CERTIFICATION PRACTICE STATEMENT

Revision 1.0

Date of publication : 14th April 2022

Effective date : 26th April 2022

COPYRIGHT © 2022 POS DIGICERT SDN. BHD. ALL RIGHTS RESERVED

REVISION CONTROL AND CHANGE HISTORY

Revision Number	Approval Date	Approved by
Revision 1.0	26th April 2022	Collin Babirukamu

Table of Contents

(this space is intentionally left blank)

1.0 Introduction

This CPS outlines the information on POS DIGICERT certificate type and services for certificates issued under the following Root Certificates:

Root Certificate.
Uganda National ECC Root Certification Authority

1.1 Overview

The purpose of this CPS is to describe the policies, practices and procedures employed by POS DIGICERT to perform Certificate Authority services. It outlines the procedures of issuing, managing, suspending, revoking and renewing certificates. The CPS is intended to legally bind all parties that intend to use and validate certificates; governing their rights, duties and liabilities in this contract. This CPS meets the formal requirements of Internet Engineering Task Force (IETF) RFC 3647, dated November 2003 with regard to content, layout and format (RFC 3647 obsoletes RFC 2527). An RFC issued by IETF is an authoritative source of guidance with regard to standard practices in the area of electronic signatures and Certificate management. While certain section titles are included in this CPS according to the structure of RFC 3647, the topic may not necessarily apply to services of POS DIGICERT. These sections state 'No stipulation'. Additional information is presented in subsections of the standard structure where necessary. Meeting the format requirements of RFC 3647 enhances and facilitates the mapping and interoperability with other third party CAs and provides Relying Parties with advance notice of POS DIGICERT's practices and procedures. POS DIGICERT conforms to the current version of CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (the "Baseline Requirements, published at www.cabforum.org. If a discrepancy arises between interpretations of this document and the Baseline Requirements, the Baseline Requirements shall take precedence over this document. Additional assertions on standards used in this CPS can be found under the respective titles / headers in this CPS wherever applicable.

The CPS is divided into 9 chapters:

Chapter 1 provides preliminary information pertaining to this CPS.

Chapter 2 outlines the important legal provisions. In this section, POS DIGICERT's obligations, limitations and warranties will be highlighted.

Chapter 3 explains the procedures and operational requirements for the application, issuance, revocation and renewal of certificate. A life-cycle approach is used to describe the certification process.

Chapter 4 explains on the operational requirements for certificate and CRL management, records management and log procedures.

Chapter 5 demonstrates the Physical, Procedure and Personnel Security Controls employed by POS DIGICERT in providing trustworthy certification services.

Chapter 6 demonstrates the Technical Security Controls for key management, network management and system development.

Chapter 7 describes the specific certificate and CRL produced and used by POS DIGICERT in providing certification services.

Chapter 8 outlines the important legal provisions. In this section, POS DIGICERT's obligations, limitations and warranties will be highlighted.

Chapter 9 describes financial responsibilities, insurance coverage, information disclosure and responsibility to protect private information.

It is important that potential subscribers fully understand the contents of this CPS before submitting a certificate application.

1.2 Document Name and Identification

In compliance with the Ugandan's Electronic Signatures Act, 2011(hereinafter referred to as the "ESA") and Ugandan's Electronic Signatures Regulations 2013 (hereinafter referred to as the "ESR"), this CPS intends to prescribe all matters concerning POS DIGICERT as CA and the certification services including certificate issuance and management, operation of certification systems, and responsibilities and liabilities of the related parties such as POS DIGICERT, (Registration Authority) RA and its Subscribers.

1.3 PKI Participants

Trust Infrastructure

POS DIGICERT's public key certification services are intended for local and foreign organisations and individuals (end-entities) to conduct secure electronic commerce in the open communication network. To achieve this objective, three key aspects must be adequately addressed:

- a robust PKI trust model to facilitate the management, control, issuance, revocation and renewal of digital certificates;
- the effective use of digital signatures in ensuring non-repudiation, authentication and integrity of electronic documents and transactions; and
- the uniformity of service and standards across POS DIGICERT and its appointed RAs.

A simplified overview of POS DIGICERT's PKI model can be diagrammatically represented as follows:

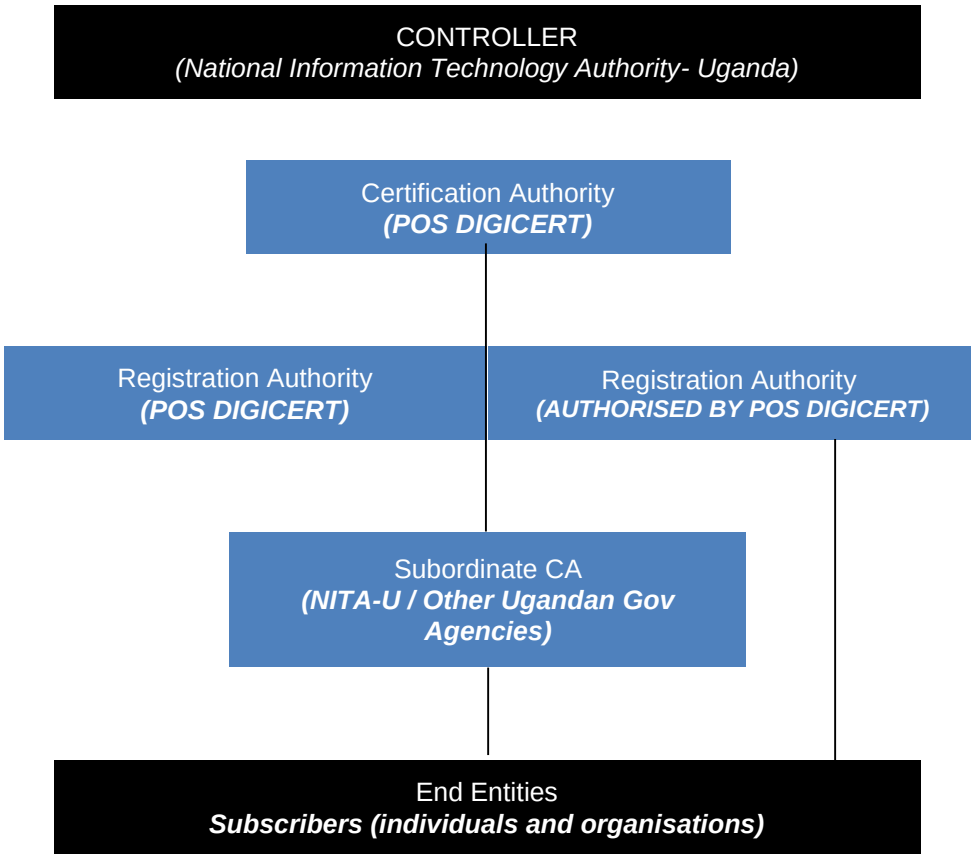

Figure 1 : POS DIGICERT PKI TRUST MODEL

Controller of CA

The function of the Controller of CA ('the Controller') is conceived under the ESA. The Controller is designated by the Minister to monitor, regulate and ensure the legitimacy of CA operations in Uganda.

The Office of the Controller is the regulatory agency established under the jurisdiction of the National Information Technology Authority- Uganda. It is fully empowered to issue licenses to CAs and certificates of recognition to Repository and Foreign CA. The Office of the Controller is not an entity in POS DIGICERT's PKI hierarchy.

1.3.1 Certification Authorities

POS DIGICERT is a licensed CA operating in compliance with the requirements of the ESA and the ESR. In electronic commerce, trust involves the combination of secure technology with reliable, visible processes for the identification and authentication of all parties. POS DIGICERT uses a trustworthy certificate management system to provide public key certification services to its subscribers.

The policies and practices adopted by POS DIGICERT are as important as the security attributes of the certificate management system. POS DIGICERT ensures that the policies and practices conform to industry standard POS DIGICERT's public key certification services have been designed to address the requirements of a diverse group of users as well as to comply with the ESA and ESR. This CPS sets out POS DIGICERT's practices to ensure the uniformity of its services and standards. POS DIGICERT's RAs will operate in accordance with the requirements of this CPS.

POS DIGICERT Root CA and other issuing CA are also owned and operated by POS DIGICERT. The key length is 2048 bits and it is created in a trustworthy environment. The Root CAs are categorised according to the certificate policies. Therefore, there can be a chain of certificates in support of each digital signature.

POS DIGICERT acts as the main naming authority in the PKI structure. The naming convention for all subjects of certificates registered through RAs will be determined by POS DIGICERT. The naming convention for Sub CA will be determined by POS DIGICERT on request from the respective Sub CA.

If the recipient does not know the CA of the signer of a given message, the recipient can search for the CA's certificate from the recognised repositories. Recipients are also advised to refer to the Controller's web site to view the CA's licence and disclosure record.

