CERTIFICATE AUTHORITY (CA) RULES

Bank of Zambia

SEPTEMBER, 2014

Bank of Zambia

PART I

CERTIFICATION AUTHORITY POLICY AND PROCEDURES

FOR THE

BOZ ZIPSS/CSD SYSTEM

September, 2014

Version: 1.0

Table of Contents

PART I 1

CERTIFICATION AUTHORITY POLICY AND PROCEDURES 1

1.1 Overview 7

1.2 Acronyms and Definitions 7

1.3 PKI participants 8

1.3.1 Certification authority 8

1.3.2 Registration authority 8

1.3.3 Subscribers 9

1.3.4 Relying parties 9

1.3.5 Other participants 9

1.4 Certificate usage 9

1.4.1 Appropriate certificate uses 9

1.4.2 Prohibited certificate uses 9

1.5 Certificate Types 9

- *Server Certificates 9*
- *Client Certificates 9*

1.6 CA Administration 10

1.6.1 Policy Administration 10

1.6.2 Contact persons 10

1.6.3 Communication with the CA 10

1.6.4 CA Roles and Responsibilities 10

1.6.5 Certification Authority Policy and Procedures approval procedures 10

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 11

2.1 Repositories 11

2.2 Publication of certification information 11

2.3 Access controls on repositories 11

3. IDENTIFICATION AND AUTHENTICATION 11

3.1 Naming of Subscribers 11

3.1.1 Types of names 11

3.1.2 Participant's ID or Code 11

3.1.3 Meaningful common names 12

3.1.4 Anonymity or pseudonymity of subscribers 12

3.1.5 Rules for interpreting various name forms 12

3.1.6 Uniqueness of names 12

3.1.7 Recognition, authentication, and role of trademarks 12

3.2 Initial identity validation 13

3.2.1 Method to prove possession of private key 13

3.2.2 Authentication of organization identity 13

3.2.3 Authentication of individual identity 13

3.2.4 Non-verified subscriber information 13

3.2.5 Validation of authority 13

3.2.6 Criteria for interoperation 13

3.3 Identification and authentication for revocation request 13

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 14

4.1 Certificate Application 14

4.1.1 Who can submit a certificate application 14

4.1.2 Enrolment process and responsibilities *14*
4.2 Certificate application processing 14
4.2.1 Performing identification and authentication functions *14*
4.2.2 Approval or rejection of certificate applications *14*
4.2.3 Time to process certificate applications *14*
4.3 Certificate issuance 14
4.3.1 CA actions during certificate issuance *14*
4.3.2 Notification to subscriber by the CA of issuance of certificate *15*
4.4 Certificate acceptance 15
4.4.1 Conduct constituting certificate acceptance *15*
4.4.2 Publication of the certificate by the CA *15*
4.4.3 Notification of certificate issuance by the CA to other entities *15*
4.5 Key pair and certificate usage 15
4.5.1 Subscriber private key and certificate usage *15*
4.5.2 Relying party public key and certificate usage *16*
4.6 Certificate renewal 16
4.6.1 Circumstance for certificate renewal *16*
4.6.2 Who may request renewal *16*
4.6.3 Processing certificate renewal requests *16*
4.6.4 Notification of renewed certificate issuance to subscriber *16*
4.6.5 Conduct constituting acceptance of a renewed certificate *16*
4.7 Certificate re-key 16
4.8 Certificate modification 17
4.9 Certificate revocation and suspension 17
4.9.1 Circumstances for revocation *17*
4.9.2 Who can request revocation *17*
4.9.3 Procedure for Revocation Request *17*
4.9.4 Revocation Request Grace Period *17*
4.9.5 Time within which CA must process the revocation request *18*
4.9.6 Revocation checking for relying parties *18*
4.9.7 CRL issuance frequency *18*
4.9.8 Maximum latency for CRLs (if applicable) *18*
4.9.9 On-line revocation/status checking availability *18*
4.9.10 On-line revocation checking requirements *18*
4.9.11 Special requirements key compromise *18*
4.9.12 Circumstances for suspension *18*
4.10 End of subscription 18
4.11 Key escrow and recovery 18
5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS **19**
5.1 Physical controls 19
5.2 Procedural controls 19
5.3 Personnel controls 19
5.4 Audit logging procedures 19
5.5 Records archival 19
5.6 Key changeover 19
5.7 Business Continuity and Disaster Recovery 19
5.8 CA or RA termination 19
6. TECHNICAL SECURITY CONTROLS **20**

6.1 Key pair generation and installation 20
6.1.1 Key pair generation 20
6.1.2 Private Key delivery to subscriber 20
6.1.3 Public key delivery to certificate issuer 20
6.1.4 CA public key delivery to relying parties 20
6.1.5 Key sizes 20
6.1.6 Public key parameters generation and quality checking 20
6.1.7 Key usage purposes 20
6.2 Private Key Protection and Cryptographic Module Engineering Controls 20
6.2.1 Cryptographic module standards and controls 20
6.2.2 Private Key backup 21
6.2.3 Private Key archival 21
6.2.4 Private key transfer into or from a cryptographic module 21
6.2.5 Private Key storage on cryptographic module 21
6.2.6 Method of activating private key 21
6.2.7 Method of deactivating private key 21
6.2.8 Method of destroying private key 21
6.3 Other aspects of key pair management 21
6.3.1 Public key archival 21
6.3.2 Certificate operational periods and key pair usage periods 21
6.4 Activation data 22
6.4.1 Activation data generation and installation 22
6.4.2 Activation data protection 22
6.5 Computer security controls 22
6.5.1 Specific computer security technical requirements 22
6.5.2 Computer security rating 22
6.6 Life cycle technical controls 22
6.6.1 System development controls 22
6.6.2 Security management controls 22
6.7 Network security controls 22
7. CERTIFICATE AND CRL PROFILES 23
7.1 Certificate profile 23
7.1.1 Version number(s) 23
7.1.2 Content of Certificates 23
a) Server Certificate 23
b) Subscriber Certificate 23
7.1.3 Algorithm object identifiers 23
7.1.4 Name forms 23
7.1.6 Certificate policy object identifier 24
7.2 CRL profile 24
7.2.1 Version number(s) 24
8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS 24
8.1 Frequency or circumstances of assessment 24
8.2 Identity/qualifications of assessor 24
8.3 Assessor's relationship to assessed entity 24
8.4 Topics covered by assessment 24
8.5 Actions taken as a result of deficiency 24
9. OTHER BUSINESS AND LEGAL MATTERS 25

9.1 Fees 25
9.2 Financial responsibility 25
9.3 Confidentiality of business information 25
9.4 Privacy of personal information 25
9.5 Intellectual property rights 25
9.6 Representations and warranties 25
9.7 Disclaimers of warranties 25
9.8 Limitations of liability 25
9.9 Term and termination 25
9.9.1 Term 25
9.9.2 Termination 25
9.9.3 Effect of termination and survival 25
9.10 Individual notices and communications with Participants 26
9.11 Amendments 26
9.11.1 Procedure for amendment 26
9.11.2 Notification mechanism and period 26
9.11.3 Circumstances under which OID must be changed 26
9.12 Dispute resolution provisions 26
9.13 Governing law 26
9.14 Compliance with applicable law 26
9.15 Miscellaneous provisions 26
9.15.1 Assignment 26
9.15.2 Severability 26
9.15.3 Enforcement (attorneys' fees and waiver of rights) 27
9.15.4 Force Majeure 27

PART II 28

SECURITY USER GUIDE 28

10 BASIC CONCEPTS 29
10.1 About this User Guide 29
10.2 Overview of Security Features 29
10.2.1 Introduction 29
10.2.2 Scope 29
10.2.3 Physical access 29
10.2.4 Logical access 29
10.2.5 Segregation of duties 30
10.2.6 Telecommunications security 30
10.2.7 BOZ ZIPSS/CSD Business continuity 30
10.2.8 Audit trails 30
10.3 Identification of Users 31
10.4 E-Tokens 31
10.5 BOZ ZIPSS/CSD Security Administration Roles 31
10.6 User Profiles 32
10.7 Groups in the BOZ ZIPSS/CSD System 32
10.8 Physical Site Security 32

11 BOZ ZIPSS/CSD USER ACCESS SECURITY 33
11.1 Overview 33
11.2 Security Tokens 33
11.3 Administrative Procedures for Tokens 33

