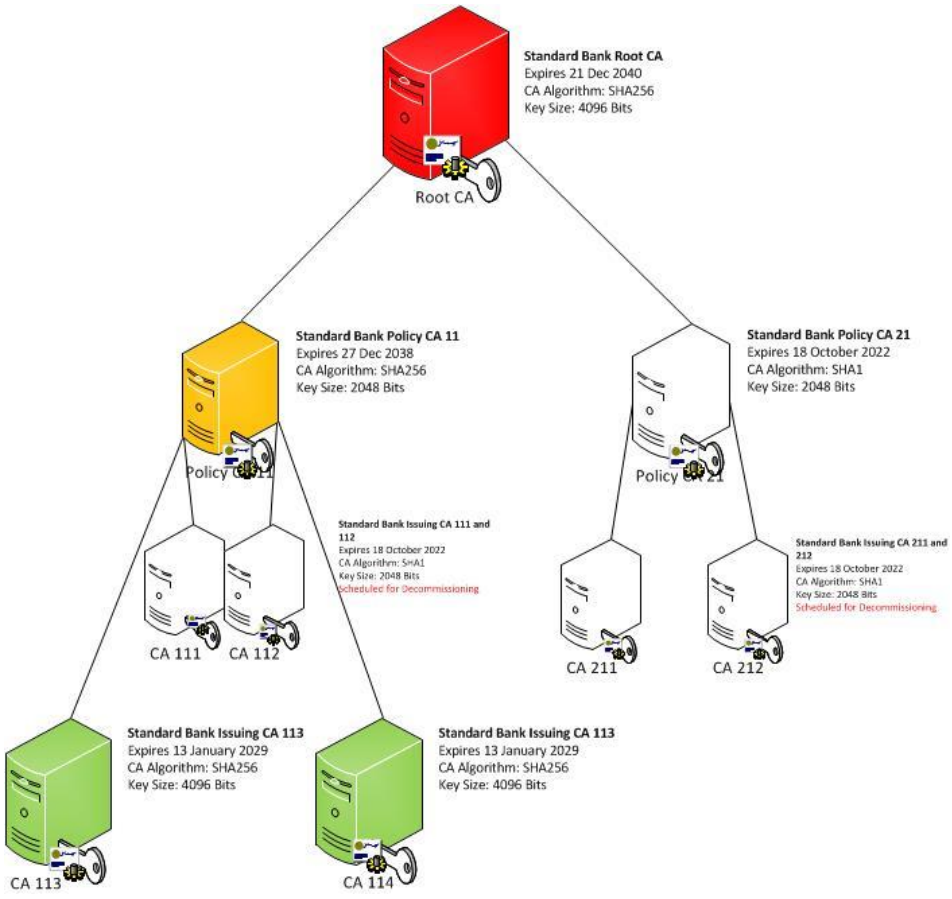

Table 2 – Standard Bank PKO High-Level Architecture

1.3.1 Certification authorities

The purpose of a Certification Authority (CA) is to attest to the binding between an entity and a public key. Although this CPS is only applicable to the Issuing CA 113/4 the description of its ROOT & Policy 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 segregated by splitting in to pieces and stored in safes at different locations.

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 **Internal Policy CA *"PCA 1x"*:** 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 **External Policy CA "PCA 2x":** 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 Issuing CA 113/4 is certified by the Policy CA to 11 to perform certificate services to issue ***"Internal Use ONLY Certificates"***. The Standard Bank Root CA Certificate Policies and the Policy CA 11 certification agreements ensure that the Issuing CA 113/4 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 Registration Authority (RA) is to register End Entities, on behalf of its parent CA. The RA is needed for physical identification/authentication of End Entities. These RA MUST not be permitted to issue certificates but process Certificate requests

A registration authority (RA) is

- an individual or
- a group of people appointed by an organization or an organizational unit

trusted by the CA 111, serving as a contact point for registration of new end entities, i.e. end entities that want to have a certificate issued. The RA does check the certificates requester's identity in an appropriate way. The RA MUST sign an agreement with the issuing CA 111, stating the obligation to adhere to the agreed procedures. The practices used for registration and certification of End Entities are documented in the Appendix A. This CPS must be approved by the Standard Bank PKO Authority ("PA") prior to the certification of the Issuing CA 111, and accredited by an independent assessor.

1.3.5 End entities

The Standard Bank Issuing CA 113/4 will sign certificates issued to natural people its employees, contractors

for secure eMail, EFS ***("Encrypted File System")*** and issued for computer entities in banks asset register(e.g. a computer, a router or an application), capable of performing cryptographic operations.

1.3.6 Relying Parties

The Relying Parties in the scope of this CPS are parties which rely on a Standard Bank issued certificate, the certificates issued to this CA, including the certificate status and the repository.

1.3.7 Applicability

One of the purposes of this policy is to promote a wide use of public-key certificates in many different applications. In order to promote interoperability this policy strongly encourages CA to support S/MIME for securing e-mail exchanges. It is also suggested that IPsec (to offer network layer security) and SSL/TLS (to offer transport layer security for protecting application protocols like HTTP, Telnet, FTP) SHOULD be supported. It‘s important to notice that this policy in principle doesn‘t want to put a priori limitation to the use of the certificates except for the case in which certificates are used in a way that is prohibited by the law of the countries where the issuing CA are established. However in order to evaluate if certificates issued under this policy are suitable for a certain application the chapter 2 about —General provisions“ has to be read carefully and fully understood. Certificate Policies that are applicable to the practices described in this document are listed at Appendix A.

All Certificates issued by the Standard Bank Issuing CA 113/4 are supported by this CPS. The Certificate Policies supported by the Standard Bank Issuing CA 113/4 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 agent of Standard Bank TRUST Hierarchy.

1.3.8.1 Restricted Applications

No stipulation

1.3.8.2 Prohibited Applications

Standard Bank CA 113/4 certification services and all other certification services within the Standard Bank PKO are not intended, designed, or authorised for use beyond the financial industry interface and processes.

1.4 CONTACT DETAILS

1.4.1 Specification administration organization

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

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

1.4.2 Contact person

Questions concerning this CPS should be addressed to:

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

In order to obtain an evaluation of CPS suitability for the policy, conforming CAs have to contact the person mentioned in 1.4.2. See section 8.3 for details about CPS approval procedures.