1.3.2 Registration Authorities

RAs are trusted entities appointed by POS DIGICERT to assist subscribers in applying for certificates, to approve certificate requests and/or to help POS DIGICERT in revoking certificates. The functions that the RAs shall carry out vary from case to case but shall also include personal authentication, token distribution, revocation reporting, name assignment and subscriber's key generation request.

The organisations that are appointed as Registration Authority (RA) for POS DIGICERT Sdn. Bhd. shall be officially published on POS DIGICERT's website and other printed materials deemed necessary ad copyrighted by POS DIGICERT. The list of POS DIGICERT's RA (if any) shall be available at www.posdigicert.com.my.

1.3.3 Subscribers

End-entities are subscribers of CA services. They could be individuals or organisations who hold and/or rely on digital certificates in electronic transactions. End-entity need not necessarily be a natural person; it could also be a certificate using system such as a secure web server or any organization. Each end-entity could own as many certificates as it needs and may use them for different purposes.

1.3.4 Relying Parties

Relying parties are entities that rely in a certificate or digital signature issued by the CA. Relying parties must verify the validity of the digital certificate by checking the appropriate Certificate Revocation List (CRL) prior to relying on information featured in a certificate.

1.3.5 Other participants

No stipulation

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

POS DIGICERT Root certificates can be used to issue digital certificates that require authentication for public domain transaction. End entity certificate or digital certificates issued under POS DIGICERT Root certificates may be used by the subscribers for the purpose of authentication, digital signature and data encryption.

1.4.2 Prohibited certificate uses

Any usage of end entity certificate issued by POS DIGICERT that inconsistent with key usage and extended key usage features in certificate extension is prohibited. For server certificates, if the domain names are related to either gambling / prostitution / terrorism / pornography it will be considered as High Risk by POS DIGICERT. If the domain names are within the High Risk definition, the application for the certificate shall be rejected.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The POS DIGICERT CPS is administered by the POS DIGICERT's Policy Authority which is based on the policies established by POS DIGICERT.

1.5.2 Contact person

Subscribers are advised to refer to POS DIGICERT's website at www.posdigicert.com.my for relevant information and assistance. For further assistance, please contact:

Pos Digicert Sdn Bhd (457608-K)
No. 8-3A-02, Star Central, Lingkaran Cyberpoint Timur,
63000 Cyberjaya, Selangor, Malaysia
Tel: +603 8800 6000 Fax: +603 8800 6088

For any business inquiries, Certification services, PKI and technical inquiries please email to customercare@posdigicert.com.my.

1.5.3 Person Determining CP Suitability for the Policy

This CPS is reviewed annually and any subsequent changes are approved by the Management of POS DIGICERT.

1.5.4 CP Approval Procedures

As stipulated in CPS Part 1.5.3.

1.6 Definitions and Acronym

1.6.1 Definitions

This document makes use of the following defined terms:

Term	Definition
AATL	Adobe Approved Trust List
AP	Authorised Personnel
Asymmetric cryptosystem	An algorithm or series of algorithms that provide a secure key pair.
Authentication	A process used to confirm the identity of a person or to prove the integrity of specific information.
Certificate	A computer-based record which – • identifies the certification authority issuing it; • names or identifies its subscriber; • contains the subscriber's public key; and • is digitally signed by the certification authority issuing it.
Certification Authority (CA)	An authority who issues a certificate.
Certification Authority Disclosure Record	An on-line and publicly accessible record which concerns a licensed certification authority which is kept by the Controller.

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.
Certificate Policy	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 Practice Statement	A declaration of the practices which a certification authority employs in issuing certificates generally, or employed in issuing a particular certificate.
Certification Revocation List (CRL)	A list of revoked certificates.
Controller	The Controller of Certification Authorities appointed under Section 26 of the ESA.
Digital Signature	A transformation of a message using an asymmetric cryptosystem so that a person having the initial message and the signer's public key can accurately determine whether the transformation was created using the private key that corresponds to the signer's public key; and whether the message has been altered since the transformation was made.
eKYC	Electronic Know Your Customer is a process to validate the identity of a certificate subscriber. POS DIGICERT uses a dedicated eKYC app to perform this function.
ESA	Electronic Signatures Act 2011
ESR	Electronic Signatures Regulations 2013
Electronic Data Interchange (EDI)	Technology involving computer-to-computer exchange of structured data between two or more companies sent in a form that allows automatic processing, with no manual intervention. It is relevant to any business that regularly exchanges information, for example, client or company records, but is especially relevant if you send and receive orders, invoices, statements and payments.
HSM	HSM is an acronym for Hardware Security Module. It is a physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing.
Issue a Certificate	The act of a certification authority in creating a certificate and notifying the subscriber listed in the certificate of the contents of the certificate.
Key Pair	A private key and its corresponding public key in an asymmetric cryptosystem, where the public key can verify a digital signature that the private key creates.
Licensed Certification Authority	A certification authority to whom a licence has been issued by the Controller and whose licence is in effect.
Message	A digital representation of information.
NITA-U	National Information Technology Authority- Uganda
Notify	To communicate a fact to another person in a manner reasonably likely under the circumstances to impart knowledge of the information to the other person.
Object Identifier (OID)	A value comprised of a sequence of integer components, which can be assigned to a registered object and which has the property of being unique among all object identifiers.
Offline	Walk-in / courier registration submissions.
Online	Registration submission done over the internet via web portal / dedicated online system.
Person	A natural person or a body of persons, corporate or unincorporated, capable of signing a document, either legally or as a matter of fact.
Policy Qualifier	Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.
POS DIGICERT	Pos Digicert Sdn Bhd
Private key	The key of a key pair used to create a digital signature.

Provisions	A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS employing the approach described in this framework.
Public key	The key of a key pair used to verify a digital signature.
Publish	To record or file in a repository.
Recipient	A person who receives or has a digital signature and is in a position to rely on it (see Relying Party).
Recognised Repository	A repository recognised by the Controller under Section 77 of the ESA.
Reliance Limit	The monetary amount recommended for reliance on a certificate under Section 75 of the ESA.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (e.g., a RA is delegated certain tasks on behalf of a CA).
Relying Party	A recipient of a certificate who acts in reliance on that certificate and/or digital signature verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.
Repository	A system for storing and retrieving certificates and other information relevant to digital signatures.
Representative	A person representing the actual applicant.
Revoke Certificate	To make a certificate ineffective permanently from a specified time forward.
RSA	The first significant asymmetric cryptographic algorithm; the initials stand for Rivest, Shamir and Adleman, its inventors. Note that RSA can also refer to a particular commercial entity; see RSA DSI. RSA is protected by US patents held by RSA DSI. It is not protected outside the US.
Sub-CA	Sub-CAs are allowed to be created for different organizations and agencies, for ease of operations and management. However, Sub-CAs shall be created purely in a technical context, to be part of the POS DIGICERT's technical infrastructure. The keys created for Sub-CA shall be located only on POS DIGICERT's technical infrastructure. The certificate issuing authority for the Sub-CA shall remain only with POS DIGICERT.
Subscriber	A person who - • is the subject listed in a certificate; • accepts the certificate; and • holds a private key which corresponds to a public key listed in that certificate
Suspend a Certificate	To make a certificate ineffective temporarily for a specified time forward.
Trustworthy System	Computer hardware and software which- • are reasonably secure from intrusion and misuse; • provide a reasonable level of availability, reliability and correct operation; and • are reasonably suited to performing their intended functions.
Uniform Resource Locator (URL)	A standardised addressing scheme which identifies a particular Internet resource, such as a Web page, a gopher server, a library catalogue, an image, or a text file.
Valid Certificate	A certificate which- • a licensed certification authority has issued; • has been accepted by the subscriber listed in it; • has not been revoked or suspended; and • has not expired: • Provided that a transactional certificate is a valid certificate only in relation to the digital signature incorporated in it by reference.
Verification of Digital Signature	In relation to a given digital signature, message and public key, to determine accurately that- • the digital signature was created by the private key corresponding to the public key; and • the message has not been altered since its digital signature was created.

Writing / Written	Includes any handwriting, typewriting, printing, electronic storage or transmission, or any other method of recording information or fixing information in a form capable of being preserved.

1.6.2 Acronyms

ARL	Authority Revocation List
CA	Certification Authority
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
ESA	Electronic Signatures Act 2011
ESR	Electronic Signatures Regulations 2013
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol with SSL
ISO	International Standard Organisation
ITU	International Telecommunications Union
PIN	Personal Identification Number
PKI	Public Key Infrastructure
NIN	National Identification Number
RA	Registration Authority
RP	Registration Personnel
RSA	Rivest, Shamir, Adleman
URL	Uniform Resource Locator
WWW	World Wide Web
X.509	ITU-T standard for certificates format

1.6.3 References

RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.

WebTrust Principle and Criteria for Certification Authorities, Principles and Criteria for Certification Authorities -Version 2.2.1

1.6.4 Conventions

No stipulation.