11.3.1 Request and Issue of Security Tokens *34*
11.3.2 Revocation/Suspension of Security Tokens *35*
11.3.3 Renewal of Certificates from the Security Tokens *35*
11.3.4 Re-issue of Security Tokens *36*
11.4 BOZ ZIPSS/CSD Profiles Management 36
11.4.1 Introduction *36*
11.4.2 How to List Current Profiles *36*
11.4.3 How to Add a Profile *37*
11.4.4 How to Modify a Profile *38*
11.4.5 How to Approve Profile Management Operations *39*
11.4.6 How to Remove a Profile *40*
11.5 BOZ ZIPSS/CSD Users Management 41
11.5.1 Introduction *41*
11.5.2 How to List Current Users *42*
11.5.3 How to Add a New User *43*
11.5.4 How to Modify a User Profile *44*
11.5.5 How to Approve User Management Operations *45*
11.5.6 How to Remove a User *46*
11.5.7 How to Disable a User *47*
11.5.8 How to Activate a User *47*
11.5.9 User Profiles and Segregating Functional Roles *48*

10. APPENDIX **50**
10.1 User Information Request Form 50
10.2 E-Token Application Form 53
10.3 E-token Revocation Form 55

11. REFERENCES **57**

1. INTRODUCTION

1.1 Overview

This document outlines the Certification Authority Rules containing the policy and procedures to govern and administer the Certification Authority and PKI on the BOZ ZIPSS/CSD system. The PKI shall be used to authenticate users to the BOZ ZIPSS/CSD system and to digitally sign electronic documents processed by the said system. This policy and procedures are for a single-purpose PKI operated and managed by the Bank of Zambia, the main administrator of the BOZ ZIPSS/CSD system. Certificates associated with this CA shall only be used for purposes of authentication and digital signatures for BOZ ZIPSS/CSD system although the CA can later issue certificates for use on other applications as required by BOZ.

This document is based on RFC3647[1], an international standard for CA and PKI implementation.

1.2 Acronyms and Definitions

BOZ	Bank of Zambia
CA	Certification Authority
Client certificates	Used to authenticate subscribers and PCs in order to provide secure access and communication
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSD	Centralized Securities Depository
EJBCA	Enterprise JavaBeans Certification Authority
e-Token	a USB-based authenticating module present on each token that provides strong user authentication and cost-effective password management
FIPS 140-2	Federal Information Processing Standard Publication 140-2, is a U.S. government computer security standard used to accredit cryptographic modules
IP	Internet Protocol
LuSE	Lusaka Stock Exchange
Messenger	Messenger - A representative of a Participant who conveys tokens to or from BOZ
MoF	Ministry of Finance
OCSP	Online Certificate Status Protocol
OID	Organizational Identity
Participant(s)	Organisations that access the BOZ ZIPSS/CSD system.

PKI	Public Key Infrastructure
RA	Registration Authority - an authority in a network that verifies user requests for a digital certificate and tells the Certification Authority to issue it
Re-key	The process of generating a new private key for an existing certificate
Relying Party	A recipient of a certificate that/who acts in reliance on that certificate and/or any digital signatures made using the CA certificate
RSA	an algorithm for public-key encryption developed by Rivest, Shamir and Adleman
BOZ ZIPSS/CSD	Real Time Gross Settlement
Server	A computer system providing infrastructure for the BOZ ZIPSS/CSD System
Server certificates	Used to authenticate servers for secure communication and web-based transactions using Secure Socket Layer (SSL) technology
SHA	Secure Hash Algorithm is a family of cryptographic hash functions
Subscriber(s)	An individual person to be authenticated to the BOZ ZIPSS/CSD System.
ZECHL	Zambia Electronic Clearing House Limited
ZIPSS	Zambia Interbank Payments and Settlement System
ZRA	Zambia Revenue Authority

1.3 PKI participants

1.3.1 Certification authority

BOZ shall play the role of the CA for the BOZ ZIPSS/CSD system. It shall be the only CA in this PKI setup.

1.3.2 Registration authority

Participants perform the Registration Authority function. These participants are:

- BOZ
- Commercial banks using the BOZ ZIPSS/CSD System
- ZECHL, ZRA, LuSE and the Ministry of Finance.

RAs validate identity information for their subscribers and provide enrolment information to the CA for action. They control the access profile in the BOZ ZIPSS/CSD system that is associated with each subscriber.

1.3.3 Subscribers

Subscribers are individuals whose work requires them to have access to BOZ ZIPSS/CSD System. Each Subscriber is enrolled by a Participant. Participants are responsible for the actions of their Subscribers and may not repudiate those actions.

1.3.4 Relying parties

Relying parties in this CA setup are:

- BOZ, as payments system operator.
- Participants
- Subscribers.

1.3.5 Other participants

In addition to participants as defined under Section 1.3.2 above, the other player with an interest in the operations of the system is Montran, the supplier of BOZ ZIPSS/CSD software.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates shall be used to authenticate Subscribers to the BOZ ZIPSS/CSD System and to digitally sign certain electronic messages used in this system.

Certificates shall be delivered on a USB token, 'e-token', that shall be inserted into a BOZ ZIPSS/CSD workstation when a Subscriber logs in. This e-token shall not be inserted into any other device.

1.4.2 Prohibited certificate uses

Any use of certificates other than that herein described is prohibited.

1.5 Certificate Types

Two types of certificates are used in a PKI, namely Server certificates and Client Certificates.

- **Server Certificates**

  The BOZ ZIPSS/CSD Server shall use a server certificate.

- **Client Certificates**

  All subscribers shall be issued with a Client Certificate.

1.6 CA Administration

1.6.1 Policy Administration

This document is administered by:

Bank of Zambia,
Information and Communications Technology (ICT) Department,
P.O Box 30080,
Lusaka, Zambia.
10101

Tel: +260211 228888-93

1.6.2 Contact persons

The contact offices for this Certification Authority policy and procedures at BOZ are:

i) Assistant Director – ICT Governance and Compliance
Information and Communications Technology Department

ii) Manager – ICT Security and Quality Assurance
Information and Communications Technology Department

1.6.3 Communication with the CA

i) CA shall be set up at BOZ and administered by ICT Department
ii) Two points of contact for users at BOZ:
   - ZIPSS Service Desk
   - CSD Service Desk
iii) If CA related, request is forwarded to ICT Service Desk for action by the CA Administrator.
iv) After acting on the request, CA Administrator communicates with respective Service Desk to contact the Participant

1.6.4 CA Roles and Responsibilities

i) CA Security Administrator
ii) CA Approval Manager
iii) BOZ ZIPSS/CSD Service Desk Administrator
iv) BOZ ZIPSS/CSD Approval Manager
v) Participant User Security Administrator

1.6.5 Certification Authority Policy and Procedures approval procedures

Changes to this document shall be made in line with BOZ Change Management procedures.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

All master documents and information related to the CA shall be held by BOZ ICT Department.

2.2 Publication of certification information

Documentary information about the PKI shall be distributed to Participants through the BOZ ZIPSS/CSD Project Secretariat during the project phase and by Payments Systems Division of the Banking, Currency and Payments Systems Department of BOZ, as needed or when changes occur.

2.3 Access controls on repositories

Access to PKI information shall be controlled in line with the BOZ Information Security Policy.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming of Subscribers

3.1.1 Types of names

i) Subscribers' enrolment shall be based on their real names.

ii) Each subscriber shall be associated with the Participant that enrolled them

iii) A Subscriber's User ID shall conform to the following format:
{xxx/} – The Participant's ID, 3 chars eg BOZ, BBZ, FNB etc.
{Initial of First name}
{Surname}
Eg. Robert Banda at Barclays Bank would be BBZ/rbanda

iv) If there is a conflict in names in the same Participant, the middle initial shall be used to differentiate between the two users
Eg. BBZ/rkBanda for Robert Kondwani Banda and BBZ/rzbanda for Robert Zondani Banda.

v) The Participant's ID will be UPPERCASE while usernames be in lower case as shown above.

3.1.2 Participant's ID or Code

The following codes shall be used for the Participants identified below:

BOZ ZIPSS/CSD PARTICIPANT	ID/CODE
AB Bank	ABB/
Access Bank	ABZ/
Banc ABC	ABC/
Barclays Bank	BBZ/
Bank of China	BOC/
Bank of Zambia	BOZ/
Cavmont Bank	CAV/
Citibank	CIT/
Ecobank	ECO/
First Alliance Bank	FAB/
Finance Bank	FBZ/
First Capital Bank	FCB/
First National Bank	FNB/
Intermarket Banking Corporation	IBC/
Investrust Bank	IVB/
Indo-Zambia Bank	IZB/
Ministry of Finance	MOF/
Stanbic Bank	SBI/
Standard Chartered	SCB/
United Bank of Africa	UBA/
ZANACO	ZNC/
ZECHL	ZEC/
Lusaka Stock Exchange	LUS/
Stanbic Nominees	SBN/
Standard Chartered Nominees	SCN/

3.1.3 Meaningful common names

The Subscriber name shall reflect the name commonly used by the Participant to identify that Subscriber for internal identification purposes.