2 GENERAL PROVISIONS

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

2.1 OBLIGATIONS

The Standard Bank Issuing CA 113/4 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 Issuing CA 113/4 in the Standard Bank PKO.

2.1.1 CA obligations

2.1.1.1 Issuing CA 113/4 Obligations

The Issuing CA 113/4 meets its obligations under this CPS by:

1 Adhering to the practices described within this CPS.
2 Publishing its CA Certificate signed by Policy CA 11 for relying parties.
3 Maintain records required demonstrating trustworthy operations and compliance with this CPS.
4 handle certificate requests and issue new certificates:
   a. accept and confirm certification requests from entities requesting a certificate according to the agreed procedures contained in this policy and in the CPS
   b. authenticate entities requesting a certificate, possibly by the help of separately designated RAs
   c. issue certificates based on authenticated entities' requests
   d. send notification of issued certificate to requesters
   e. handle certificate revocation requests and certificate revocation
   f. accept and confirm revocation requests from entities requesting a certificate to be revoked according to the agreed procedures contained in CPS/policy
   g. authenticate entities requesting a certificate to be revoked
5 Publish issued Certificates in a nominated directory.
6 Ensure 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 Issued certificates and publishing Certificate status information in a CRL to a nominated directory.
8 Publish updates to this CPS and applicable CP as soon as a new version is available.

2.1.1.2 Certified Entities Obligations

Entities Certified by this Issuing CA 113/4 fulfil their obligations under this CPS by:

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 Issuing CA 113/4 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 Issuing CA 113/4 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

2.1.2 RA obligations

An RA of CA 113/4 SHALL operate as a RA service and the compliance includes:

- to authenticate the identity of the subject
- to validate the connection between a public key and the requester identity including a suitable proof of possession method
- to confirm such validation versus the CA
- to adhere to the agreement made with the CA

2.1.3 Subscriber obligations

The subscribers of Issuing CA 113/4 SHALL behave according to this CPS and the compliance includes:

- to read and adhere to the agreed procedures
- to properly protect its private key, being the only possessor if the subscription refers to an individual person. In the case of a private key of a hardware or software component the protection and the control of the key MUST be done on an accepted Security Module
- to accept that in the usage of public key certificates CA's liability is limited according to what is specified by section 2.2
- to authorise the treatment and conservation of personal data
- to notify immediately the CA upon private key compromise

2.1.4 Relying party obligations

A relying party MUST be familiar with the CPS and this policy before drawing any conclusion on how much trust he can put in the use of a certificate issued by CA 113/114. A relying party MUST check CRLs when validating the use of a certificate. Moreover a relying party MUST ONLY use the certificate for the proscribed applications and MUST NOT use the certificates for forbidden applications. Relying Parties fulfil their obligations under this CPS by:

1. Obtaining a trustworthy copy of the Issuing CA 113/114's certificate signed by the Policy CA 11.
   - Exercising reasonable judgment 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 113/114, 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 Issuing CA 113/4 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 Issuing CA 113/4 makes no other warranties or promises and has no further obligations to the certified entities or Relying Parties, except as set forth under this CPS, furthermore the core of relation criteria is defined in the contractual employment agreement between the bank and natural people working, contracting or supplying services to the bank and in the ownership of non-natural entities (such as Computers, applications etc.)

Considering that this policy is primarily established to promote the adoption of certificates as a mean to increase computer and network security in a broad variety of applications, the subsection 1.3.4 states that there are no a priori limitation to applicability of certificates issued under this policy. If no limitation is put on certificate applicability, this policy suggests that CA liability will be restricted to the guarantee of making the necessary controls to verify the identity of every requester as described in the CPS and to the adoption of the minimal security measures needed to protect CA's private key. In every case the complete list of accepted liabilities MUST be specified in the CPS.

2.2.2 Disclaimers

Except for express warranties stated in this CPS, Standard Bank Issuing CA 113/4 disclaims all other warranties, promises and other obligations.

In no event shall Standard Bank Issuing CA 113/4 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 Issuing CA 113/4 has been advised of the possibility of such damages.

2.2.3 Loss Limitations

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

2.2.4 Other exclusions

Standard Bank Issuing CA 113/4 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 Issuing CA 113/4
- 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 Issuing CA 113/4
- 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 Issuing CA 113/4 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 Issuing CA 113/4 an agent, fiduciary, trustee, or other representative of the 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 Issuing CA 113/114.

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

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

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

2.4.3 Dispute resolution procedures

2.4.3.1 Hierarchy of Certificate Policy

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

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

2.4.3.2 Process

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

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

2.5 FEES

2.5.1 Certificate issuance or renewal fees

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

2.5.2 Certificate access fees

No stipulation

2.5.3 Revocation or status information access fees

No stipulation

2.5.4 Fees for other services such as policy information

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

2.5.5 Refund policy

No stipulation.

2.6 PUBLICATION AND REPOSITORY

2.6.1 Publication of Root CA information

The following information shall be made available in a repository to all parties that use Standard Bank Issuing CA 113/4 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 shall be in accordance with section 8. Certificates shall be published as soon as they are issued. Published CRL's (Certificate Revocation Lists) shall have a finite validity period. Publication of a new CRL will be done before expiration of the subsequent CRL. The lifetime of a CRL will be in accordance with section 4.4.9 of this CPS.

2.6.3 Access controls

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

2.6.4 Repositories

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

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

2.7 COMPLIANCE AUDIT

The purpose of the audit is to verify the quality of the services provided by the Standard Bank Issuing CA 113/114, 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 Issuing CA 113/114.
- 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 Issuing CA 113/114 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 shall 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 Issuing CA 113/4 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 Issuing CA 113/4 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 to identify and authenticate a certificate requester to the CA 113/4 or one of its RA's before certificate issuance. It also describes how parties requesting rekey or revocation are authenticated. This component also addresses naming practices, including name ownership recognition and name dispute resolution.

3.1 INITIAL REGISTRATION

3.1.1 Types of names

All Certificates require a distinguished name that is in compliance with the X.500 standard for Distinguished Names. Each Certificate Policy states requirements for naming of a CA 113/4 issued with certificates under that policy. The CA 113/4 proposes and the PA approves the distinguished name.
The naming attributes of the subscriber to be requested to identify and authenticate the requester depend on the type of certificate that the subscriber requires. In the choice of the types and format of names used in the fields of the certificate policy is conforming to RFC 3647 [5].