2.0 Publication and Repository Responsibilities

2.1 Repositories

POS DIGICERT shall operate as a recognised repository that fully complies with the requirements of the ESA and the ESR. The repository contains certificates of subscribers and POS DIGICERT CA root certificates. POS DIGICERT publishes all CA Certificates, revocation data for issued Certificates, and CPS in Repositories. POS DIGICERT ensures that revocation data for issued Certificates and its Root Certificates are available through a Repository 24 hours a day, 7 days a week with a minimum of 99.5% availability overall per year.

POS DIGICERT refrains from making publicly available sensitive and/or confidential documentation including security controls, operating procedures and internal security policies. These documents are, however, made available to auditors assigned by the Ugandan Electronic Signature Act 2011 as required during any WebTrust Audit performed on POS DIGICERT.

2.2 Publication of certification information

POS DIGICERT shall publish all information regarding its services and business practices in its publicly accessible repository at www.posdigicert.com.my. POS DIGICERT is obliged to publish this information to inform or educate its subscribers on the subject related to PKI and digital signatures. Notice of revocation shall be published in the form of CRL and ARL.

2.3 Time or frequency of publication
POS DIGICERT may consider sending bulletin or newsletter in the form of an email to inform subscribers of its new services or updates and changes in its services or practices as and when necessary. Frequency of publication of CRL is specified in **CPS Part** 4.9.7.

2.4 Access Controls on Repositories
POS DIGICERT does not impose any restrictions of access control to the information publish at its web site, which includes the CA certificate, latest CRL and a copy of this document. POS DIGICERT imposes a more restricted access control policy to the repository at its discretion.

3.0 Identification and Authentication
3.1 Naming
POS DIGICERT CA ensure that all subject information submitted shall conform and verified in accordance with the requirements and procedures prescribed in this CPS and matches the information confirmed and documented by the Registration Authority pursuant to its verification processes prior to certificate issuance.

3.1.1 Type of Names
Each CA Applicant must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate subjectName field. Information contained in Individual Certificate are the real name as per the Ugandan NIN or Passport, NIN Number or Passport Number and E-mail Address.

3.1.2 Need for Names to be Meaningful
The Subject Name must have a reasonable association with the authenticated name of the subscriber.

3.1.3 Anonymity or pseudonymity of subscribers
POS DIGICERT may not issue end entity anonymous or pseudonymous certificate.

3.1.4 Rules for Interpreting Various Name Forms
As stipulated in **CPS Part** 3.1.1 and 3.1.2.

3.1.5 Uniqueness of Names
POS DIGICERT verifies the uniqueness of Subscribers DN (Distinguished Name).

3.1.6 Recognition, Authentication, and Role of Trademarks
This CPS, and the information which it contains, is the property of POS DIGICERT and its affiliates and licensors, and is protected from unauthorised copying and dissemination by Ugandan copyright law, trademark law, international conventions and other intellectual property laws. POS DIGICERT is a trademark or a registered trademark of POS MALAYSIA BERHAD and/or POS DIGICERT SDN BHD in Malaysia and certain countries. All POS DIGICERT product names and logos are trademarks or registered trademarks of POS DIGICERT. All other company and product names and logos are trademarks or registered trademarks of their respective owners in certain countries.

3.2 Initial Identity Validation
As stipulated in **CPS Part** 3.1

3.2.1 Method to Prove Possession of Private Key
In the event that the key pair is generated by the certificate applicant, the possession of the private key, shall be proven by sending the certificate signing request (CSR) or the application via online registration system, which includes its public key, to POS DIGICERT.

3.2.2 Authentication of Organization Identity
No stipulation

3.2.3 Authentication of Individual Identity
The RP of POS DIGICERT or its RA or the appointed Authorised Personnel is principally responsible for ensuring that the required information is obtained from the subscriber prior to approving the application for a certificate. The application must be rejected should the information be incomplete or is discovered to be inaccurate upon investigation.

The following section will outline the procedures in applying for and reviewing of a certificate application. The table below specifies the requirements for obtaining certificates. The table briefly describes the certificate application process based on the certificate policies. Mandatory requirements will be highlighted where necessary.

Class 2 Certificate (Individuals)

Attribute	Details
Level of trust	Intermediate / High (depending on the media user)
Assurance	The subscriber is not a falsely created person insofar as the records of the subscriber's identity are maintained by reliable and independent third parties. RAs and Sub CA provide that the subscriber is as portrayed by the information provided by government agencies. Trust is based on confirmation of the subscriber's identity. This is done through online submission or physical presentation of the identification documents. Alternatively, identities may be confirmed against a reliable third party database. For example, the RA could request for the original identification document (see **CPS Part** 4.1). All material representations made by the subscriber to POS DIGICERT, including all information known to the subscriber and represented in the certificate, shall be accurate and complete to the best of the subscriber's knowledge.
Issued to	Ugandan and foreign individuals (aged 18 years and above).
Validation	Strict verification and authentication by the CA, RA, its appointed AP or a reliable database is required for software certificates. Confirmation is based upon the official identification document issued by government agencies (e.g.: NIN / Passport). Additionally, wherever applicable a letter of authorisation from the relevant agency that the certificate is to be used for shall be provided by the applicant. Pos Digicert also utilises its own eKYC solution as its user authentication and validation tool. The reliability of the information is determined at the sole discretion of the CA, RAs or Sub CA or database owner.
Possible usage	Class 2 individual certificates are used for communications requiring various levels of security. Some possible applications include on-line registration via the web, validation of user-identity for downloading of software or software upgrades and communication of user-ID creation within an organisation. For AATL certificates, it is used to provide document recipients with improved assurance that certified PDF documents are authentic via automatic online PDF validation provided by Adobe.
Certificate Application Process and Its Requirements	• Available to all Ugandan and foreign individuals who are 18 years and above. • An authorisation letter is required if a representative / agent is appointed to apply for the certificate. • Online registration can be made via POS DIGICERT's online registration system or via its appointed RA. • Identification documents required to accompany the application is either; copy of NIN or Passport. A selfie photo would also be required for authentication and validation via eKYC. • For online applications, the photocopy of NIN / Passport supplied MUST be certified true copy by the organisation's Head of Department / Director.

	• For all Sub CA applications, requests shall have to come from the organisation assuming the role of Sub CA itself, subject to prior arrangement between POS DIGICERT and the Sub CA.
Information Required for Certificate Issuance	• name (as indicated on the applicant's NIN or Passport); • email address; • the telephone number; • postal address (this should be the place where the applicant will reside for more than one year in the immediate future, if no such place is available, the current place of residence will suffice); • a copy of new NIN / Passport number; • date of birth; • gender; • challenge pass phrase (if applicable) any other information required as stated in POS DIGICERT's application form (printed / online form)
List of Intermediate Certificates Affected	• IndividualSign ECC Intermediate Certificates

3.2.4 Non-Verified Subscriber Information
For all Certificate types, POS DIGICERT must validate all information of the subject to be included within the Subject DN of a certificate. POS DIGICERT may include specific disclaimers or notices to identify non-verified Subscriber information to Relying Parties.

3.2.5 Validation of Authority
As stipulated in **CPS Part** 3.2.3

3.2.6 Criteria for Interoperation
As stipulated in CPS Part 2.1

3.2.7 Authentication of Domain Name and Country Name
No stipulation.

3.3 Identification and Authentication for Re-Key Requests
3.3.1 Identification and Authentication for Routine Re-Key
The certificate renewal process is similar to an application for a new certificate unless agreed upon the relying parties between the Certification Authority and the Sub CA subscriber. The certificate renewal is also technically defined as "rekey" and often used interchangeably. However, for all classes of certificates with the exception of Class 1, the subscriber only needs to provide information that has changed since the expiration date of the certificate. Class 1 certificates can only be renewed by re-applying for a new certificate using the same procedure as described in **CPS Part** 4.2. Subscribers shall be solely responsible to update POS DIGICERT in regards to any information changes during this renewal process.

3.3.2 Identification and Authentication for Re-Key After Revocation
POS DIGICERT CA and RA do not renew POS DIGICERT Certificates that have been revoked. If a Subscriber wishes to use POS DIGICERT Certificate after revocation, the Subscriber must apply for a new certificate and replace the certificate that has been revoked.

3.4 Identification and Authentication for Revocation Request
Subscriber may request revocation of their POS DIGICERT Certificate at any time through validation by RA that processed the Subscriber's POS DIGICERT Certificate application. RA shall validate that the Subscriber is the person, organization, or entity to whom the POS DIGICERT Certificate was issued. The RA shall authenticate a request from a Subscriber for revocation of the certificate by validating the request against the records in the application / system / database.