3.1.4 Anonymity or pseudonymity of subscribers

i) Anonymous subscribers shall not be allowed.
ii) Pseudonyms shall not be allowed.

3.1.5 Rules for interpreting various name forms

i) Ordinary names normally used to identify a person shall to be used.
ii) To avoid a name clash between two people with the same names a variant may be used such as the inclusion of a middle initial (see Section 3.1.1 above).

3.1.6 Uniqueness of names

All Subscriber names enrolled by a Participant shall be unique.

3.1.7 Recognition, authentication, and role of trademarks

No trademarks shall be used for a Subscriber by its participants.

3.2 Initial identity validation

i) Participants act as Registration Authorities (RAs).
ii) Participants enrol Subscribers, and Subscribers may only be enrolled by Participants.
iii) It is up to the Participants how they validate the identity of their Subscribers.

3.2.1 Method to prove possession of private key

Subscribers shall prove their possession of private keys by using their e-tokens to successfully sign on to the BOZ ZIPSS/CSD System.

3.2.2 Authentication of organization identity

i) Each Participant must maintain at BOZ a list of at least **three (3)** signatories authorised by the Participant to request changes to their Subscribers.
ii) This list must be conveyed to BOZ using secure communication methods for physical documents as prescribed in the BOZ Information Security Policy and the respective Participants' Security policies.
iii) Two signatures from this list are required to sign on any request to the CA.

3.2.3 Authentication of individual identity

Each Participant shall apply own methods of authenticating individual identity.

3.2.4 Non-verified subscriber information

There shall be no Subscriber information in the system that is not provided by the enrolling Participant.

3.2.5 Validation of authority

Authority shall be verified by the authorised signatures submitted to BOZ.

3.2.6 Criteria for interoperation

There shall be no interoperation between this PKI and any other PKI. However, this PKI can later be used for other applications needing secure transmission and authentication in the BOZ.

3.3 Identification and authentication for revocation request

When a properly authorised certificate revocation form is received from a Participant, the CA shall revoke the identified Subscriber's certificate.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Any Participant can submit a certificate application as part of the request to implement a new BOZ ZIPSS/CSD user. It must be authorised as set out in Section 3.2.2 above.

4.1.2 Enrolment process and responsibilities

As RAs, Participants are responsible for

i) Identifying their applicants,
ii) Determining the appropriate level of access and
iii) Requesting the required level of access using relevant forms.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

BOZ shall accept a valid application from a Participant to mean that the Participant has established the identity of the Subscriber to its satisfaction, and that it shall take responsibility for that person's actions using the BOZ ZIPSS/CSD System.

4.2.2 Approval or rejection of certificate applications

Applications for a certificate shall be accepted by BOZ if it meets all the stipulated requirements.

4.2.3 Time to process certificate applications

Certificates shall be processed and be ready for collection within 2-3 working days.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CA shall:

i) Validate the request for consistency, and, if not sure on authenticity, contact the Participant for resolution.

ii) Log the request in a database.

iii) Generate the key-pair, public and private key on the e-token.

iv) Generate a certificate including the public key for the Subscriber

v) Make the e-token ready for collection by the participant.

4.3.2 Notification to subscriber by the CA of issuance of certificate

i) Notification shall be made by the CA to the respective Service Desk who shall then contact the Participant by telephone, email or any other appropriate means.
ii) The Participant shall then send a designated person to uplift the certificate from BOZ.
iii) The designated person shall collect the certificate and sign for it.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

i) Any initial use of the issued certificate shall be deemed as acceptance.
ii) Failure to notify the CA of rejection of certificate within 3 working days of collecting a certificate shall be assumed as acceptance.

4.4.2 Publication of the certificate by the CA

The certificate shall be installed onto the BOZ ZIPSS/CSD servers by the CA.

4.4.3 Notification of certificate issuance by the CA to other entities

No other party shall be notified of certificate issuance.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The following usage rules apply to the BOZ ZIPSS/CSD certificates and shall be adhered to by Participants and Subscribers:

i) BOZ ZIPSS/CSD certificates are only to be used to sign onto the BOZ ZIPSS/CSD System and applying digital signatures on transmitted data. No other use is permitted.
ii) The e-tokens containing certificates may only be inserted into BOZ ZIPSS/CSD workstations.
iii) A certificate is granted to an individual Subscriber.

iv) Each certificate may only be used with the user ID and password that has been issued to the Subscriber.

v) Subscribers are prohibited from using another Subscriber's certificate, user ID or password.

vi) Disclosure of passwords is prohibited.

vii) Acceptance of certificates by a Participant constitutes agreement with these rules.

4.5.2 Relying party public key and certificate usage

The only relying parties are other Subscribers who are bound by the same policies.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

i) The Participant is responsible for tracking the expiry dates of certificates
ii) The enrolling Participant shall request new certificates and e-tokens from the CA before their expiry.

4.6.2 Who may request renewal

Only authorised persons acting for the Participant may request certificate renewal using the Renewal Request form to the CA.

4.6.3 Processing certificate renewal requests

i) The CA shall check the Subscriber information in the CA database before issuing a new certificate, keys, and e-token.
ii) The CA shall issue and renew the certificate with new keys.
iii) The CA shall install the new certificate on an e-token.
iv) The process of delivery and acceptance is the same as that for a new enrollment described above.
v) The Participant shall return the expired e-token containing the expired certificate to BOZ through the authorized delegated person.

4.6.4 Notification of renewed certificate issuance to subscriber

i) The Participant shall notify the Subscriber that their certificate has been renewed and is awaiting collection.
ii) The Participant shall issue the certificate to the Subscriber using their internal delivery procedures.

4.6.5 Conduct constituting acceptance of a renewed certificate

Use of a renewed e-token or non-rejection of 3 working days constitutes acceptance of an e-token.

4.7 Certificate re-key

i) Certificates shall not be re-keyed.

ii) If it is necessary to replace a certificate, the process described for certificate renewal at Section 4.6.3 above shall be followed.

4.8 Certificate modification

i) Certificates shall not be modified.
ii) However, a Participant can alter a Subscriber's authorisations in BOZ ZIPSS/CSD System without needing to change or reissue the certificate.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

i) A certificate shall be revoked by the CA when any of the following has transpired or any other circumstance as deemed fit by the CA:
- The e-token is reported to have been lost or compromised;
- The Subscriber no longer works for the Participant that enrolled him or her
- The Subscriber no longer requires access to the BOZ ZIPSS/CSD System.

ii) It is the responsibility of the enrolling Participant to inform the CA immediately any of these events occur.

4.9.2 Who can request revocation

i) RAs request revocation on behalf of their enrolled Subscribers.
ii) In exceptional circumstances the CA can revoke certificates even when the relevant Participant has not requested, in order to preserve the integrity of the system.

4.9.3 Procedure for Revocation Request

i) The Participant must submit the appropriate form duly signed to the CA.
ii) If urgent revocation is sought, an authorised signatory may telephone the CA with the request. However, revocation shall only be done upon the CA's satisfaction that the caller is indeed the authorised signatory. The form shall still be required to be filled in so as to keep a record of the request.

4.9.4 Revocation Request Grace Period

There is no grace period. The CA shall act upon the request as soon as it is received.

4.9.5 Time within which CA must process the revocation request

The CA shall process a revocation request as soon as practical but by the end of the business day on which the revocation request was received.

4.9.6 Revocation checking for relying parties

Relying parties can use the automated CRL checking on the BOZ ZIPSS/CSD System.

4.9.7 CRL issuance frequency

The CRL shall be updated whenever a certificate is revoked.

4.9.8 Maximum latency for CRLs (if applicable)

The CRL in use on the BOZ ZIPSS/CSD System shall be updated as soon as possible after a new CRL is created by the CA.

4.9.9 On-line revocation/status checking availability

The CRL is automatically checked by the BOZ ZIPSS/CSD System.

4.9.10 On-line revocation checking requirements

These are handled automatically by the BOZ ZIPSS/CSD System whenever a user logs in and at defined intervals while users remain logged on.

4.9.11 Special requirements key compromise

Participants must report key compromise to the CA as soon as possible.

Participants remain responsible for all use of BOZ ZIPSS/CSD by their enrolled Subscribers.

4.9.12 Circumstances for suspension

Certificates cannot be suspended.

4.10 End of subscription

Certificates shall be revoked or expired when no longer required.

4.11 Key escrow and recovery

Private key escrow and recovery is not provided by the CA.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

The CA server shall be hosted in the Server Room in the ICT Department of BOZ. In addition to the physical access controls to the BOZ premises, there is controlled physical access to the Server Room which is labelled as a 'Red area'.