3.1.2 Need for names to be meaningful

In all Cases, the name of CA 113/4 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 Issuing CA 113/4 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 Issuing CA 113/4 generates and stores its 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 Policy CA 11 verifies the signature with the public key listed in the request for certification.

3.1.8 Authentication of organization identity

This CPS supports only 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 an 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.

In many cases public-key certificates constitute a mean to guarantee strong cryptographic authentication of communicating entities. Bearing in mind this premise, PKO policy states that authentication of individual identity is REQUIRED. The RECOMMENDED method of authentication requires that individual presents personally to

the authenticating CA or RA showing suitable identification documents. Other methods like videoconference MAY be adopted. If the subject to be certified is a software component the person who submits the request MUST prove that he has the necessary authorisation The exact procedure MUST be detailed in this CPS.

3.2 ROUTINE REKEY

This policy doesn't mandate any compulsory rekey. After certificate expiration, the CA MAY issue a new certificate both for the same key or for a new key. The rekey authentication MAY be accomplished with the same procedure indicate in section 3.1 for initial registration or using digitally signed requests. These requests MUST be sent to the CA before certificate expiration.

This CA MAY issue more than one certificate for the same key, furthermore this CA 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. A public key whose certificate has been revoked for private key compromise MUST NOT be recertified. The public key MAY be re-certified if the revocation is only due to certificate suspension. In the latter case the rekey authentication MAY be accomplished with the same procedure indicated in section 3.1 for initial registration or using digitally signed requests. These requests MUST be sent to the CA before certificate expiration.

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 ***("Issuing CA 113/4 Operations Guide")*** to the Issuing CA 113/4

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 Issuing CA 113/4 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 Issuing CA 113/4 delivers the required level of trustworthiness. If this validation yields a satisfactory result the PA will send a subscriber agreement to the Issuing CA

Upon receipt of the signed subscriber agreement the PA will settle 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 Issuing CA 113/114.

At the Issuing CA 113/4 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 Issuing CA 113/4 indicates a complete and final approval of the certificate application by the Issuing CA 113/4.

The issued certificate will be handed over to the Issuing CA administrator. The Issuing CA 113/4 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 ***("Issuing CA 113/4 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 Issuing CA 113/4 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 Issuing CA 113/4 will be notified of the successful installation and a copy of the creation ceremony will be sent to the Issuing CA 113/4.

By accepting a certificate, the Issuing CA agrees:

- to be bound by the continuing responsibilities, obligations and duties imposed on him by the subscriber agreement, the CP and this CPS
- no unauthorised person has ever had access to the Issuing CA's private key.
- all information given by the Issuing CA to the Issuing CA 113/4 and included in the certificate is true

4.4 CERTIFICATE SUSPENSION AND REVOCATION

The Issuing CA 113/4 is responsible for issuing and publishing CRL's. The Issuing CA 113/4 shall update its CRL to reflect changes in revocation status and must issue timely CRL's.

4.4.1 Circumstances for revocation

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

Examples are:

- An improper or faulty issue of a Certificate is discovered.
- Material Certificate information becomes inaccurate
- The 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 subscriber agreement
- 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 Issuing CA 113/4 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 Issuing CA 113/4
- 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 shall be requested promptly after detection of a compromise or any other event giving cause for revocation.

The Issuing CA must immediately notify the Issuing CA 113/4 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 Issuing CA 113/4

In writing Authentication of the revocation request shall meet the requirements in 3.4 The Issuing CA 113/4 shall archive all revocation requests, the cause for revocation, the means of authenticating the request and the resulting actions taken by the Issuing CA 113/4. To process a revocation request:

1 The Issuing CA 113/4 authenticates the revocation request
2 The Issuing CA 113/4 makes the arrangements for the key-holders attendance
3 The Issuing CA 113/4 revokes the Certificate.
4 The Issuing CA 113/4 submits an updated CRL to the repository, including the revoked certificate.
5 The Issuing CA 113/4 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 PolicyCA owning a revoked certificate must securely destroy all instances of the private key.

4.4.4 Revocation request grace period

No stipulation.

4.4.5 Circumstances for suspension

No stipulation.

4.4.6 Who can request suspension

No stipulation.

4.4.7 Procedure for suspension request

No stipulation.

4.4.8 Limits on suspension period

No stipulation.

4.4.9 CRL issuance frequency

The Issuing CA 113/4 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 Issuing CA 113/4 will immediately issue and publish a replacement CRL. The previous CRL will be deleted from the directory.

Issuing CA 113/4 will ensure that a CRL is issued prior to the expiry of the previous CRL, to ensure that there is always a current available CRL, even in the event of delays in CRL's propagating through to relying parties.

4.4.10 CRL checking requirements

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

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

4.4.11 On-line revocation/status checking availability

No stipulation.

4.4.12 On-line revocation checking requirements

No stipulation.

4.4.13 Other forms of revocation advertisements available

No stipulation.

4.4.14 Checking requirements for other forms of revocation ads

No stipulation.

4.4.15 Special requirements regarding key compromise

No stipulation.

4.5 SECURITY AUDIT PROCEDURES

The security audit procedures in this section are valid for the Issuing CA 113/4 system and software components which may affect the outcome of the certificate issuing processes and the CRL.

Cryptographic tokens used in the Issuing CA 113/4 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 Issuing CA 113/4 system shall log, for audit purposes:

- All physical access to Issuing CA 113/4 Strong Room
- ISSUING CA 113/4 server start-up, shutdown and take-down
- ISSUING CA 113/4 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 ISSUING CA 113/4 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 shall be 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 shall be retained for the standard archival period as defined in 4.6.2.

4.5.4 Protection of audit log

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

The configuration of the offline Issuing CA 113/4 which includes CA application audit log, operating system generated logs and essential configuration files are written to CD-ROM before the Issuing CA 113/4 is returned to its safe.

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

4.5.5 Audit log backup procedures

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

4.5.6 Audit collection system (internal vs. external)

No stipulation.

4.5.7 Notification to event-causing subject

No stipulation

4.5.8 Vulnerability assessments

No stipulation

4.6 RECORDS ARCHIVAL

4.6.1 Types of event recorded

The records shall include all relevant evidence in the Issuing CA 113/4's possession including:

- Configuration files of the Issuing CA 113/4 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 Issuing CA 113/4.
- 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 shall be retained and protected against modification or destruction for at least 30 years from the date of archival, unless applicable law or regulations require a longer period.