4.0 Certificate Life-Cycle Operational Requirements
4.1 Certificate Application
As stipulated in **CPS Part** 3.2.2 & 3.2.3

4.1.1 Who can Submit a Certificate Application
As stipulated in **CPS Part** 3.2.2 & 3.2.3

4.1.2 Enrolment Process and Responsibilities
As stipulated in **CPS Part** 3.2.2 & 3.2.3

4.2 Certificate Application Processing
4.2.1 Who Can Submit a Certificate Application?
POS DIGICERT maintains systems and processes to sufficiently authenticate the Applicant's identity in compliance with this CPS. Initial identity vetting may be performed by POS DIGICERT's validation team as set forth in CPS Part **3.2** or by Registration Authorities under contract. All communications sent through as email are securely stored along with all information presented directly by the Applicant via the online registration system.

4.2.2 Enrolment Process and Responsibilities
As stipulated in **CPS Part** 3.2.2 & 3.2.3

4.2.3 Certificate Application Processing
POS DIGICERT will make reasonable efforts to adhere to the following time-schedule in issuing certificates. However, no guarantees can be provided as circumstances beyond the control of POS DIGICERT may inhibit such adherence. In particular, the timeliness of the following schedule will depend on the amount of co-operation received from the subscriber, including but not limited to payment, and the provision of accurate and complete information. Incomplete application forms will invariably cause the application to be delayed or rejected.

All time frames quoted depend upon the receipt of the confirmation to proceed with the application from the applicant. The following sets out the time-schedule for the issuance of certificates:

Class 2 and AATL certificate
For online applications, soft certificates (Basic and Enhanced), the issuance and setting of PIN is immediate. The PIN shall be set by the subscribers themselves via the online registration system. For other mode of applications involving soft cert, PKI Token, smart card (Basic and Enhanced) or HSM, the issuance requires 5 business days, and the PIN number will be sent separately on the certificate issuance day via regular mail. For Sub CA, the issuance is as per agreement with the Sub CA itself.

4.3 Certificate Issuance
4.3.1 CA Actions During Certificate Issuance
Certificate issuance by POS DIGICERT Root CA requires an authorised Trusted Role member from POS DIGICERT to issue a direct command for the Root CA to perform a certificate signing operation. POS DIGICERT shall ensure it communicates with any RA accounts capable of causing Certificate issuance using multi-factor authentication. This includes RAs directly operated by POS DIGICERT or RAs contracted by POS DIGICERT. RAs shall perform validation of all information sent to the CA and ensure that any database used to store any information is suitably protected from unauthorized modification or tampering.

4.3.2 Notifications to Subscriber by the CA Issuance of Certificate
As stipulated in **CPS Part** 3.2.1

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Certificates are issued to the subscribers upon successful processing of the application and the acceptance of the certificates by the subscribers.

Subscribers demonstrate their acceptance of the certificate by adhering to the following procedures:

Attribute	Details
Class 2 (Individual & Organisation)	For AATL certificate it shall only be provided in HSM. For soft certificate the subscribers will be requested to create a PIN number to access the private key via the online registration system. Subscriber indicates acceptance by receiving / downloading the certificate from POS DIGICERT or its RAs and / or usage of the digital certificate whichever comes first.
Class 2 (Sub CA)	The subscriber shall receive the certificate and the related private key in a media agreed upon by the Sub CA and POS DIGICERT. Similar to Class 2 (Basic / Enhanced) unless indicated in the agreement between POS DIGICERT and the Sub CA.

The subscriber is advised to verify all details contained within the certificate. Errors or omissions must be communicated immediately to POS DIGICERT. It is imperative that the subscriber is aware of this requirement. POS DIGICERT's scope of responsibility extends only to ensure that the information contained within the certificate accurately reflects the information that was provided to POS DIGICERT by the subscriber during the application stage.

4.4.2 Publication of the Certificate by the CA

As stipulated in **CPS Part** 2.2

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

As stipulated in **CPS Part** 3.2.1

4.5 Key Pair and Certificate Usage

The certificates containing public key that is intended for verifying digital signature created using the corresponding private key, should only be used for its intended usage. Certificates shall not be used in an illegal or discriminatory manner including, but not limited to, trafficking of illegal material, engaging in activities that compromise national security and utilising the certificate for accessing illegal material. If certificates are used in an illegal manner, POS DIGICERT will not hesitate to revoke the certificate without prior notice to the subscriber. In addition, future applications made by the subscriber shall be prejudiced against this.

4.5.1 Subscriber Private Key and Certificate Usage

It is the responsibility of the subscriber to ensure that all the information that has been provided to a RA for the purpose of obtaining a certificate is accurate and kept up-to-date as soon as practicable. Subscribers are to maintain the integrity of the private key of the corresponding public key pair that is kept in POS DIGICERT's repository. POS DIGICERT will not be held liable, be in breach of this CPS, negligent, or be subject to any form of liability as a result of a breach in the integrity of the private key. Subscribers must inform POS DIGICERT or its RAs within 48 hours of a change to any information included in their certificate or certificate application request. Subscribers must also inform POS DIGICERT or its RAs within 8 hours of a suspected compromise of one/both of their private keys. Subscribers are not to submit to POS DIGICERT or its RAs any material that is offensive, racially discriminative or prejudiced in any other manner, obscene, pornographic, illegal, hateful within the context of Ugandan laws or the subscriber's local applicable law (where there is discrepancy between the laws, Ugandan law will take precedence), or stolen. The list provided is not meant to be exhaustive. In a more general term, the material submitted must not be of such a manner that it will;

- violate any law whether Ugandan or otherwise; and / or
- causes POS DIGICERT or its RAs be liable for breach of a law whether Ugandan or otherwise.

4.5.2 Relying Party Public Key and Certificate Usage
The relying parties are obliged to:

- restrict reliance on the certificates issued by POS DIGICERT to the appropriate usage for those certificates in accordance with this CPS and with the certificate policy under which the certificate was issued;

- verify certificates before verifying a digital signature, including the use of CRLs and, in accordance with the certification path validation procedure specified in ITU-T Rec. X.509:19971 ISO/IEC 9594-8 (1997), taking into account any critical extensions; and

- trust and make use of certificates only if a valid certificate chain is established between the relying party and the certificate owner.

4.6 Certificate Renewal
Certificates issued by POS DIGICERT must be renewed periodically. All certificates issued by POS DIGICERT have a validity period of six (6) months to three (3) years (whichever applicable). This complimentary certificate is issued for testing purpose only and is not be subjected to the ESA / ESR.

4.6.1 Circumstances for Certificate Renewal
As stipulated in **CPS Part** 3.2.2, 3.2.3 & 3.3

4.6.2 Who may Request Renewal
As stipulated in **CPS Part** 3.2.2, 3.2.3 & 3.3

4.6.3 Processing Certificate Renewal Requests
POS DIGICERT may require reconfirmation or verification of the information in a certificate prior to certificate issuance.

4.6.4 Notification of New Certificate Issuance to Subscriber
As stipulated in **CPS Part** 3.2.1

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate
As stipulated in **CPS Part** 4.4

4.6.6 Publication of the Renewal Certificate by the CA
All POS DIGICERT certificates shall be published to POS DIGICERT's repository and deliver it to the Subscriber as stipulated in **CPS Part** 2.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities
As stipulated in **CPS Part** 3.2.1

4.6.8 Notice of Expiration
POS DIGICERT will provide notice to the subscriber on the expiry date as follows:

Notice	ALL CERTIFICATE TYPE
First	30 days prior
Second	14 days prior
Third	7 days prior

The time frames specified above are relative to the expiry date of the certificate. For example, Class 2 certificate users will be notified initially one month prior to the expiry date; the notification will be sent again one week prior to the expiry date.

The expiry notice time frames for certificate issued by RA and Sub CA are similar to Class 2 unless indicated in the agreement between POS DIGICERT and the RA / Sub CA.

POS DIGICERT shall notify the subscriber by email. The contact information of the subscriber that was submitted during the application stage or that was subsequently updated in the digital certificate will be

used as the destination for the transmission of this reminder. Expired certificates will not be revoked or removed. Upon expiration of the certificate, subscribers can either:

- cease to be a subscriber; or
- renew the expired certificate.

4.7 Certificate Re-Key
4.7.1 Circumstances for Certificate Re-Key
As stipulated in **CPS Part** 3.2.2, 3.2.3 & 3.3

4.7.2 Who May Request Certification of a New Public Key
As stipulated in **CPS Part** 3.2.2, 3.2.3 & 3.3

4.7.3 Processing Certificate Re-Keying Requests
POS DIGICERT may require revalidation of the Subscriber prior to re-keying a certificate. POS DIGICERT shall comply requirements as stipulated in **CPS Part** 3.2.2, 3.2.3 & 3.3 for validation of the Subscriber.