5.2 Procedural controls

Certificates shall be generated by one of the two staff members who have the required access in the ICT Department.

5.3 Personnel controls

The CA shall be operated by Planning and Control Division of the ICT Department at BOZ.

5.4 Audit logging procedures

All activities on the CA shall be logged and reviewed by BOZ Internal Audit. Logs are subject to normal BOZ backup procedures.

5.5 Records archival

All CA activity logs shall be archived and maintained according to retention period stipulated in the BOZ Information Security policy.

5.6 Key changeover

This applies to procedure to provide a new public key to a Subscriber following a re-key by the CA. However, since re-keys are not allowed in this PKI, this procedure is not applicable.

5.7 Business Continuity and Disaster Recovery

The CA setup shall be backed up in line with the BOZ Business Continuity Plan for critical applications on the network.

5.8 CA or RA termination

If the CA is terminated, the database of certificates shall either be destroyed or transferred to a new CA at the discretion of the BOZ Management Committee.

Each participant is an RA. If an RA is terminated, all its subscribers' IDs and certificates shall be revoked.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

The user keys shall be generated either using generation module on the CA software for Server certificates or by e-Token, the hardware module present on each e-Token for Subscriber certificates.

6.1.2 Private Key delivery to subscriber

The private key shall never leave the e-token hardware module, hence there shall be no need for separate delivery to the Subscriber but shall be delivered on the e-token.

6.1.3 Public key delivery to certificate issuer

The Subscriber's public keys are delivered in the Subscriber's certificates held on the e-token.

6.1.4 CA public key delivery to relying parties

Public keys in certificates are delivered to BOZ ZIPSS/CSD as part of the CA activities.

6.1.5 Key sizes

The user certificate key sizes shall be 2048 bits RSA with SHA-256.

6.1.6 Public key parameters generation and quality checking

The e-token shall use cryptographic hardware for keys generation with Federal Information Processing Standards (FIPS) 140-2 Level 2 and 3 certifications.

6.1.7 Key usage purposes

i) The key usage purposes for all certificates shall be digital signature, non-repudiation and key encryption.
ii) If it is a Subscriber certificate, it shall also be used for client authentication and if a Server certificate, for server authentication.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

i) The e-token used for Subscriber key-pair generation shall have FIPS 140-2 level 2 and 3 certification.
ii) Server key-pairs are placed into Server certificates for installation by the relevant support group for each system.

6.2.2 Private Key backup

The CA does not backup any private keys.

6.2.3 Private Key archival

The CA does not provide private key archival.

6.2.4 Private key transfer into or from a cryptographic module

The private key shall never leave the e-Token cryptographic hardware where it is generated.

6.2.5 Private Key storage on cryptographic module

This is handled by the cryptographic module of the CA Software.

6.2.6 Method of activating private key

There shall be no separate activation step. The certificates are generated with immediate validity.

6.2.7 Method of deactivating private key

Private keys are deactivated when the relevant certificate expires or is revoked.

6.2.8 Method of destroying private key

When a certificate is renewed, the previous certificate shall be deleted along with its keys. The old keys shall be placed in the CRL.

6.3 Other aspects of key pair management

6.3.1 Public key archival

i) All certificates and their included public keys are kept permanently in the CA database.
ii) The expired certificates are also held on the database.

6.3.2 Certificate operational periods and key pair usage periods

The CA's own certificate shall be valid for a period of 10 years.

Subscriber certificates shall have a validity of 1 year. As key-pairs are fixed to the relevant certificates, the terms for the certificates are also the terms for the keys.

6.4 Activation data

6.4.1 Activation data generation and installation

CA operators shall be required to use individual strong, complex passwords that are non-dictionary words, alphanumeric characters with minimum length of 6.

The passwords shall have to be renewed after a maximum period of 3 months. Shorter periods are encouraged in line with respective password policies.

6.4.2 Activation data protection

CA operators are required to protect these passwords and not to divulge them to others.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The CA server shall be hosted in the Server Room in the ICT Department of BOZ. In addition to the physical access controls to the BOZ premises, there is controlled physical access to the Server Room which is labelled as a 'Red area'.

6.5.2 Computer security rating

The CA application and environment shall assigned the information classification of 'Top Secret' and shall be treated accordingly as defined in the BOZ Information Security Policy.

6.6 Life cycle technical controls

6.6.1 System development controls

The CA software used shall be internationally accepted and widely available. No development needs to be undertaken by BOZ.

6.6.2 Security management controls

The logs, the configuration files and the entire CA system shall be regularly checked and verified by Auditors.

6.7 Network security controls

The CA computer shall be on the network. Network access controls shall be enforced as stated in the ICT Security manual.

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate profile

7.1.1 Version number(s)

All certificates shall be X.509 version 3 or later certificates.

7.1.2 Content of Certificates

a) Server Certificate

A Server certificate shall include the following information:

- Applicant's domain name
- Applicant's public key
- Issuing CA (BOZ)
- BOZ Electronic signature
- Type of algorithm
- Validity period of digital signature
- Serial number of digital signature

b) Subscriber Certificate

A Subscriber's certificate shall include the following information:

- Subscriber's name
- Organizational Identity of Participant
- Applicant's public key
- Code of Applicant's country
- Issuing CA (BOZ)
- BOZ Electronic signature
- Type of algorithm
- Validity period of digital signature
- Serial number of digital signature

7.1.3 Algorithm object identifiers

The accepted signature algorithm shall be SHA-256 with RSA encryption.

7.1.4 Name forms

Within the Distinguishing Name (DN) of a user certificate, the following elements must be set:

- Organisational Unit (OU): The Bank Identification Code (three characters) of the Subscriber or Server

- Common Name (CN): the assigned username (Initial and Surname)
- Country (C): The ISO 3166-2 country code for Zambia is 'ZM'

7.1.6 Certificate policy object identifier

All issued certificates shall comply with the stipulated standard.

7.2 CRL profile

7.2.1 Version number(s)

CRLs shall be created in X.509 v2 or later format.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

i) Compliance shall be audited at BOZ by external auditors on an annual basis to give independent assurance.
ii) Participants are expected to have their RAs and Subscriber enrolment functions audited.

8.2 Identity/qualifications of assessor

As part of the regular audit cycle for BOZ and Participants the assessor shall be identified.

8.3 Assessor's relationship to assessed entity

BOZ shall use their appointed external auditor. Participants are expected also to use their external auditors as assessors.

8.4 Topics covered by assessment

Assessment shall be done to verify whether policies and procedures set out in this document are being followed.

8.5 Actions taken as a result of deficiency

All parties are required to correct any deficiency found by the Auditor.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fees for use of the CA and e-tokens shall be in line with a pricing model to be developed and circulated by BOZ to all the Participants.

9.2 Financial responsibility

All BOZ ZIPSS/CSD participants are responsible for the actions of their Subscribers using the BOZ ZIPSS/CSD system.

9.3 Confidentiality of business information

Confidentiality of information used and processed by the CA shall be as stated in the BOZ Information Security Policy.

9.4 Privacy of personal information

The CA shall not publish lists of Subscribers to anybody else except to the enrolling Participants.

9.5 Intellectual property rights

There are no intellectual property rights inherent in the PKI.

9.6 Representations and warranties

BOZ warrants that the CA shall be operated as set out in this document. Participants warrant that they shall take due care in identifying their Subscribers.

9.7 Disclaimers of warranties

No warranties are implied except as set out herein.

9.8 Limitations of liability

As set out in Part X of the Electronic Communications and Transactions Act of 2009.

9.9 Term and termination

9.9.1 Term

This policy and practice statement has no fixed term. It may be amended from time to time.

9.9.2 Termination

If a Participant ceases to operate, or if a Participant ceases to use the BOZ ZIPSS/CSD System, all of that Participant's Subscriber certificates shall be revoked and their access to the BOZ ZIPSS/CSD System denied. The Participant shall return all of its Subscribers' e-tokens to BOZ.

9.9.3 Effect of termination and survival

This policy does not apply to Participants or Subscribers after they have ceased to be Participants or Subscribers. Other policies connected with their access to BOZ ZIPSS/CSD system and the information therein may continue to apply.

9.10 Individual notices and communications with Participants

i) Each Participant must notify the CA of their contact person, including name, address, telephone and email.

ii) Participants are responsible for advising the CA whenever this changes.

9.11 Amendments

9.11.1 Procedure for amendment

BOZ shall review and amend this policy from time to time in consultation with the Participants. Any Participant may propose a change at any time.

9.11.2 Notification mechanism and period

BOZ shall notify amendments to this policy to all Participants no less than 30 days before the amendments come into effect.

9.11.3 Circumstances under which OID must be changed

There are no circumstances under which the Organisational Identification, OID shall be changed.