4.6.3 Protection of archive

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

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

4.6.4 Archive backup procedures

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

Long term storage of records is accomplished on WORM media.

4.6.5 Requirements for time-stamping of records

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

4.6.6 Archive collection system (internal or external)

Internal

4.6.7 Procedures to obtain and verify archive information

The Issuing CA 113/4 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 Issuing CA 113/4 shall make documentation available that demonstrates the Issuing CA 113/4's compliance with section 2.7 of this CPS.

The Issuing CA 113/4 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 Issuing CA 113/4 key changeover procedures in the "Issuing CA 113/4 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 Issuing CA 113/4 will be suspended and the Issuing CA 113/4 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")***.

PKO operations have the responsibility of bringing up the ISSUING CA 113/4 within 24 hours from notice or disaster. The Issuing CA 113/4 is replicated on Issuing CA 114 that performs the same set of responsibilities. As the Issuing CA's 113 & 114 are physically located at different sites and they act as fail-over backup for each other.

DR scenario for ISSUING CA 111/2 and recovery process is defined in Standard Bank W/Intel Server DRP guidelines.

4.8.2 Entity Public Key is revoked

In the event of the need for revocation of the Issuing CA 113/4's public key, the CA must:

- immediately notify the PA
- Inform its Subordinate Issuing CA's.
- The Issuing CA 113/4 certificate must be removed from all relying parties trust lists

The Issuing CA 113/4 will be brought down and a new Issuing CA 113/4 key generation process will occur. Certificates issued prior to the revocation shall be re-signed.

4.8.3 Entity Key is compromised

If an incident occurs resulting in the Issuing CA 113/4 private key being compromised, the Issuing CA 113/4 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 Issuing CA 113/4 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 Issuing CA 113/4 to protect their operations.

For detailed description of security architecture please refer to ***"PKI Design"*** and for security access protocols please refer to ***"Issuing CA 113/4 Deployment Guide".***

All the processes and protocols are also defined in specific worksheets that act as route maps to deploy then use the ISSUING CA 113/4. 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 ISSUING CA 113/4.

5.1 PHYSICAL SECURITY CONTROLS

Physical security controls shall be implemented to control access to the Issuing CA 113/4's hardware, software, data and tokens.

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

The Standard Bank Issuing CA 113/4 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 shall be 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 Issuing CA 113/4 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 Issuing CA 113/4 shall be 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 under contract to Standard Bank, and it:

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

2 Has an appropriate level of physical security in place.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles for CA's

To ensure that one person acting alone cannot circumvent safeguards, responsibilities at a Issuing CA 113/4 system need to be attended by multiple roles and individuals. Each account on the Issuing CA 113/4 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 Issuing CA 113/4 equipment according to defined rules
- Generating, distributing, and otherwise managing CRL's
- Administrative functions associated with maintaining the Issuing CA 113/4 database and assisting in compromise investigations.

System Administrator (SA)

- Retrieving Issuing CA 113/4 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 Issuing CA 113/4'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 shall be done at least with each Issuing CA 113/4 startup

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 shall be 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 Issuing CA 113/4 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 Issuing CA 113/4'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. The Issuing CA 113/4 cryptographic keys are generated in FIPS 1402. Level 3 Hardware Security Modules.

End entities cryptographic keys are locally generated by their application (WIDGETs) during the requesting process. This policy suggests the adoption of the former procedure for signing key pair to be used for non-repudiation purposes. The latter procedure MAY be adopted for encryption key pair or bulk authentication key pair.

6.1.1 Key pair generation

The Issuing CA 113/4 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 Issuing CA 113/4 to undertake adequate measures to ensure that all public keys are unique within its domain before certificate binding takes place.

6.1.2 Private Key delivery to entity

All Issuing CA's and subscribers at trusted roles must generated their own key-pair, there is no key delivery. The subscriber entities MUST generate their own key pair. It is important to notice that the issuing CA will not generate Key-Pair on behalf of its subscribers.

6.1.3 Public Key delivery to certificate issuer

The Issuing CA 113/4 public key will be delivered on diskette to the (offline) Policy CA 11 for certification. Issuing CA 113/4 Key pairs of trusted roles are created in the protected environment of the Issuing CA 113/4.

For individual certification, the each entity SHALL submit a certification request containing the public key, locally generated, to the CA/RA.

The Issuing CA 113/4 supports at least PKCS#10 and SPKAC formats, and optionally MAY support other ones. If the public key is not generated by the entity in the presence of the CA/RA staff then the CA WOULD NOT accept formats that do not provide proof of possession.

6.1.4 Issuing CA 113/4 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 ***("Finger Print")*** 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.

6.1.5 Key sizes

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

6.1.5 Public key parameters generation

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

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

6.1.6 Parameter quality checking

No stipulation.

6.1.7 Hardware/software key generation

The Issuing CA 113/4 and all other PKO entity keys are generated in Hardware Security Modules (HSMs).

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

The purposes for which a key can be used MAY be restricted by the CA through the KeyUsage extension in the certificate. This is a field that indicates the purpose for which the certified public key is used.

Certificates issued under this policy MUST have the KeyUsage extension flagged as critical. This means that the certificate SHALL be used only for a purpose for which the corresponding key usage bit is set to one.
The Issuing CA's certificates KeyUsage extension MUST contain the following bits set to one:
digitalSignature - nonRepudiation - keyCertSign - cRLSign It MAY contain also other bits set to one.

No further stipulation, this will be handled by the subscriber agreements

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for Cryptographic Module

Cryptographic modules in use within the Standard Bank PKO comply with industry standard at least at level of FIPS 140-2 Level 3.

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

The Issuing CA 113/4 private key is split between Hardware security module and 9 smartcard(s) protected by a key encryption key (KEK) this key is split into nine (9) segments. Each segment is stored on a different smart card, and different persons hold each a smart card. In order to reconstruct the Issuing CA 113/4 key, at least three out of these nine persons need to convene at the CA'S to reconstruct the KEK and to restore the Issuing CA 113/4 key. This means that no two persons shall possess the means required to activate the Issuing CA 113/4 key. This process is only required when the Microsoft CA services are (re)started on Windows server whiting which the CA operates.