4.7.4 Notification of New Certificate Issuance to Subscriber
As stipulated in **CPS Part** 3.2.1

4.7.5 Conduct Constituting Acceptance of a Re-Key Certificate
As stipulated in **CPS Part** 4.3.1

4.7.6 Publication of the Re-Keyed Certificate by the CA
All POS DIGICERT certificates shall be published to POS DIGICERT's repository and deliver it to the Subscriber as stipulated in **CPS Part** 2.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities
As stipulated in **CPS Part** 3.2.1

4.8 Certificate Modification
4.8.1 Circumstances for Certificate Modification
As stipulated in **CPS Part** 3.2.2, 3.2.3 & 3.3

4.8.2 Who May Request Certificate Modification
As stipulated in **CPS Part** 3.2.2, 3.2.3 & 3.3

4.8.3 Processing Certificate Modification Requests
POS DIGICERT may require performing verification on any information which may change in the certificate prior issuing modified certificate. POS DIGICERT shall comply requirements as stipulated in **CPS Part** 3.2.2, 3.2.3 & 3.3 for validation of the Subscriber.

4.8.4 Notification of New Certificate Issuance to Subscriber
As stipulated in **CPS Part** 3.2.1

4.8.5 Conduct Constituting Acceptance of Modified Certificate
As stipulated in **CPS Part** 4.3.1

4.8.6 Publication of the Modified Certificate by the CA
All POS DIGICERT certificates shall be published to POS DIGICERT's repository and deliver it to the Subscriber as stipulated in **CPS Part** 2.2

4.8.7 Notification of Certificate Issuance by the CA to Other Entities
No Stipulation

4.9 Certificate Revocation and Suspension
4.9.1 Circumstances for Revocation
Revocation of certificates can occur due to the reasons specified in **CPS Part** 4.9. In the event that POS DIGICERT believes or has reason to believe, due to reliable evidence or while acting in good faith,

that a certificate should be revoked, POS DIGICERT will take all necessary to do so even if this is without the consent of the subscriber. In most instances, the revocation occurs when there is a security breach of the private key or the certificate will materially affect the truth of the information reflected in the certificate and thus possibly mislead a person relying on that information. In the event that the subscriber requested for a revocation, POS DIGICERT will take all necessary precautions to verify the identity of the subscriber. Revocation will not proceed without the verification that the purported party is indeed the subscriber. Upon revocation of the certificate, POS DIGICERT shall within one business day indicate that it is revoked by updating the CRL. The CRL will be published in at least one recognised Repository at an interval specified in **CPS Part** 4.9.7. Subscribers with revoked certificates are allowed to reapply for a new certificate at the discretion of POS DIGICERT. Under no circumstances can the revoked certificate be reinstated to its original state after revocation.

4.9.2 Who Can Request Revocation?

Revocation can be requested by the following:

- Controller
- POS DIGICERT
- Subscriber

4.9.3 Procedure for Revocation Request

Revocation by POS DIGICERT:

In general, a revocation could be initiated by POS DIGICERT when one or a combination of the following conditions has occurred:

a) upon such instruction from the Controller or upon the requirements of an applicable law;
b) the certificate was not issued in accordance with the requirements of Section 70 of ESA;
c) certificates become unreliable due to the following:
d) breach of the private key's security including unauthorised use;
e) the information contained within the certificate as supplied by the applicant has changed in such a manner that it will be grossly inaccurate to allow the certificate to continue to be operative without it being withdrawn and updated;
f) the applicable obligations, terms and conditions under this CPS have been materially breached by the certificate holder; or
g) a material fact contained in the certificate is misstated or known to be misstated; or
h) non-payment of any certificate fees issued by POS DIGICERT or service fees; or
i) upon verifying against any blacklist record listing provided by any Ugandan government agencies.

The above list is not meant to be exhaustive but merely to highlight the more common cases of suspension or revocation. Should the revocation be carried out a notice of revocation will be sent to the subscriber. This notice will contain:

- a notice that the subscriber's certificate has been revoked;

POS DIGICERT shall notify the subscriber by email. The contact information of the subscriber that was submitted during the application stage or that was subsequently updated in the digital certificate will be used as the destination for the transmission of this notice.

Revocation by Subscriber:

Revocation by a subscriber can be initiated due to the following reasons:

a) breach of the private key's security including unauthorised use;

b) the media containing the private key is loss or damaged;

The above list is not meant to be exhaustive but merely to highlight the more common cases of suspension or revocation.

Subscribers are allowed to request for a revocation of certificate via the mobile apps or web based application provided to the Subscribers.

The informational content of the message channelled to POS DIGICERT to initiate revocation will depend on the mode of communication chosen. The following table will summaries this point and includes verification procedures to prevent malicious acts of sabotage where a certificate is revoked without the subscriber's knowledge:

Certificate Class	Verification procedures
Class 2 (Individual)	Subscribers are allowed to request for a revocation of certificate via the mobile apps or web based application provided to the Subscribers. The RA shall authenticate a request from a Subscriber for revocation of the certificate by validating the request against the records in the application / system / database.
Class 2 (Sub CA)	Subscribers shall provide the information as above to the Sub CA or POS DIGICERT upon request for revocation. Unless stated otherwise, POS DIGICERT shall assume all requests from Sub CA on behalf of subscribers as legitimate.

POS DIGICERT's decision on whether to revoke the certificate will be final. If the revocation is instructed by the Controller, notice will be sent to the subscriber before the revocation is made. The subscriber will be notified via email or regular mail when the certificate is revoked. Upon the successful revocation of the certificate, the Certificate Revocation List will be updated to reflect this fact within one business day after receiving the request of the revocation.

4.9.4 Revocation Request Grace Period
As stipulated in **CPS Part** 4.9.1

4.9.5 Time Within Which CA Must Process the Revocation Request
POS DIGICERT shall confirm a request for revocation and revoke a certificate within one business day after receiving both a subscriber's written request and evidence reasonably sufficient to confirm the identity of the person requesting the revocation or of the agent.

4.9.6 Revocation Checking Requirements for Relying Parties
An Authorized party shall only rely on a Certificate's contents after checking with the applicable CRL for the latest Certificate status information, either manually or automatically.

4.9.7 CRL Issuance Frequency
All revocation will be updated in the CRL automatically after the revocation at the system and POS DIGICERT shall publish the CRL in its repository and other recognised repository (if available) one business day after the certificate being revoked.

4.9.8 Maximum Latency for CRLs
As stipulated in **CPS Part** 4.9.7

4.9.9 On-Line Revocation/Status Checking Availability
Status of revocation will be made available in a publicly accessible Certificate Revocation List. POS DIGICERT shall publish the revocation status in the website, which POS DIGICERT deems appropriate.

4.9.10 On-Line Revocation Checking Requirements
An authorized party or relying party must confirm the validity and latest certificate status information via CRL as stipulated in **CPS Part** 4.9.6

4.9.11 Other Forms of Revocation Advertisements Available
POS DIGICERT may use other forms of publication for revoked certificates as described in POS DIGICERT's CPS.

4.9.12 Special Requirements Re-Key Compromise
POS DIGICERT or the RA shall use commercially reasonable efforts to notify the Relying Parties or Subscribers that their private key has been compromised. In the event of private key compromise, POS

DIGICERT shall generate a new signing key pair and corresponding Root Certificate and revoked the compromised certificate and publish a revised CRL within one business day.

4.9.13 Circumstances for Suspension
POS DIGICERT does not offer suspension services of certificates.

4.9.14 Who Can request Suspension
POS DIGICERT does not offer suspension services of certificates.

4.9.15 Procedure for Suspension Request
POS DIGICERT does not offer suspension services of certificates.

4.9.16 Limits on Suspension Period
POS DIGICERT does not offer suspension services of certificates.

4.10 Certificate Status Services
4.10.1 Operational Characteristics
As stipulated in **CPS Part** 4.9.7 and 4.9.9

4.10.2 Service Availability
POS DIGICERT provides certificate services 24 x 7 without interruption. POS DIGICERT shall publish the revocation status as stipulated in **CPS Part** 4.9.7.

4.10.3 Operational Features
As stipulated in **CPS Part** 4.9.7, 4.9.9 and 4.10.2

4.11 End of Subscription
For all certificate types, the certificate subscription may be end by revoking or allowing the certificate to expire without renewal request

4.12 Key Escrow and Recovery
4.12.1 Key Escrow and Recovery Policy and Practices
Escrow of private keys by an external third party is not performed.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices
Escrow of private keys by an external third party is not performed.

5.0 Facility, Management, and Operational Controls
5.1 Physical Controls
5.1.1 Site Location and Construction
POS DIGICERT's office is located at Cyberjaya, Selangor Darul Ehsan, Malaysia.
NITA-U's data centre is located at National Data Center, Plot 9, Calville Street, Kampala, Uganda.

5.1.2 Physical Access
Physical access to the POS DIGICERT is restricted to authorised personnel.

5.1.3 Power and Air Conditioning
POS DIGICERT deploys UPS system that shall ensure uninterrupted services for all CA systems and applications in case of power failures which all essential power is connected to standby generator system. POS DIGICERT uses air-conditioning system and raised floor to ensure optimum ventilation and protection.

5.1.4 Water Exposures
POS DIGICERT installs the core CA systems at a reasonable height to protect them from flood damage.