9.12 Dispute resolution provisions

All disputes under this policy should in the first instance be resolved through mutual discussion. If the parties are unable to agree, the aggrieved party may take the matter to the courts.

9.13 Governing law

Governing law shall be the laws of the Republic of Zambia specifically and not limited to the Electronic Communications and Transactions Act of 2009.

9.14 Compliance with applicable law

All parties must comply with applicable law at all times.

9.15 Miscellaneous provisions

9.15.1 Assignment

No Participant may without the prior written consent of BOZ assign, change or otherwise dispose of or part with the benefit of this policy or any of its rights or interests herein or obligations hereunder.

9.15.2 Severability

If any provision of this policy is for any reason invalid, illegal, void or unenforceable, that will do derogate from or affect the remainder of this policy to the intent that the offending provision will by reason of such invalidity, illegality, fact of being void or unenforceability be deemed omitted.

9.15.3 Enforcement (attorneys' fees and waiver of rights)

No failure, delay, relaxation or indulgence on the part of any party in exercising any power or right conferred upon such party in terms of this policy operates as a waiver of such power or right, nor does any single or partial exercise of any such power or right preclude any other or future exercise thereof, or the exercise of any other power or right under this policy.

9.15.4 Force Majeure

9.16.5.1 If by force majeure any party is rendered unable wholly or in part to carry out its obligations under this policy (except payment obligations) or is delayed in its operations to be performed pursuant to this policy (except payment obligations) such party may within 14 days from the date of commencement of such force majeure give written notice thereof to the other party stating the date and extent of such suspension and the nature of the force majeure causing the same. Upon the giving of such notice, the obligations of the party claiming force majeure shall be suspended during the continuance of such force majeure so far as such obligations are affected by the force majeure.

9.16.5.2 The party claiming force majeure shall use all due diligence to remove the effects thereof but nothing in this clause requires any party to settle any industrial dispute except in such manner as it in its absolute discretion deems fit.

9.16.5.3 Any party the performance of whose obligations has been so suspended shall resume performance thereof as soon as reasonably possible after the circumstances preventing such performance have terminated and shall promptly thereafter so notify the other party in writing.

9.16.5.4 In the event that a party has invoked the provisions of this Clause and a force majeure continues for a period of six (6) months thereafter the parties shall consult forthwith in good faith in order to determine what steps shall be taken by them to carry out the intentions of the policy. If within a further period of one month the parties are unable to agree on any such steps this Agreement may be terminated by either party on not less than two (2) weeks written notice to the other and thereafter no party shall be under any further obligation to the other party.

9.16.5.5 Each party shall notify the other immediately upon its becoming aware of any event known or likely to give rise to a possible suspension of its obligations pursuant to this Clause 9.16.5.

9.16.5.6 For the purpose of this policy the term *"force majeure"* includes (but is not limited to) fires, flood, storms and other damage caused by the elements, strikes, riots, explosions, governmental action or inaction, currency restrictions, acts of God, insurrection and war and any other cause whether of the kind specifically enumerated above or otherwise which is not reasonably within the control of the party claiming *force majeure.*

Bank *of* Zambia

PART II

SECURITY USER GUIDE

FOR

BOZ ZIPSS/CSD SYSTEM

10 Basic Concepts

10.1 About this User Guide

This User Guide is designed for the BOZ staff who are responsible for security management and users of the BOZ ZIPSS/CSD system.

This Guide covers all the activities involved in the set up and management of users, including the process for the issue of access control tokens with digital certificates.

10.2 Overview of Security Features

10.2.1 Introduction

Security is a crucial aspect of BOZ ZIPSS/CSD operations. The system provides security features regarding access control, telecommunications security, audit trails, fallback and recovery facilities. However, all these are in vain if security policies and procedures are not rigorously followed by users and technical staff. In this section we describe the main security matters of which users should be aware.

10.2.2 Scope

The BOZ ZIPSS/CSD system security features cover:

- Physical Access
- Logical Access
- Segregation of duties
- Telecommunications
- BOZ ZIPSS/CSD Business continuity
- Audit trails

10.2.3 Physical access

At participant sites, physical access to BOZ ZIPSS/CSD workstations should be protected. Physical site security at the BOZ should also be strictly controlled.

10.2.4 Logical access

Access to the BOZ ZIPSS/CSD servers is controlled by way of security device (e-token) login. The token must be present for login to take place, and the user who has been assigned a particular token must be present to enter their PIN. The certificate from the token has to be renewed whenever it expires.

The period during which a user is logged on, is known as a BOZ ZIPSS/CSD Session. Although the system will close down a session if no activity has taken place for some minutes, it is the responsibility of users to ensure that BOZ ZIPSS/CSD terminals are not left unattended when logged in.

To ensure that only authentic users are logged onto BOZ ZIPSS/CSD system while running the BOZ ZIPSS/CSD applications, a username and password is required as well as the physical token and its PIN. The next section explains how to obtain and

use these. Passwords should be updated regularly in accordance with BOZ ICT security policy.

10.2.5 Segregation of duties

To assure the integrity of the BOZ ZIPSS/CSD service, it is important that individual users cannot both enter transactions and approve them. Nor should those who can provide the tokens, usernames and passwords for system access also be users themselves. The system provides features to force different steps to be undertaken by different users, but manual controls outside the system are necessary to enforce segregation of duties.

The BOZ will expect Participants to ensure that duties are allocated in a way that ensures that only valid transactions can be entered into the system.

10.2.6 Telecommunications security

Participant connection to the central BOZ ZIPSS/CSD system takes place over encrypted lines via VPN. BOZ ZIPSS/CSD encrypts every transmission from terminals to the system and from the system to users. This process uses SSL Internet security.

This process ensures that:

- Payments cannot be added, deleted or changed while being transmitted once they have been entered,
- Participants cannot deny that they submitted a particular transaction.
- No payments or message details can be read by unauthorized persons while in transit.

10.2.7 BOZ ZIPSS/CSD Business continuity

The BOZ ZIPSS/CSD system is fully duplicated at a Disaster Recovery (DR) site, so that if there is a disaster at Head Office, operations can move almost instantaneously to the DR site. To facilitate this, BOZ ZIPSS/CSD logs every transaction to the DR site. All transactions processed on the live system are logged and replicated onto the server at DR Site.

10.2.8 Audit trails

Audit trail logs of all daily transactions and account movements are stored on the live system and kept at the DR site. The logs show the operator, date and time of every action. In the event of a dispute, users are able to review messages and transactions, and the process of their submission. Auditors and supervisors can examine all the activities carried out on the system, including transaction and static data amendments.

All transaction data is accessible for audit purposes on the BOZ ZIPSS/CSD database.

10.3 Identification of Users

All users must be identified and authenticated to the BOZ ZIPSS/CSD application before they can sign on. The BOZ ZIPSS/CSD Security Administrator is responsible for ensuring that the processes for user registration and access are effectively managed and comply with overall BOZ ICT security policy. The Participants will apply their own internal procedures for identifying and approving access by their internal users to the BOZ ZIPSS/CSD system.

10.4 E-Tokens

Tokens are used to secure point-to-point access between the BOZ ZIPSS/CSD servers and the user Webstations. Users need to use their e-Token in order to log in. The BOZ CA Security Administrator will assign the tokens.

10.5 BOZ ZIPSS/CSD Security Administration Roles

The BOZ ZIPSS/CSD Security Administration Team comprises of the distinct members shown below:

i) At Bank of Zambia:

- **BOZ CA Security Administrator (CASA)** – this Security Administrator is in charge of issuing certificates and e-Token for authorized BOZ and Participants' users.
- BOZ CA Approval Manager – this officer approves all requests on certificates and e-Token before the CA Security Administrator can perform the requested task.
- BOZ ZIPSS/CSD Service Desk Administrator – although not strictly a Security role, this Administrator will be receiving all requests and queries from the Participants on the respective Service Desks. If CA related, s/he shall forward these requests to the relevant Security Administrators.

ii) At the Participant's end (including BOZ):

- **Participant's User Security Administrator (PUSA)** – this Officer is in charge of adding new users to the system by entering specific user information and creating the user profile using the BOZ ZIPSS/CSD interface. The new user would have been approved internally in the business unit based on the business approval rules before information on the new user is entered into the system.
  When requested, this Administrator would also modify existing user information and profile. Each Participant should appoint an Officer who should ideally come from the business area.

- **User Approval Officer** – this Officer is in charge of approving the new or modified users. S/he decides whether a user becomes active in the BOZ ZIPSS/CSD system or not. S/he should also decide whether a user can be deleted or not. This Officer is one of the three signatories whose names should have been deposited with the BOZ Certification Authority.