6.2.3 Private Key escrow

There is no key escrow. ***("At this time")***

6.2.4 Private Key backup

The ICA 113/4 Private Key is backed up in the same manner as described in 6.2.2; three of the nine smartcards are stored in Backup location in segregated storage.

6.2.5 Private Key archival

The ICA 113/4 Private Key is archived up in the same manner as described in 6.2.2; three of the nine smartcards are stored at off-site cold-storage.

6.2.6 Private Key entry into cryptographic module

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

The Issuing CA 113/4 private key is unloaded from the HSM as described in 6.2.2.

6.2.7 Private Key activation

The Standard Bank Issuing CA 113/4 Private Key is not maintained online, it can be restored as described in 6.2.2. Once loaded, 3 people holding a SA role are required to activate the HSM.

6.2.8 Method of deactivating private key

Private keys stored in a HSM can be deactivated by either the HSM itself, through the self-protection

mechanism, a reset, or by the CAA, trough an interface command or by shutting down the software-interface.
"THIS IS PART OF THE TAKE-DOWN PROCESS"

6.2.9 Method of destroying private key

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

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

"THIS IS PART OF THE TAKE-DOWN PROCESS"

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public key archival

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

6.3.2 Usage periods for the public and private keys

The ISSUING CA 113/4 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.

6.4 ACTIVATION DATA

Activation Data for the Issuing CA 113/4 are maintained in secret shares as defined in section 6.2.2. and used as multi-factor authentication process.

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

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific computer security technical requirements

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

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

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

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

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

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System development controls

The executable code that makes up the CA system software is vital to the correct functioning of the system. All executable code must be installed from the original software distribution media. The configuration of the Issuing CA 113/4 system as well as any modification must be documented and controlled.

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

6.6.2 Security management controls

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

6.6.3 Life cycle security ratings

No stipulation.

6.7 NETWORK SECURITY CONTROLS

The Issuing CA 113/4 is never connected to a network.

6.8 CRYPTO ENGINEERING CONTROLS

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

7 CERTIFICATE AND CRL PROFILES

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

7.1 CERTIFICATE PROFILES

7.1.1 Version number(s)

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

7.1.2 Certificate Extensions

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.

In compliance with [3], the inclusion of the following certificate extensions is RECOMMENDED: It is also RECOMMENDED the use of other two extensions: CRLDistributionPoint for providing information useful to retrieve the CRL, and SubjectAltNames when there is the need to include an RFC822 e-mail address to a certificate. Both these two extensions SHOULD be marked as NOT CRITICAL.

Extension name	**Extension Value**
SubjectKeyIdentifier	NOT CRITICAL
AuthorityKeyIdentifier	NOT CRITICAL
BasicConstraints	CRITICAL
KeyUsage	CRITICAL
CertificatePolicies	NOT CRITICAL

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.

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

The Certificate Policies extension field has a provision for conveying, along with each certificate policy identifier, additional policy-dependent information in a qualifier field.
This policy suggests that the qualifier field SHOULD be a CPS Pointer qualifier that contains a pointer to a Certification Practice Statement (CPS) published by the CA.
The pointer is in the form of a uniform resource identifier (URI).
No further stipulation, this is left to the Issuing CA

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 shall 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 shall be 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

8.3 CPS approval procedures

The Issuing CA 113/4 MUST be evaluated for compliance with this policy statement. In order to obtain CPS approval conforming this has submitted this CPS to the contact people specified in section 1.4.3. Therefore The Issuing CA 113/4 awaits confirmation to be recorded subsequent to the provisioning of this CA. The time limit for completing the evaluation is established in 60 days. It might be acceptable that this CA self-certify its own compliance with the policy; in this case, if later non-compliance with the policy is reported to Standard Bank PKO Administration ***("PA")***, then this CA certificate SHALL be revoked.

APPENDICES

A CP's Supported Under this CPS

A.1 Standard Bank Issuing CA 113/4 Certificate & Policies

Standard Bank Public Key Operations links to TRUST Hierarchy Anchor defines and implements the Bank's Issuing CA 11 Certificate Authority.

The initial release version of the Issuing CA 113/4 uses the Microsoft standard certificate templates as Certificate Polices for Secure eMail, EFS and entity identification as for IPSEV & VPN based on certificates. The modified Certificate templates are appended in A.3.

A.1.1 Standard Bank Issuing CA 113/4 Certificate

OID: 1.3.6.1.4.1.16543.401.113.1.1.1

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
Issuing CA 113	113/4
Certificate	1
Version	1.1