5.1.5 Fire Prevention and Protection
POS DIGICERT installs fire detector, portable fire extinguisher, and automatic fire extinguishing facilities to prevent the core certification systems from fire damage.

5.1.6 Media Storage
POS DIGICERT controls physical access to its major storage media that are stored in safes. POS DIGICERT critical system data is incrementally backed-up on a daily basis. Full back-ups are performed on a weekly, monthly and annual basis.

5.1.7 Waste Disposal
POS DIGICERT shreds and crushes documents, diskettes, and other items to prevent information from such materials from being leaked.

5.1.8 Off-Site Backup
POS DIGICERT maintains offline backup storage of subscriber certificates, including CRL for ten (10) years after the corresponding digital certificates are issued.

5.2 Procedural Controls
5.2.1 Trusted Roles
The roles and responsibilities of operative personnel employed by POS DIGICERT are segregated according to their CA function. The System Administrator and PKI Engineer have access to the computer that hosts POS DIGICERT CA software to maintain the POS DIGICERT PKI.

5.2.2 Number of Persons Required per Task
Critical CA operations need authorisation from at least one Security Officer. However, the following operations need authorisation from two Security Officers:

- adding and deleting Security Officer;
- creating CA keys;
- issuing cross-certificates;
- creating Key Encryption Card (used to encrypt and decrypt CA keys);
- activating a CA private key for signing activities

5.2.3 Identification and Authentication for Each Role
The individuals fulfilling any of the trusted roles in POS DIGICERT possess a smart card / token based certificate for initiating core CA processes. The smart card / PKI Token (which is protected by PIN) is stored in a secure place protected under a dual access control mechanism.

5.2.4 Roles Requiring Separation of Duties
As stipulated in **CPS Part** 5.2.1 and 5.2.2

5.3 Personnel Controls
5.3.1 Qualifications, Experience, and Clearance Requirements
All POS DIGICERT operative personnel are competent in their performance and shall provide reasonable assurance of their trustworthiness while serving in a trusted position in the trusted organisation.

5.3.2 Background Check Procedures
All operative personnel in POS DIGICERT are required to go through a stringent background check upon joining and on an annual basis.

5.3.3 Training Requirements
POS DIGICERT makes available training for their personnel to carry out CA or RA functions. Training includes CPS requirements, operation of the CA software and hardware, operational and security procedures, disaster recovery and business continuity management.

5.3.4 Retraining Frequency and Requirements
Refresher training of technical personnel is conducted as and when required.

5.3.5 Job Rotation Frequency and Sequence
POS DIGICERT shall conduct job rotation for all critical posts to provide continuity and integrity of CA service.

5.3.6 Sanctions for Unauthorised Actions
POS DIGICERT's policies and procedures specify the sanctions against personnel for unauthorised actions, unauthorised use of authority, and unauthorised use of systems.

5.3.7 Independent Contractor Requirements
Independent Contractor Personnel shall sign a non-disclosure agreement (NDA) as part of their initial terms and conditions of contract or employment.

5.3.8 Documentation Supplied to Personnel
POS DIGICERT makes available documentation including CPS, security policy, system environmental documents to personnel, during training or employment.

5.4 Audit Logging Procedures
5.4.1 Types of Events Recorded
All significant security events on POS DIGICERT CA software are automatically time stamped and recorded in audit trail files. These include but are not limited to the following events:

- successful and failed attempts to create, remove, login as, set reset and change passwords of and revoke privileges of POS DIGICERT's operative personnel and its Registration Officer;

- failed interactions with the directory including failed connection attempts, read and write operations by POS DIGICERT CA software; and

- all events related to certificate revocation, security policy modification and validation, POS DIGICERT CA software start-up and stop, database backup, attribute certificate, DN change, management, database and audit trail management, certificate life-cycle management and other miscellaneous events.

5.4.2 Frequency of Processing Log
Critical system events, access attempts and CA software operation events are logged on a daily basis. The audit trail is reviewed at least once per week.

5.4.3 Retention Period of Audit Log
The yearly backup of the audit trails files is retained for ten (10) years under normal operations.

5.4.4 Protection of Audit Log
The audit trail is stored in regular operating system flat files. Audit trail for CA software operation events is digitally signed to ensure integrity. Each log record contains the timestamp, the type of log entry and the identity of log event. A new audit trail file is created when the current audit trail file reaches a pre-set size. Only the authorised Manager or the Security Officer is authorised to view and process audit trail files.

5.4.5 Audit Log Backup Procedures
Audit trail files are backed up by the System Administrator on a daily, weekly and monthly basis. All files including the latest audit trail file are stored either in a LTO 4 Cartridge media or storage disks and kept in a secure archive facility.

5.4.6 Audit Collection System (Internal vs. External)
The audit trail accumulation system is part of the CA software system. The log can be viewed using a standard CA Software Administrative Module.

5.4.7 Notification to Event-Causing Subject
CA Operations personnel notify the security Officer when a process or action causes a critical security event or discrepancy.

5.4.8 Vulnerability Assessments
Events in the audit process are logged and reviewed, to monitor system vulnerabilities.

5.5 Records Archival

5.5.1 Types of Record Archived

All events related to certificate revocation, security policy modification and validation, POS DIGICERT CA software start-up and stop, database backup, attribute certificate management, DN change, database and audit trail management, certificate life-cycle management and other miscellaneous events are recorded and archived.

5.5.2 Retention Period for Archive

The archive of the POS DIGICERT CA database and audit trail files will be retained for at least ten (10) years.

5.5.3 Protection of Archive

The POS DIGICERT CA archive media is kept in a fireproof safe and retained in a restricted access facility to which only authorised personnel have access. Protection of the audit trail is as described in **CPS Part** 5.4.4.

5.5.4 Archive Backup Procedures

The archive files are backed up as they are created. Originals are stored on-site and housed with the POS DIGICERT CA system. Backup of the archive files is stored at a secure and separate geographic location.

5.5.5 Requirements for Time-Stamping of Records

No Stipulation.

5.5.6 Archive Collection System (Internal or External)

The archive collection system (backup facility) for the POS DIGICERT CA database is internal to the POS DIGICERT CA system. The archive collection system (backup facility) for the audit trail files is described in **CPS Part** 5.4.6.

5.5.7 Procedures to Obtain and Verify Archive Information

On monthly basis the archive tapes are retrieved by a PKI / System Engineer and verified to ensure that no damage or loss of data has occurred. If any loss has occurred, the backup archive is retrieved to become the new master archive and a new backup is produced.

5.6 Key Changeover

POS DIGICERT's key pairs will be retired from service at the end of their respective lifetimes as defined in **CPS Part** 6.3.2. New Certification Authority key pairs will be created as required to support the continuation of POS DIGICERT Certification Authority Services. POS DIGICERT will continue to publish CRLs signed with the original key pair until all certificates issued using that original key pair has expired. The Certification Authority key changeover process will be performed such that it causes minimal disruption to Subscribers and Relying Parties.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

POS DIGICERT will use its business continuity procedures that consist of process or steps to be taken in the event of disaster including corruption or loss of computing resources that can affect POS DIGICERT business or services. The business continuity plan is included in the audit scope to validate the effectiveness restoration process and the recovery plan. CA personnel in trusted role should be trained accordingly to ensure they operate accordingly to the procedures defined in the recovery plan.

5.7.2 Computing Resources, Software, and / or Data Are Corrupted

POS DIGICERT has established business continuity procedures that outline the action steps in the event of the corruption or loss of computing and networking resources, software and/or data.

5.7.3 Entity Private Key Compromise Procedures

If a CA's private key is compromised or suspected to be compromised, the CA shall perform the following procedures:

- inform Controller;

- inform subscribers, cross-certifying CAs and relying parties;
- terminate the certificates and CRLs distribution service for certificates/CRLs issued using the compromised private key;
- request the revocation of the CA's certificate.

If a RA's private key is compromised or suspected to be compromised, the RA SHALL inform the CA and request the revocation of the RA's certificate. If subscriber's private key is compromised or suspected to be compromised, the entity SHALL inform the relying parties and request the revocation of the entity's certificate. Subscriber may request to have new key. In the event of the POS DIGICERT private key being compromised, POS DIGICERT shall revoke and re-issue all certificates in use at that instant.

5.7.4 Business Continuity Capabilities after a Disaster
In the event of a natural or other type of disaster the operation of POS DIGICERT repository will be re-established at disaster recovery site.

5.8 CA or RA Termination
In the event that POS DIGICERT ceases operation, the Controller shall appoint another licensed certification authority to take over the certificates issued by the certification authority whose license has been revoked or surrendered or has expired and such certificates shall, to the extent that they comply with the requirements of the appointed licensed certification authority, be deemed to have been issued by that licensed certification authority. POS DIGICERT shall develop a termination plan accordingly to minimise disruption to Customers, Subscribers, and Relying Parties. Further information on RA termination it is detailed out in the RA Appointment Guideline which is available under the Repository Section on POS DIGICERT's website www.posdigicert.com.my.