10.6 User Profiles

The BOZ ZIPSS/CSD application uses a series of menus to allow access to system functions. User access controls are designed to restrict the access of each user to certain functions only. Each user needs to be assigned functions appropriate to their role.

For each Participant user, the Participant User Security Administrator assigns Usernames and initial Passwords on the BOZ ZIPSS/CSD system and establishes User Profiles that determine which functions each user will be able to access within the system. When the user logs onto the system, the only functions displayed to them will be those allowed by their User Profile.

10.7 Groups in the BOZ ZIPSS/CSD System

A Group is used in the BOZ ZIPSS/CSD system to refer to all the users belonging to a Participant.

Each Participant Group is designated by the Participant 3-character code and is automatically created by the system upon Participant creation. Participant Security Administrators can only gain access to the profiles for their own Group.

10.8 Physical Site Security

Best practice for BOZ ZIPSS/CSD suggests that the primary and DR computer rooms should be subject to an access control system. In BOZ, these have been classified as highly sensitive areas and have been labeled as 'Red Areas'. Personnel should have access only on a necessity basis and access should be subject to identity controls. The only people with access are:

- Authorized management of the BOZ
- Computer operators
- Security personnel

The only other persons that should be admitted to the computer rooms are:

- Auditors
- Suppliers' engineers called to rectify faults or install new equipment
- Cleaners
- Premises staff to maintain or improve facilities.

Access to the computer room by auditors, cleaners, suppliers' engineers or premises staff should be supervised at all times by one of the computer operators or the Management of BOZ.

11 BOZ ZIPSS/CSD user access security

11.1 Overview

Before individuals can login to BOZ ZIPSS/CSD as users, they must receive security clearance. All users must be identified to the BOZ ZIPSS/CSD application before they can sign on.

Tokens are used to secure the point-to-point access between the BOZ ZIPSS/CSD servers and the user Webstations. Both user and token must be present in order to log in.

The BOZ's CA Security Administrator will assign the tokens and control the access of the Participant User Security Administrator for each Participant. For each Participant's users, the Participant User Security Administrator assigns Usernames and Username Passwords, and establishes User Profiles that determine which functions each user will be able to access within the system. The user will not see functions on his or her screen, which are outside his or her profile. In its' capacity as a participant, the User Security Administrator at the BOZ also establishes User Profiles for BOZ users.

On receiving a token, username and password, users should immediately log-in and change the password. The processes for login and password maintenance are covered below. Similarly, PIN numbers should be changed immediately upon receiving the e-Token.

Users can change passwords and PINs at any time. In this way, only users will know their own passwords, and no other user can log in under their username without knowing both the password and PIN.

BOZ ICT Security policy on Password Management shall be followed.

11.2 Security Tokens

To establish the secure connection with the BOZ ZIPSS/CSD system, BOZ ZIPSS/CSD Webstations used by the BOZ and Participants require a token that contains a digital certificate to be inserted, and a password to be entered. This ensures that no unauthorized person can gain access to the system. Each user will have one token.

The BOZ CA Security Administrator is responsible for issuing procedures for the e-Token, passwords and other CA related procedures.

11.3 Administrative Procedures for Tokens

The procedures for issue and management of the BOZ ZIPSS/CSD tokens need to be secure and be strictly adhered to.

11.3.1 Request and Issue of Security Tokens

The CA Approval Manager supervises and approves the e-Token issue process, which is carried out by the CA Security Administrator.

The detailed steps in the process are as follows:

i) BOZ users will request access to BOZ ZIPSS/CSD via their User Security Administrator. Access will be granted only on business need basis for carrying out a specific job in the Bank:
- The user's Supervisor will complete a request form for a new BOZ user to be admitted
- The User Approval Officer will approve the User's request and profile
- After approval, the form will be sent to the CA Security Administrator who will assign a Username and initial password and issue a certificate on an e-Token.
- The e-Token will be sent to the BOZ ZIPSS/CSD Service Desk for the Participant's designated person to pick up.
- The password will be sent to the user through a separate secure channel of communication.

ii) The CA Security Administrator who controls the stock of blank tokens, will retain the request forms and log the request, keeping the following details, the last six to be completed when the token is ready for delivery:
- Bank name
- Person at Participant authorizing issue
- Contact details for collection
- Participant Support person responsible for this issue
- Common name (a character string that connects this certificate with a Username in BOZ ZIPSS/CSD system), provided on the request form
- Date of issue
- Expiry date
- Serial number of token
- Current certificate id
- Issue number
- Renewal number

iii) A separate log register should be kept for each Participant, and all events for each token must be recorded so that a full token history is retained for every token.

iv) The CA Security Administrator also performs the following tasks:
- Controls the "Certificate Authority Server", and uses this to download a digital certificate onto the new token.
- Changes the token's password from the manufacturer's default to a password unique to BOZ.
- Passes the token back to the BOZ BOZ ZIPSS/CSD Service Desk with the following certificate information:
    - User name,
    - Expiry date and
    - Certificate ID

v) The BOZ ZIPSS/CSD Service Desk Administrator shall fill the issue details in the log and arrange for the Participant User Security Administrator to collect the token Issue number and renewal number will both be '1' for the initial issue.

vi) The tokens are issued with a default user PIN, which must be changed as soon as it is received. The Participant User SA (or CASA at the BOZ) must ensure that this is done.

11.3.2 Revocation/Suspension of Security Tokens

The CASA or a Participant User SA (PUSA) can request the deactivation of a token. This request comes to the BOZ ZIPSS/CSD Service Desk at the BOZ. The PUSA must provide the serial number and the certificate ID for the token to be revoked.

Once the request has been approved by the User Approval Officer and the CA Approval Manager respectively, the token is revoked and the certificate is disabled on the certificate server.

Whenever a revocation takes place, the CA Security Administrator has to reload the Certificate Revocation List (CRL- list of all revoked certificates) onto the BOZ ZIPSS/CSD system in time for the next day's start-up of the system. The new CRL must be replicated to the DR site immediately.

The Username is immediately disabled to prevent access to the system by the user associated with that token.

Note that in the BOZ CA, no token or certificate will be suspended. They will be revoked and a new certificate and token be issued should the Subscriber be cleared and need to use the system again.

Whenever a reactivation takes place, the CASA has to reload the CRL onto the BOZ ZIPSS/CSD system in time for the next day's start-up of the system. The change must be replicated to DR Site immediately.

11.3.3 Renewal of Certificates from the Security Tokens

For security reasons, certificates must be renewed every 12 months.

For prudent operational reasons and to ease fall-back operational recovery, the initial tokens should be issued with a spread of renewal dates over a few months, not all due on one day.

The PUSA will issue a warning 2 weeks in advance to the relevant user that a certificate must be renewed

It is the PUSA's responsibility to ensure that the relevant token is returned securely to BOZ for certificate renewal.

BOZ ZIPSS/CSD Service Desk Administrator passes the tokens for renewal to the BOZ's CASA who will then erase the expired certificate from the token and download a new certificate to the old token

The CASA updates the issue date, expiry date, renewal number and Certificate id in the token log

S/he then sends the renewed token to the Service Desk to be collected.

11.3.4 Re-issue of Security Tokens

If a token is lost or damaged, its certificate must be revoked and a new token re-issued. The re-issue process is essentially the same as the issue process. PUSA and CASA must update the issue number as well as other details in the token log. This will indicate if a Participant is having particular problems with lost tokens.

Revoked but unexpired certificates must be included in the CRL which is uploaded into the system at daily start-up.

11.4 BOZ ZIPSS/CSD Profiles Management

11.4.1 Introduction

The BOZ ZIPSS/CSD system uses Profiles to restrict user access to different menu options from within the BOZ ZIPSS/CSD systems. There are Group Profiles (profiles set for a Participant) and User Profiles (profiles available to normal users).

A certain number of generic profiles can be defined by the BOZ operators to identify certain functions user can perform. This system defined user profiles can be used as root profiles at user creation stage to restrict the user functions. When a user is added he can be further restricted to be able to access only a subset of its root profile. Same a user menu access can be modified at a later date to have access to new menu functions but only in the limit of its root profile.

11.4.2 How to List Current Profiles

To display a list of all the profiles currently defined in the system, use the menu entry:

- **Administrative > Profile > List**

List Screen appears Screen Id: PRFLST002

Select profile status from the dropdown list provided, and then Click **Ok**.

List Profiles in list Screen appears Screen Id: PROLST002

A list of all the available profiles is displayed.

The profile related information available in the list consists of the ID of the profile, name of the profile, the profile type (Administrator, Participant, Clearing House), the status of the profile (ACTIVE or REMOVED) and the next status of the profile.

Clicking on a profile in the list will result in the display of more information regarding the profile selected:

List Profile Screen appears Screen Id: PROLST003

To go back to the List users screen, Click on the **Back to List** button. To move backward or forward in the list, in the reveal mode, use the **Previous** or **Next** buttons.