Table 3 – Standard Bank PKO Issuing CA 113/4 Certificate OID

A.1.2 Certificate DUMP CA 113

```
X509 Certificate:
Version: 3
Serial Number: 61034f69000000000009
Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
    Algorithm Parameters:
    05 00
Issuer:
    CN=Standard Bank Policy CA 11
    OU=IT Security
    OU=PKO Services
    O=Standard Bank Group
    L=JNB
    S=GP
    C=ZA

Subject:
    CN=Standard Bank CA 113
    OU=Crypto Services
    OU=PKO Services
    O=Standard Bank of South Africa Limited
    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 cb 22 ba 70 10 11 96
    0010  04 fd e5 3b 35 bc 8e de  2f 6c 57 7b 45 77 e4 3a
    0020  fe 0f 54 91 95 2b 54 ad  8d 13 df f1 b2 c7 f3 8c
    0030  59 85 de 03 f6 a4 74 42  77 e6 24 f8 c4 60 57 bb
    0040  31 7e 14 06 ce d3 54 62  45 bb 82 d8 3c 93 34 40
    0050  32 a2 d9 a7 de ef 30 55  b6 2a b1 5e 3d fd 6b 35
    0060  6d 1f b9 cf fe 4e bc 30  bd be 9b 64 f6 f0 65 74
    0070  03 49 84 e3 11 a0 1a fb  9a 1e 4d a2 65 84 3f 08
    0080  cf 33 a1 61 9d 20 6d 86  63 65 06 ea 8b ae ae bc
    0090  d6 d8 a7 d9 de 7d 8d 4e  75 cc bb 33 71 fe 13 95
    00a0  19 dd 32 59 8f 82 34 b9  74 f2 99 f0 00 55 fe 34
    00b0  2e 11 6a 84 e6 0d 7b 25  8f d3 4c ae 19 cd f5 e4
    00c0  06 6d 03 20 68 25 63 02  72 ce 18 e6 ef cc 94 cf
    00d0  86 08 9c ff f9 59 f2 37  52 89 eb 9c 64 d3 1d 37
    00e0  00 4a 3c 43 dc d1 09 1c  2b 72 67 25 9d 13 99 dd
    00f0  6b cd d2 61 97 21 1d 5a  36 71 94 a5 5e 6f 5f b7
    0100  1d 32 04 61 d7 ab 15 f0  79 2c b9 34 a3 5b e4 f7
    0110  82 24 63 70 a1 01 f8 d0  5e c6 8f fa 7f ec b9 62
    0120  ba e7 0c ef 5f 4d 62 1f  ae 9b a9 fd e1 63 69 b3
    0130  83 fe ec 48 45 e9 8c c7  b4 69 dc c3 43 97 87 de
    0140  a8 8c a2 ea e5 2a 3b b0  d2 1b b6 cd 40 ab d0 ce
    0150  b6 2c 36 c2 bf c0 d0 19  bb 54 f8 e3 f2 e4 1f af
    0160  c5 67 35 10 39 0e eb 9c  fc d9 1a a0 f4 62 4f 7b
    0170  aa 46 d1 b3 e3 e2 b3 1e  02 2b a5 4e 9e cf cd 10
    0180  4e 79 fe e7 01 4e 71 37  c2 e1 90 95 9e 5b 48 31
    0190  7f 8e e0 ff 1b 44 ff 38  0e ab 61 00 01 d2 3c c2
    01a0  2b 0d e7 b0 71 e1 b0 0e  0f 47 2d a8 24 36 72 09
    01b0  3c 40 16 de 42 ec 07 3e  6b ec 35 38 30 29 3b c9
    01c0  a8 34 a5 a6 56 c7 31 70  b6 87 d9 83 3b 69 29 1e
    01d0  e8 21 5e ee 19 f5 f3 3e  ad 97 69 cf 82 50 95 2e
    01e0  57 03 b8 f6 93 28 c8 01  41 d9 c7 79 db 4a 0b 54
    01f0  4e d8 95 01 b2 f9 cb 1a  4d 38 b6 05 74 05 8c e5
    0200  f1 72 2a 44 3c 94 c4 09  13 02 03 01 00 01
Certificate Extensions: 9
    1.3.6.1.4.1.311.21.1: Flags = 0, Length = 3
    CA Version
        V0.0

    2.5.29.14: Flags = 0, Length = 16
    Subject Key Identifier
        87 29 d4 59 93 98 f7 6e c9 8e da 1c 5f a3 90 bd d9 ad 57 3b

    2.5.29.32: Flags = 0, Length = 92
    Certificate Policies
        [1]Certificate Policy:
             Policy Identifier=1.3.6.1.4.1.16543.401.113.2.2.1
             [1,1]Policy Qualifier Info:
                  Policy Qualifier Id=User Notice
                  Qualifier:
                       Notice Text=Legal Policy Statement
             [1,2]Policy Qualifier Info:
                  Policy Qualifier Id=CPS
                  Qualifier:
                       http://pko.standardbank.co.za/CA-113-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 (86)

    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=36 d7 9c 61 11 ab a9 53 f9 ad 24 08 21 c6 41 34 67 30 68 7a

    2.5.29.31: Flags = 0, Length = 131
    CRL Distribution Points
```

```
        [1]CRL Distribution Point
             Distribution Point Name:
                  Full Name:
                       URL=http://pko.standardbank.co.za//Standard%20Bank%20Policy%20CA%2011.crl


    1.3.6.1.5.5.7.1.1: Flags = 0, Length = 131
    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//05766pkojnb0011_Standard%20Bank%20Policy%20CA%2011.crt
        [2]Authority Info Access
             Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
             Alternative Name:


Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
    Algorithm Parameters:
    05 00
Signature: UnusedBits=0
    0000  f4 f3 ef 90 9a ae ae 98  ef 8f 9c 97 80 c8 89 f2
    0010  f2 00 3c 35 56 59 a2 80  82 ea 4b c8 2c 95 32 6d
    0020  80 ee fd b5 25 b4 03 c2  f9 a4 02 fc 7a 58 26 53
    0030  8c 88 dc b3 0f c5 32 a9  1e 58 ae 1b 33 d9 d2 23
    0040  63 d0 d9 4a f6 46 b6 38  ff bb f4 24 1d 3f 01 bf
    0050  5f 8d 9c 26 cf cb fe 01  11 b9 e8 92 2a a7 1a 14
    0060  fa 83 5c e9 8a f3 cc f0  69 61 d8 c6 f9 4f 6a ab
    0070  e6 87 aa 23 9e 96 fd c1  97 4c 80 b9 7b 77 2f a7
    0080  c3 d9 e2 7d 6d 87 70 2e  70 a8 4a 40 17 3c 46 47
    0090  cb c6 d8 b1 51 56 6d bf  9d 30 77 a5 28 2f 5c 95
    00a0  77 8e ce d4 a6 d4 b9 89  f9 6e 24 49 e5 94 b2 11
    00b0  25 91 47 18 22 d2 a1 84  6a ad 79 6e 24 2b 31 a3
    00c0  bc 57 b0 85 34 fa 02 f3  b0 ea 82 0b be bb 0c d3
    00d0  21 2d aa 4f e4 36 11 b1  16 e2 e5 3e 27 66 a9 24
    00e0  74 45 e7 42 b9 a3 58 bc  7d 62 c3 7b 9e f3 64 76
    00f0  ec 77 fd 9a c4 1e 62 2d  fb d7 5c bc 1b 8a 08 25
    0100  df cb a2 a7 f5 47 e3 d9  8a 3f de 5d 49 24 c0 fd
    0110  de 48 0b 61 cd 7a cd fd  2e 1e 8b ed d3 47 b0 3c
    0120  9f db 1a 9e 48 18 49 c8  4f db 86 7b 0c d5 00 09
    0130  f3 34 8c 9f 73 69 cc 0b  3c 93 00 a1 58 e7 de 57
    0140  bf 86 86 e2 e3 55 e4 e3  c0 cb 70 4a 34 3f f3 51
    0150  98 fd e6 c2 d6 36 10 ed  77 28 3b 0f a6 6e ea 88
    0160  c2 68 15 80 5b b4 7a 4c  7a 68 c4 8c 70 91 93 17
    0170  6b 81 b9 1a dc 5d 32 f1  3e 42 88 3e 0e 31 3c 46
    0180  dd b1 0a 28 8b 9e f7 21  07 9f 3b 3c 04 50 26 82
    0190  55 da dd b7 7a 2f 14 0a  a2 52 bf c4 94 a0 89 ac
    01a0  9c c1 23 a1 79 78 2c 31  7e bc 99 8a c6 34 6a c9
    01b0  fa 31 89 da b5 ee 9e cc  e5 f1 75 03 14 ab 44 3d
    01c0  8b 56 17 6f 9f fb 7f 0a  fa e2 21 6a 78 6d c7 8f
    01d0  98 6a c9 06 f3 d9 0d 60  5c f3 e9 67 5b a7 38 da
    01e0  57 84 df ac b2 12 f5 59  7a 07 c0 01 14 a3 44 a8
    01f0  f6 57 16 48 8c de d2 5a  22 2b 24 46 3d 57 49 1b
Non-root Certificate
Key Id Hash(rfc-sha1):      87 29 d4 59 93 98 f7 6e c9 8e da 1c 5f a3 90 bd d9 ad 57 3b
Key Id Hash(sha1):          df bb 8b c2 5c a4 06 6f e8 e7 a4 95 67 f9 9c 16 63 fd a0 3c
Cert Hash(sha1):            31 b2 31 f7 b8 16 6d 8d c0 df da 38 8d 2c 24 33 8c 79 31 8f
```