6.0 Technical Security Controls
6.1 Key Pair Generation and Installation
6.1.1 Key Pair Generation
The POS DIGICERT CA and Sub CA signing key pairs are generated, as and when necessary through proper documented procedures, on hardware and are protected by the master encryption key. The master encryption key is stored in an ISO 7816 smart card, PKI Token or any other forms of crypto token. The digital signature key pair for the subscribers can either be generated by the CA software or, in some cases, by hardware token.

The keys generated by POS DIGICERT are generated by either hardware for CA Keys and subscriber's keys or software for subscriber's keys. However, hardware tokens, for example HSM, smart cards and PKI Tokens, are used to generate key pairs. Meanwhile for AATL certificates, the subscriber key pair is generated, stored and protected in HSM or the subscribers own the PKI Token which are FIPS 140-2 Level 3 compliant. The subscriber shall access the private key from the HSM / own PKI Token directly.

6.1.2 Private Key Delivery to Subscriber
If POS DIGICERT is requested to generate the key pair, the private key will be stored in either a smart card, PKI Token, virtual smart card or any other forms of token and shall be delivered securely to subscribers. For the key pair generated by the subscriber using standard browsers, no delivery of the private key is required.

6.1.3 Public Key Delivery to Certificate Issuer
If POS DIGICERT is requested to generate the key pair, the public key will be stored in either a smart card, PKI Token, virtual smart card or any other forms of token that contain the private key of an entity and shall be delivered securely to subscribers.

6.1.4 CA Public Key Delivery to Relying Parties
The CA verification public key (CA certificate) will be made available to subscribers in a recognised repository.

6.1.5 Key Sizes
POS DIGICERT Root CA signing key pair is 2048 bits and the signing key pair of other CA at the lower level of the PKI hierarchy at minimum of 2048 bits.

6.1.6 Public Key Parameters Generation and Quality Checking
POS DIGICERT employs and recommends its subscribers to use digital signature schemes approved by the ESA and the ESR. No stipulation for parameter quality checking.

6.1.7 Key Usage Purpose (as per X.509 v3 Key Usage Field)
Certificates issued by POS DIGICERT contain the KeyUsage certificate extension restricting the purposes to which the certificate can be applied. The signing key pair is used to provide authentication, integrity and support for non-repudiation services. The POS DIGICERT CA and Sub CA signing key is used to sign certificates; CRLs issued by POS DIGICERT. The encryption key pair is used to protect a symmetric key used to encrypt data, and provides confidentiality services.

6.2 Private Key Protection and Cryptographic Module Engineering Controls
6.2.1 Cryptographic Module Standards and Controls
The cryptographic module used by POS DIGICERT CA hardware to generate keys is designed to comply with international standards (FIPS 140 – 2 Level 3). The key pairs are generated by the CA's HSM which is owned by the subscriber.

6.2.2 Private Key (n out of m) Multi-Person Control
Actions that require the authorisation from two persons include:

- assigning/removing Registration Officer privileges to/from Security Officer;
- creation of new certificate policies;
- activating a given CA's private key to initiate certificate generation;
- generation of CA key pair; and
- cross-certifying with other CAs.

Any other actions besides the above only requires the authorisation from a single person.

6.2.3 Private Key Escrow
Escrow of private keys by an external third party is not performed.

6.2.4 Private Key Backup
The POS DIGICERT CA private keys are backed up in the CA database in an encrypted format. The subscriber's private signing key is never backed up, to provide support for non-repudiation services. The POS DIGICERT signing key is encrypted and its integrity is protected by the CA master keys stored in the smart card. The CA database is backed up at a minimum on a daily basis. Recovery of information from the CA database can only be done by the Security Officer and PKI Engineer.

6.2.5 Private Key Archival
The CA signing key pair and verification public key certificates are backed up in the POS DIGICERT CA database. The POS DIGICERT database is archived according to the procedures described in **CPS Part** 5.4.6.

6.2.6 Private Key Transfer into or from a Cryptographic Module
As stipulated in **CPS Part** 6.1.1

6.2.7 Private Key Storage on Cryptographic Module
As stipulated in **CPS Part** 6.1.1

6.2.8 Method of Activating Private Key
The CA signing private keys are generated by the hardware, within the cryptographic module. Private keys are stored encrypted in the cryptographic module. For both the software and hardware token cases, they are decrypted only when they are actually being used.

6.2.9 Method of Deactivating Private Key
The CA signing private keys remain active for the period that an authorised person logs into the POS DIGICERT CA system. The login period ends when the CA system is shut down.

6.2.10 Method of Destroying Private Key
All sensitive keys in the memory of the CA system are overwritten with zeros when they are no longer in used. Permanent destruction of private keys is achieved with secure delete operations.

6.2.11 Cryptographic Module Rating
As stipulated in **CPS Part** 6.2.1

6.3 Other Aspects of Key Pair Management
6.3.1 Public Key Archival
As stipulated in **CPS Part** 6.2.5

6.3.2 Certificate Operational Periods and Key Pair Usage Periods
The validity period of the CA key pairs is 5 years unless agreed by the subscriber of Sub CA and POS DIGICERT. For Root CA, the validity is 20 years.

6.4 Activation Data
6.4.1 Activation Data Generation and Installation
All passwords are unique and unpredictable and offer a security level appropriate to that of the protected Key Pair.

6.4.2 Activation Data Protection
POS DIGICERT enforces a combination of cryptographic and physical access control mechanisms to protect password that used for Key Pair activation from unauthorised use.

6.4.3 Other Aspects of Activation Data
POS DIGICERT activation data may only be held by POS DIGICERT personnel in trusted roles.

6.5 Computer Security Controls
6.5.1 Specific Computer Security Technical Requirements
The CA workstation is physically secured as described in **CPS Part** 5.1. Access to the certificate database and audit trails is restricted as described in **CPS Part** 5.5.4 and 5.5.7. All computers installed with the CA software are configured to perform CA operations only. All irrelevant services of the operating system are disabled. The operating system enforces identification and authentication of all users.

6.5.2 Computer Security Rating
All computers that host the CA software comply with C2 level security requirements.

6.6 Life Cycle Technical Controls
All software components of the PKI developed by POS DIGICERT are developed in conditions and following a process that ensure their security. POS DIGICERT ensures, during software updates, the origin and integrity of the software. POS DIGICERT ensures that all software updates are done in a secure way. Updates are performed by personnel in a Trusted Role. POS DIGICERT separate the development and testing infrastructures from the production infrastructure of the PKI.

6.6.1 System Development Controls
Applications are developed and implemented in line with POS DIGICERT systems development and change management standards. POS DIGICERT provides client software to its Managed PKI for performing RA and certain CA functions. Such software is developed in accordance with POS DIGICERT system development standards.

6.6.2 Security Management Controls
POS DIGICERT has mechanisms and / or policies in place to control and monitor the configuration of its CA systems. Upon installation and periodically thereafter, POS DIGICERT validates the integrity of its CA systems.

6.6.3 Life Cycle Security Controls
As stipulated in **CPS Part** 6.6.1 and 6.6.2

6.7 Network Security Controls
POS DIGICERT performs all its CA and RA functions using secured networks in compliance with Audit Requirements Guide to prevent unauthorised access and malicious activity. POS DIGICERT protects its communications of sensitive information through the use of encryption and digital signatures.

6.8 Time-Stamping
Please refer to POS DIGICERT's TSA Practice Statement which is available for download at www.posdigicert.com.my/repository.

7.0 Certificate, CRL, and OCSP Profiles
7.1 Certificate Profile
This section describes the profile of certificates issued by POS DIGICERT. Some of the important elements of this profile will be highlighted. This enables users of this CPS to understand the structure of a certificate and identify possible applications to take advantage of this structure.

Certificate format version	Version 3
Certificate serial number	Unique value as per Issued Certificate
Digital signature algorithm identifier for CA	SHA-256 and above or ECC-384 and above
CA distinguished name	c=UG, o=GOU
Validity period	As per business contract terms requires but not exceeding three years as sanctioned by ESA 2011 Section 74. Most common validity period applies is either 1 year or 2 years or 3 years. e.g. 2 years' validity: start = 01/01/2021 end = 01/01/2023
Subject distinguished name	c=UG, o=GOU, CN = e.g. Michael
Subject unique identifier	NIN Number; or Passport Number; or Domain Name or; Any Other Acceptable Unique Identifier.
CA signature	SHA-256 and above or ECC-384 and above

Figure 3: X.509 v3 Certificate format

7.1.1 Version Number(s)
POS DIGICERT issues certificates in compliance with X.509 version 3.

7.1.2 Certificate Extensions
POS DIGICERT issues certificates that comply with the IETF RFC 5280 X.509 certificate format (see Figure 3). This standard provides POS DIGICERT with management and administrative controls to ensure that the application of the certificates is consistent with its policies. Such control can be achieved by defining the policies in the certificate extensions. A standard Object Identifier indicates the function of each extension. Each IETF RFC 5280 extension comprises two fields:

- Criticality; and
- Value.