11.4.3 How to Add a Profile

To add a new profile of any kind, use the menu entry.

- **Administrative > Profile > Create**

Enter Profile Screen appears Screen Id: PRFPRFCRE001

Enter the new profile name and select the profile type from the list provided (Administrator, Participant or Clearing House).

Click **Ok**:

Enter Profile Screen appears Screen Id: PRFPRFCRE002

The name and type of the new profile are displayed. At this point, the name of the profile can still be modified.

From the list of the menu entries, select the appropriate ones for the profile about to be created. Clicking on the check box available for each menu leaf can do the selection.

Clicking on the **Reset** button, located at the bottom of the page, will result in the clearing of all the information entered on the page (profile name and menu entries selection).

Clicking on the **Cancel** button, located at the bottom of the page, will result in the cancellation of the Create Profile activity. An operation cancellation message is displayed.

After the profile has been appropriately configured (name is defined and menu entries are selected), Click on the **Ok** button located at the bottom of the page.

In the cases where the profile name introduced is already in use, the system will display a warning message on the top of the page.

If all the information entered is valid, Clicking on the **Ok** button will result in the display of the details. The information displayed on this screen is structured in the same manner as in the reveal from the List of existing profiles. This is the confirmation screen:

Enter Profile Screen appears Screen Id: PRFPRFCRE003

Click Ok to create the new profile. The new added profile is placed in the Approve queue (APPROVE status) and a confirmation message is displayed on the top of the page:

Operation successful Screen appears Screen Id: PREND

(The Profile now needs to be approved – See **Approve Profiles** below).

11.4.4 How to Modify a Profile

To modify any information with respect to an existing profile, use the menu entry:

- **Administrative > Profile > Modify**

Modify Profiles in list Screen appears Screen Id: PRFMOD001

A list of all the profiles with ACTIVE status is displayed (the default profiles cannot be modified).

The profile related information available in the list consists of name of the profile (**Profile name**), the profile type (**Type**), status of the profile (**Status**), and next status the profile (**Next Status**).

Clicking on the item from the list that you want to modify will result in the display of the create profile screen. The only difference is that the **Profile name** text field and the checkboxes available for each menu leaf are filled with the information that defines the profile to be modified:

Modify Profile Screen appears Screen Id: PRFMOD002

Clicking on the **Reset** button, located at the bottom of the page, will result in the clearing of all the information entered on the page (menu entries selection).

Clicking on the **Cancel** button, located at the bottom of the page, will result in the cancellation of the modify profile activity. An operation cancellation message is displayed.

The type of the profile cannot be modified. The **Profile type** text field is in read-only format.

After the profile has been modified Click on the **Ok** button located at the bottom of the page.

Modify Profile Screen appears Screen Id: PRFMOD003

The information displayed on this screen is structured in the same manner as in the reveal from List of existing profiles. This is the confirmation screen. Clicking on the **Cancel** button will result in the cancellation of the modify profile activity. An operation cancellation message is displayed.

Clicking on the **Ok** button will result in the actual modification of the profile. The modified profile is placed in the Approve queue (APPROVE status) and a confirmation message is displayed on the top of the page.

11.4.5 How to Approve Profile Management Operations

All actions performed with respect to adding new profiles or modifying existing profiles activities must be approved. The Security Officer who approves new or modified profiles must be different from the Security Officer who performed the entry or modification (4 eyes principle). Until this approval has been performed, the profile cannot be assigned to any users.

To approve a new or modified profile, use the menu entry:

- **Administrative > Profile > Approve**

Approve Profile in list Screen appears Screen Id: PRFAPP001

A list of all the available profiles that are in APPROVE status is displayed (if any).

If there are no items to be approved, the system will display a specific message.

The profile related information available in the list consists of the profile (**Name**), profile type (**Type**), status of the profile (**Status**), and the next status of the profile (**Next Status**). The only status available is APPROVE.

Click on the item in the list that you want to approve. This will result in the display of more information with respect to that item:

Approve Profile Screen appears Screen Id: PRFAPP002

Should the Security Officer responsible for approving the profile consider that the profile cannot be approved with its current structure, he/she should place the profile in REPAIR status (Click the **Reject** button), so that it can be modified accordingly.

The repair activity is performed via the **Modify**, and is presented later on in this manual.

Clicking on the **Approve** button will result in the activating of the new modified profile. The approved profile is ready to be assigned to specific users.

In both cases, a confirmation message is displayed. In the cases where the four eyes rule is not followed, a warning message is displayed.

11.4.6 How to Remove a Profile

A profile can only be removed if there are no users assigned to it. If a user tries to delete a profile while there are users in the system assigned to it, a warning message is displayed.

To delete an existing profile from the list of defined profiles, use the menu entry:

- **Administrative > Profile > Remove**

Remove Profiles in list Screen appears Screen Id: PRFREM001

A list of all the available profiles that are in ACTIVE status is displayed (the default profiles cannot be removed).

Click on the item to be removed:

Remove Profile Screen appears Screen Id: PRFREM002

Clicking the **Ok** button move the profile to the APPROVE status, with next status REMOVE.

To complete the removal, use the **Approve** function described above.

The profile can be seen using the list function and selecting the status REMOVED from the dropdown list provided.

11.5 BOZ ZIPSS/CSD Users Management

11.5.1 Introduction

The facilities in the BOZ ZIPSS/CSD system for all Security Administrators are essentially the same. However, the BOZ's BOZ ZIPSS/CSD Security Administrator has a profile which allows a broader range of actions across the whole user population than a Participant Security Administrator, whose domain is limited to users in their own Group.

It is anticipated that there will be one lead Security Administrator per Participant, but that a limited number of other staff may assist in Security Administration roles. It is necessary that certain functions are under dual control, so that the same person may not, for example, both enter new user details into the system **and** approve their activation. Where only one staff member carries out the Security Administration role, the Participant BOZ ZIPSS/CSD Administrator must carry out the approval processes.

In this chapter, we describe the system facilities available to Security Administrators. Security Administrators cannot use the transaction facilities of the system.

11.5.2 How to List Current Users

To display a list of all the users currently defined in the system, access the menu entry:

- **Administrative > User > List**

List Screen appears Screen Id: USRLST001

Select the Status of the users that you want listed (ACTIVE, DISABLED or REMOVED).

Select the Group or All Groups.

Click **Ok**:

List – Users in list Screen appears Screen Id: USRLST002

The user related information available in the list consists of the identifier used to login (**Username**), the user group name (**Group Name**), the status of the user (**Status**), and the next status of the user (**Next Status**).

Click on a user in the list to view more information regarding that user:

List User Screen appears Screen Id: USRLST003

An audit trail shows all operations performed on the user, the user performing and the time.

Click **Back to List** go back to the List users screen.

Click on **Previous** or **Next** to move backward or forward in the list.

11.5.3 How to Add a New User

To create a user, use the menu entry:

- **Administrative > User > Create**

Enter User Screen appears Screen Id: USRLDG001

Select the Group that the User belongs to and Click **Ok**:

Enter User Screen appears Screen Id: USRENT001

Enter the Username, Full name, initial password (the user is required to change the password for security reason when the user first logs in), number of days to password expiration, maximum password retry (3 times), preferred language (English only), Group Name and Profile.

Use the dropdown list provided to select the user Profile. All the profiles that are active into the system are available for selection in this list; however, a user can only be assigned a profile associated with the user's Group.

Click **Ok** to proceed:

Enter User Screen appears Screen Id: USRENT002

Check the details and Click **Ok** to complete the **Create User** operation. The user is placed in APPROVE status.

(The User now needs to be approved – See **Approve an existing User** below)

11.5.4 How to Modify a User Profile

To modify any information regarding an existing user, use the menu entry:

- **Administrative > User > Modify**

Modify User Screen appears Screen Id: USRMOD000

Select Group.

Click **Ok**:

Modify Users in List Screen appears Screen Id: USRMOD001

A list of all the active users is displayed.

The information available in the list consists of the user identifier (**Username**), user group (**Group Name**), profile assigned (**Profile Name**), the status of the user (**Status**) and the next status of the user (**Next Status**).

Click on the user that you want to modify:

Modify User Screen appears Screen Id: USRMOD002

Make the necessary changes in any of the fields provided.

Click **Ok**:

Modify User Screen appears Screen Id: USRMOD003

Clicking on the **Cancel** button will result in the cancellation of the modify user activity. An operation cancellation message is displayed.

Click **Ok** to complete the modify operation. The user is placed in APPROVE status and will need approval before it can become active.

11.5.5 How to Approve User Management Operations

All actions performed with respect to adding new users or modification of existing user activities must be approved. The Security Officer who approves new or modified users must be different from the Security Officer who performed the entry or modification.