A.1.3 Certificate DUMP CA 114

```
Version: 3
Serial Number: 61036a5400000000000a
Signature Algorithm:
    Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
    Algorithm Parameters:
    05 00
Issuer:
    CN=Standard Bank Policy CA 11
    OU=IT Security
    OU=PKO Services
    O=Standard Bank Group
    L=JNB
    S=GP
    C=ZA

 NotBefore: 2014/02/15 11:51 AM
 NotAfter: 2022/10/18 09:59 AM

Subject:
    CN=Standard Bank CA 114
    OU=Crypto Services
    OU=PKO Services
    O=Standard Bank of South Africa Limited
    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 bf 36 40 42 5f c8 6e
    0010  e2 a0 3e 5c e6 63 dd 9a  52 bb 19 19 9f ed d7 0e
    0020  62 8f 81 25 b3 6d 03 bc  61 05 dd 08 7b ef 1b 26
    0030  1a 91 1b bf 71 2a 96 27  72 0a af 85 52 c9 58 45
    0040  35 56 92 2e a4 76 e9 72  4e 19 6d c6 ee b2 8f c6
    0050  6e 7b ef bc 8c be c4 99  e3 34 d8 3b 08 30 b8 c1
    0060  56 b0 68 7d cf a1 17 36  35 a3 ab 97 b4 4e 1d 43
    0070  e7 fd 5b 75 80 86 01 b9  d9 0a 39 66 92 05 6f 7d
    0080  36 42 d8 46 b8 01 da f4  b1 21 43 5e 17 14 89 4d
    0090  50 64 a2 39 13 33 55 20  ff 8a e7 da 4e 89 f5 aa
    00a0  c6 28 e4 5c 65 c6 d1 69  1b d4 19 8e 48 ff 4c b1
    00b0  d2 06 ac 7a 88 5f eb 78  78 ea 50 a3 fb b1 8d 4c
    00c0  3c 46 82 46 fe 61 dc 58  fa 39 f5 21 8b de 1f b3
    00d0  17 9f 24 4e c2 6a fe 97  a6 37 a0 f3 ce a0 c4 31
    00e0  02 d3 c5 4d e8 63 13 31  a1 8e a2 50 6b 4b d0 c3
    00f0  8b 78 5c 0a 47 ee 26 eb  6f 8d cd b0 1c d5 11 96
    0100  8b 71 09 2a 3c d4 1c 46  7a 3d f0 01 be da b4 75
    0110  e2 c5 6d c9 b3 6a 21 bd  d1 49 f1 c9 44 80 b1 ca
    0120  ba 3f 67 09 ae 7f 65 10  0e 5e d2 b2 61 9a 9d 12
    0130  f0 96 c2 f1 0d e8 61 ed  44 37 09 bc 21 56 67 bf
    0140  53 c0 4d 62 f6 0b 5c f8  20 1f 43 07 64 a9 0e 57
    0150  4d da 80 7f 1b 36 65 8f  e3 20 c3 d5 44 e3 ce 50
    0160  84 f4 1a d2 41 f5 e5 63  9c 99 6b 9c 1b a2 ec 7f
    0170  41 e6 2f 85 98 da 0d 81  52 18 e9 56 dc 91 c4 e4
    0180  56 c9 5b c4 f7 ad a0 38  2d 7c 9d 12 76 63 2e 5d
    0190  52 17 94 57 23 4f bf 50  4f 2f c9 a6 8e 7d 7e 82
    01a0  4e d3 c8 96 20 e4 28 11  86 5f 89 f6 42 46 35 af
    01b0  ff c7 51 6e db 55 7d 53  bb 2f b8 05 ff 10 c2 46
    01c0  29 4c 4f c8 0c cd 1c a1  3f 85 2e c4 95 e5 8a 00
    01d0  69 ec 1f ac ae d7 05 d0  78 39 97 17 d6 c7 6c 1d
    01e0  3d d1 f3 53 a7 f5 d4 ea  88 a8 d6 c8 78 02 2f f7
    01f0  b6 ef 49 13 70 f6 fd 8b  c2 d3 19 ac a7 2e 21 ca
    0200  b1 06 80 03 dc ce e9 91  a1 02 03 01 00 01
Certificate Extensions: 9
    1.3.6.1.4.1.311.21.1: Flags = 0, Length = 3
    CA Version
        V0.0

    2.5.29.14: Flags = 0, Length = 16
    Subject Key Identifier
        6a e2 c1 7b b6 94 08 fb c5 77 1e f9 a5 62 f7 5f ce 70 ca 24

    2.5.29.32: Flags = 0, Length = 54
    Certificate Policies
```

```
          [1]Certificate Policy:
               Policy Identifier=1.3.6.1.4.1.16543.401.114.2.2.1
               [1,1]Policy Qualifier Info:
                    Policy Qualifier Id=CPS
                    Qualifier:
                         http://pko.standardbank.co.za/CA-113-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 (86)

     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=36 d7 9c 61 11 ab a9 53 f9 ad 24 08 21 c6 41 34 67 30 68 7a

     2.5.29.31: Flags = 0, Length = 131
     CRL Distribution Points
          [1]CRL Distribution Point
               Distribution Point Name:
                    Full Name:
                         URL=http://pko.standardbank.co.za//Standard%20Bank%20Policy%20CA%2011.crl


     1.3.6.1.5.5.7.1.1: Flags = 0, Length = 131
     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//05766pkojnb0011_Standard%20Bank%20Policy%20CA%2011.crt
          [2]Authority Info Access
               Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2)
               Alternative Name:

Signature Algorithm:
     Algorithm ObjectId: 1.2.840.113549.1.1.5 sha1RSA
     Algorithm Parameters:
     05 00
Signature: UnusedBits=0
     0000  e7 74 6a 46 90 ce dc ba  90 77 13 98 35 43 1f 76
     0010  9d 74 14 2f b5 81 88 df  a3 f9 a5 38 21 43 bd da
     0020  8b d7 0e 4b 29 70 b4 2b  1b 60 10 06 f3 f5 5a 66
     0030  b8 92 02 73 9c 7d 93 49  67 1d c0 3c 5d 62 79 b1
     0040  c4 36 41 03 71 95 40 3d  b4 38 1e 09 aa 03 81 db
     0050  3e 53 27 f6 22 2e af 46  14 16 bf f9 49 a9 f6 67
     0060  c3 c2 a2 21 bd 49 2a 28  5e e5 c5 04 69 f6 b1 aa
     0070  d6 2b 29 37 d0 15 f0 44  f7 38 db 75 3f e3 8d 60
     0080  71 c4 44 04 44 46 fe ae  3f 12 21 84 d2 9c 9e 8d
     0090  4f 38 e5 40 24 13 3b aa  42 9f 29 ad 8b f5 34 db
     00a0  40 c8 bf 82 97 59 97 bf  7e f6 de c4 c6 4b f0 a4
     00b0  30 64 4e 7a 1b 4f 3b a3  44 0c a9 d4 97 29 7d 39
     00c0  4b f6 df c6 be 3a d0 9f  0d 70 cd 60 81 e0 93 4f
     00d0  56 7e d9 cc 3b cc 7c 24  19 b3 b4 d4 56 36 a1 3e
     00e0  b9 dd 20 68 e3 37 d6 85  8c b2 7b b5 d1 ba a6 72
     00f0  b4 36 90 65 c8 78 13 f8  57 27 a0 d7 49 94 3e 66
     0100  1f 0e ff b6 71 c5 eb ea  d2 1d 5e aa 46 f5 10 e6
     0110  39 7c a8 4b 7f e0 c3 67  56 97 8b 69 e9 7d a4 3e
     0120  0c 97 72 d0 ba 06 6c 5a  41 67 a5 1b 84 76 7b 9d
     0130  e8 d8 80 a8 c6 af bd 0e  83 8e 53 88 41 43 20 a9
     0140  34 33 a9 04 65 7c c6 f5  84 cb c3 b1 29 21 9d 70
     0150  d7 2b 03 0d 8c 2b 5b 73  68 c0 0a 03 9c d8 b4 42
     0160  3d dd b8 74 c1 7a d7 aa  33 16 f5 85 d3 b1 c7 58
     0170  55 c4 b3 41 a3 62 d8 40  a8 51 92 16 98 e7 e9 66
     0180  dd fb 54 b3 5f 97 e0 34  49 2a cc 7b 86 aa ee 2e
     0190  9c a4 e2 65 35 73 70 1d  cb 15 91 f2 1f 2f d5 43
     01a0  d7 fb 24 37 c6 d2 8e 88  40 63 e2 dd 15 8c fc 41
     01b0  9e 43 08 88 50 3f 1b 04  b8 34 9f 46 67 fd 40 42
     01c0  c2 74 37 be 64 e7 73 dd  bf 75 ec 47 46 1b fa 5d
     01d0  dc a2 40 d2 7f f4 6a ce  45 40 0a 41 a7 ad 71 e9
     01e0  fa 89 f8 80 5a 13 2d 6e  76 15 02 a5 39 31 15 a7
     01f0  2e d1 4d 15 50 cd 90 35  94 b5 0a 6e 0a ff ef 43
```

```
Non-root Certificate
Key Id Hash(rfc-sha1): 6a e2 c1 7b b6 94 08 fb c5 77 1e f9 a5 62 f7 5f ce 70 ca 24
Key Id Hash(sha1): b2 ac ff f5 54 0e d5 a9 62 4a f9 a7 f5 e3 ce 7d 56 d5 54 e8
Cert Hash(sha1): 7d db ad e8 55 9e e4 67 03 8e ec 24 5d 97 b7 fe f6 57 b8 3f
```