To approve a new or modified user, use the menu entry:

- **Administrative > User > Approve**

User Approve Screen appears Screen Id: USRAPP000

Select the user Group (the group that the user belongs to) or select All.

Click **Ok**:

Approve Users in list Screen appears Screen Id: USRAPP001

A list of all the available users that are in APPROVE status is displayed (if any). In the cases where there are no items to be approved, the system will display a specific message.

In the cases where the "four eyes" rule is not obeyed, a warning message is displayed.

Click on the user to be approved. Its detailed information is displayed:

Approve User Screen appears Screen Id: USRAPP002

The Status, Next Status, Username, Full name, number of days to password expiration, maximum password retry (3 times), preferred language (English only), Group Name and Profile) are displayed.

In the cases where the Security Officer responsible for approving the user considers that the user cannot be approved with its current structure, the Security Officer will have to Click the **Reject** button, and the user will go back to its previous status.

Clicking on the **Approve** button will result in the activation of the new/modified user. The approved user can then plug in their e-token (which contains their security certificate), enter their PIN and login. On first login, the user is prompted to change their password and will be redirected to the login page. Access is granted after this step.

11.5.6 How to Remove a User

To remove an existing user from the list of active users, use the menu entry:

- **Administrative > User > Remove**

Remove User Screen appears Screen Id: USRREMT000

Select Group.

Click **Ok**:

Remove Users in list Screen appears Screen Id: USRREM001

Click on the user that is to be removed:

Modify User Screen appears Screen Id: USRREM002

Click Cancel to avoid removing the user.

Click **Ok** to move the User to the APPROVE status, with next status REMOVED.

The user removal must now be approved. A second authorized officer should use the **Approve** function to complete the user removal.

The users that have been removed from the system can still be viewed by selecting the Removed filter on the List screen.

11.5.7 How to Disable a User

To disable an existing user from the list of active users, use the menu entry:

- **Administrative > User > Disable**

Disable User Screen appears Screen Id: USRDIS000

Select Group.

Click **Ok**:

Disable Users in list Screen appears Screen Id: USRDIS001

Click on the user that is to be disabled:

Modify User Screen appears Screen Id: USRDIS002

Click **Cancel** to avoid disabling the user.

Click **Ok** to move the User to the APPROVE status, with next status DISABLED.

The disablement of the User must now be approved. A second Security Officer should use the **Approve** function to complete the user disablement.

11.5.8 How to Activate a User

To activate an existing user from the list of Disabled users, use the menu entry:

- **Administrative > User > Activate**

Activate User Screen appears Screen Id: USRACT000

Select Group.

Click **Ok**:

Activate Users in list Screen appears Screen Id: USRACT001

Click on the user that is to be activated:

Modify User Screen appears Screen Id: USRACT002

Click Cancel to stop the Activation process and return the user to Disabled status.

Click **Ok** to move the User to the APPROVE status, with next status ACTIVE.

The user must now be approved. A second authorized officer should use the **Approve** function to complete the user Activation.

11.5.9 User Profiles and Segregating Functional Roles

The main facilities provided by the BOZ ZIPSS/CSD Webstation facility to Participants are:

- On-line access to account and transaction information;
- Queue management tools;
- On-line transaction entry
- Gateway access

When establishing a new user, Participants need to consider whether the new user will have access to all the Participant functions or whether access should be restricted to particular functions. For example, it is unlikely that a Participant would wish to give all users the facility to manipulate queue priorities.

Similarly, the BOZ must ensure an appropriate segregation of duties between users responsible for transaction entry and approval.

Granting access to the **Administrative/User** function, in particular should be restricted to specialized Security Administrators.

10. APPENDIX

10.1 User Information Request Form

Bank *of* Zambia

BOZ ZIPSS/CSD SYSTEM

USER INFORMATION REQUEST FORM

Form No BOZ ZIPSS/CSD CA01

Name of Participant (organization/bank)		Participant's ID *(3 chars eg. BOZ)*	
Physical Address for delivery		Date	

1. BOZ ZIPSS/CSD SECURITY ADMINISTRATOR

1.1 Participant's User Security Administrator - PUSA

Full Name	Designation	User Name (Initial and Surname)	Email address	Telephone no

1.2 Alternative Participant's User Security Administrator					
	Full Name	Designation	User Name (Initial and Surname)	Email address	Telephone no

2. USER DETAILS

No	Full Name	Designation	User Name (Initial and Surname)	Email address	Telephone no

3. APPROVING OFFICERS - Authorized Signatories

No	Full Name	Designation	Email address	Telephone no	Signature
3.1					
3.2					
3.3					

10.2 E-Token Application Form

Bank *of* Zambia

BOZ ZIPSS/CSD SYSTEM

e-TOKEN APPLICATION FORM

Form No BOZ ZIPSS/CSD CA02

Name of Participant (organization/bank)		Participant's ID *(3 chars)*	
Physical contact for Collection			

1. APPLICATION DETAILS

Name of Originator *(Participant's User Security Administrator - PUSA)*						**Date of Application**	
Subscriber's First name		Initial *(optional)*		Surname			
Subscriber's Designation							
User ID (*assigned by PUSA*)							
Subscriber's E-mail address							
e-Token Usage *(Tick where applicable)*	BOZ ZIPSS/CSD Only		CSD Only		Both BOZ ZIPSS/CSD & CSD		
User Profile *(To be ticked by PUSA)*	**Inputter**	**Authorizer**		**Administrator**		**Other (Specify)**	

2. AUTHORIZATION

Participant's Authorized Signatories (Registered with the Bank of Zambia)

2.1 BOZ ZIPSS/CSD SYSTEM

	Name	Designation	Comment	Signature	Date
1.					
2.					

2.2 CSD SYSTEM

	Name	Designation	Comment	Signature	Date
1.					
2.					

3. **APPROVALS** *at Bank of Zambia*

3.1 BOZ ZIPSS/CSD Approval Manager *(BCPS Department)*

	Name	Designation	Comment	Signature	Date

3.2 CSD Approval Manager *(Financial Markets Department)*

	Name	Designation	Comment	Signature	Date

4. e-Token Issuance *– Only issue after all above information is provided and form is duly signed*

Date Received		Time Received	
Subscriber's Name		BOZ ZIPSS/CSD User ID	

Certificate Issuance Approval (*Tick)*	Yes		No	
Reason if not approved				
Name of BOZ CA Approver		Signature	Date	

e-Token Serial No		Certificate ID	
Issue No		Renewal No	
Date of Issue		Expiry Date	
Issued by: (*BOZ CA Security Administrator – CASA*)		Signature	

5. **Delivery to BOZ BOZ ZIPSS/CSD Service Desk**

	Name	Signature	Date	Time
Received by BOZ ZIPSS/CSD Service Desk for Collection				

10.3 E-token Revocation Form

Bank *of* Zambia

BOZ ZIPSS/CSD SYSTEM

e-TOKEN REVOCATION FORM

Form No BOZ ZIPSS/CSD CA03

Name of Participant (organization/bank)		Participant's ID *(3 chars)*	
Physical Address			

1. REQUEST DETAILS

Name of Originator *(Participant's User Security Administrator - PUSA)*				**Date of Application**	
e-Token Serial No			Certificate ID		
Subscriber's First name		Initial *(optional)*		Surname	
Subscriber's Designation					
User ID			Subscriber's E-mail address		
Reason for Revocation					

2. AUTHORIZATION

Participant's Authorized Signatories (Registered with the Bank of Zambia)

2.1 BOZ ZIPSS/CSD SYSTEM

	Name	Designation	Comment	Signature	Date and Time
1.					
2.					

2.2 CSD SYSTEM

	Name	Designation	Comment	Signature	Date and Time

1.					
2.					

3. **APPROVALS** *at Bank of Zambia*

3.1 BOZ ZIPSS/CSD Approval Manager *(BCPS Department)*

	Name	Designation	Comment	Signature	Date and Time

3.2 CSD Approval Manager *(Financial Markets Department)*

	Name	Designation	Comment	Signature	Date and Time

4. e-Token Revocation *– Only action after all above information is provided and form is duly signed*

Date Received		Time Received	
Subscriber's Name		BOZ ZIPSS/CSD User ID	

4.1 Name of BOZ CA Approver

	Name	Designation	Comment	Signature	Date and Time

4.2 Revoked by BOZ CA Security Administrator – CASA

Date revoked		Time Revoked		Has Notification of Revocation been sent (Y/N)?	
Name			Signature		

11. REFERENCES

i) http://www.faqs.org/rfcs/rfc3647.html
ii) Electronic Communications and Transactions Act of 2009
iii) BOZ Information Security Policy