A.2 Standard Bank Issuing CA 113/4 Configuration

Root Certificate Authority	
CA Unique Name	Standard Bank CA 113/4
Version Type	V3
Current Certificate Version	1.0
	Install certificate from a PKCS#7 text file from the Standard Bank Issuing CA 113/4
CA Lifetime	12 Years
CA Key Length	4096
CRL Validity Interval	21 Days
CRL Publishing Interval	2 Days
CSP PKI Algorithm	RSA
CSP HASH Algorithm	SHA-256
CRL Locations:	LDAP to Active Directory and HTTP
Subject DN	O = Standard Bank of South Africa Limited OU = IT Security Services C = ZA L = JHB ST = GP

A.3 Glossary

A.3.1 Terms

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

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

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

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

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

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

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

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

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

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

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

IPR – Intellectual Property Rights

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

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

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

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

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

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

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

A.3.3 References

[1] RFC 2527 —Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework“ March 1999 [ftp://ftp.isi.edu/in-notes/rfc2527.txt]

[2] RFC 2119 —Key words for use in RFC’s to Indicate Requirement Levels“ March 1997 [ftp://ftp.isi.edu/in-notes/rfc2119.txt]

[3] RFC 2459 —Internet X.509 Public Key Infrastructure: Certificate and CRL Profile“ January 1999 [ftp://ftp.isi.edu/in-notes/rfc2459.txt]

[4] RFC 2560 —Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol œ OCSP“ June 1999 [ftp://ftp.isi.edu/in-notes/rfc2560.txt]

[5] 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