The 'Criticality' field is a single-bit toggle flag. When set to true, this indicates that the corresponding 'Value' field contains data that cannot be ignored by an application. For humans, this translates into understanding the data within the 'Value' field and having the knowledge of handling these data. For example, it could contain a disclaimer on the use of the certificate or a URL that points to a location where this information is available. When set to false, it indicates that the data within the 'Value' field can be ignored.

7.1.3 Algorithm Object Identifiers (OID)
POS DIGICERT issues certificates with algorithms indicated by the following OIDs:

Pos Digicert OID : 1.3.6.1.4.1.50501
Pos Digicert CPS/CP OID : 1.3.6.1.4.1.50501.1
Pos Digicert DTS OID : 1.3.6.1.4.1.50501.3
Pos Digicert Adobe Signing OID : 1.3.6.1.4.1.50501.5

7.1.4 Name Forms
The Distinguished Name ('DN') and subject DN fields contain the full X.500 DN of the certificate issuer or certificate subject.

7.1.5 Name Constraints
Each distinguished name (DN) of POS DIGICERT CertificateSubject includes 'O = Pos Digicert Sdn. Bhd.

7.1.6 Certificate Policy Object Identifier
As stipulated in **CPS Part** 7.1.3.

7.1.7 Usage of Policy Constraints Extension
No Stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics
POS DIGICERT may state in brief statements in the Policy Qualifier field of the Certificate Policy extension.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension
The only certificate extension, which shall be identified as critical in certificates issued by this CA, is the CRLDistributionPoints extension. The CRL or ARL will be retrieved from the CRL distribution point directory entry indicated in the certificate.

7.2 CRL Profile
The following field CRL format is used in this PKI:

- version: set to v2;
- signature: identifier of the algorithm used to sign the CRL;
- issuer: Distinguished Name of the CA issuing the CRL;
- this update: time of CRL issue;
- next update: time of next expected CRL update; and
- revoked certificates: list of revoked certificate information.

7.2.1 Version Number (s)
CRLs issued by POS DIGICERT are X.509 version 2 CRL.

7.2.2 CRL and CRL Entry Extensions
A number of X.509 version 2 CRL and CRL entry extensions are used in this PKI. The following CRL and CRL entry extensions are used in this PKI:

X.509 v2 CRL Extension	Criticality	Optional	Notes
AuthorityKeyIdentifier	No	No	only element [0] (AuthorityKeyIdentifier) is filled in contains a 20 byte hash of the subjectPublicKeyInfo in the CA certificate
CRLNumber	No	No	Incremented each time a particular CRL is changed
ReasonCode	No	No	CRL entry extension – only reason codes [0], [1], [3], [4] and [5] supported [6],[2]
IssuingDistributionPoint	No	No	Element [0] (distributionPoint) includes the full DN of the distribution point Element[1] (onlyContainsUserCerts) is included for CRLs Element [2] (onlyContainsCACerts**)** is included for s Element [1] and [2] are never present together in the same revocation list Elements [3] and [4] are not used.

Unsupported Extensions
The following X.509 version 2 CRL extensions are not used in this PKI:

- issuer alternative name;
- invalidity date;

- certificate issuer; and
- delta CRL indicator.

7.3 OCSP Profile
If required, POS DIGICERT shall operate OCSP responder in accordance with RFC6960 (X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP) and highlights this within the AIA extension via an OCSP responder URL. POS DIGICERT's OCSP average response time for checking the revocation status of a certificates shall be within 10 seconds.

7.3.1 Version Number(s)
POS DIGICERT CA shall support OCSP version 1, request and responses.

7.3.2 OCSP Extension
The OCSP Responder certificate shall comply with RFC 5280 (Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile).

8.0 Compliance Audit and Other Assessments
8.1 Frequency and Circumstances of Assessment
A comprehensive compliance audit on POS DIGICERT CA operations is performed annually as required by Section 38 of the ESA and the WebTrust for CA guidelines.

8.2 Identity/Qualifications of Assessor
Annual performance audit will be performed by qualified auditors registered with the Office of the Controller. Please refer to www.nita.go.ug for further details.

8.3 Assessor's Relationship to Assessed Entity
Regardless of the purpose of the audit, the auditor and the audited party (POS DIGICERT) shall not have any kind of relationship that could derive in a conflict of interests. In the case of internal auditors, these may not have any operational relationship with the area being audited.

8.4 Topics Covered by Assessment
The annual compliance audit investigates the operations of POS DIGICERT CA and its RA functions to ensure their compliance with the ESA and the ESR. Each audit will include, but is not limited to, compliance with Pos Digicert CPS and the WebTrust standards for Certification Authorities version 2.2.

8.5 Actions Taken as a Result of Deficiency
Based on the information gathered in the audit, the qualified auditor shall categorise POS DIGICERT's compliance as one of the following:

a) full compliance, if POS DIGICERT appears to comply with all the requirements of the ESA, ESR and the WebTrust standards for Certification Authorities version 2.2;

b) non-compliance, if POS DIGICERT:

   i. complies with a few or none of the requirements of the ESA, ESR and the WebTrust standards for Certification Authorities version 2.2;
   ii. fails to keep adequate records to demonstrate compliance with more than a few requirements; or
   iii. refuses to submit to an audit.

There are three possible actions to be taken as a result of identification of a deficiency:
- continue to operate as usual;
- continue to operate but at a lower assurance level; and
- cease operation

8.6 Communications of Results
The qualified auditor shall, within fourteen (14) days from the completion of a compliance audit under Regulation 42, submit a written report to the Controller. All information, which is not considered by POS

DIGICERT to be public domain information, is to be kept confidential. Some specifics are addressed in **CPS Part** 2.8.

8.7 Self Audit / Assessment
POS DIGICERT also conducts its own self-assessment on a yearly basis using the latest WebTrust standards as the guiding standards to evaluate and ensure its CA risk management, governance and internal control processes are operating effectively.

9.0 Other Business and Legal Matters
9.1 Fees
9.1.1 Certificate Issuance or Renewal Fees
Certificate fees can be obtained from NITA-U.
9.1.2 Certificate Access Fees
POS DIGICERT does not levy any fee for accessing certificates through POS DIGICERT web site.

9.1.3 Revocation or Status Information Access Fees
POS DIGICERT does not levy any fees for accessing the revocation list of certificates.

9.1.4 Fees for Other Services
POS DIGICERT may charge for other additional services such as digital signing solutioning & timestamping.

9.1.5 Refund Policy
Application fee is non-refundable.

9.2 Financial Responsibility
9.2.1 Insurance Coverage
POS DIGICERT shall only be liable for the issued certificates to an amount not exceeding the amount stated as per the Reliance Limit in CPS Part 9.8.1.

9.2.2 Other Assets
No Stipulation

9.2.3 Insurance or Warranty Coverage for End-Entities
The warranty period for Certificate and its holding medium is one (1) month. The warranty period commences from the date that the Certificate and its holding medium is first emailed / dispatched from POS DIGICERT.

9.3 Confidentiality of Business Information
9.3.1 Scope of Confidential Information
The private signing key belonging to POS DIGICERT's subscriber is confidential to that subscriber. Information held in audit trails is considered confidential to POS DIGICERT and shall not be released outside of POS DIGICERT, unless required by law (see in **CPS Part** 9.4.6). Personal and corporate information held by the POS DIGICERT, other than that which is explicitly published as part of a certificate, CRL, ARL and CPS is considered confidential and shall not be released unless required by law (see in **CPS Part** 9.4.6). Generally, the results of annual audits are kept confidential, with exceptions as outlined in **CPS Part** 8.0.

9.3.2 Information not within the Scope of Confidential Information
Information included in certificates, CRLs and issued by POS DIGICERT and POS DIGICERT's certificate policies are not considered confidential. Information in this CPS itself is not considered confidential. However, POS DIGICERT policy requires that it shall primarily be made available to subscribers of its certification services, including those in cross certified CA domains. Confidentiality of information in the POS DIGICERT repository is dependent on the particular data items and applications. Confidentiality of relevant information in the repository is achieved through the use of access controls.

9.3.3 Responsibility to Protect Confidential Information
POS DIGICERT is obliged under the ESA to disclose or release production of records and identification document, accounts, computerised data and other relevant documents to the enforcement officials. When POS DIGICERT revokes a certificate, its RAs or the Controller, the list of revocation can be found

in the CRL. A revocation reason is included in the CRL entry for the revoked certificate. This revocation reason code is not considered confidential and can be shared with all other users and relying parties. However, no other details concerning the revocation are disclosed. POS DIGICERT SHALL release information of the owner or subscriber if authorised by the subscriber.

9.4 Privacy of Personal Information
9.4.1 Privacy Plan
POS DIGICERT shall follow the Ugandan Data Protection & Privacy Act (2019) to handle the personal information of the subscriber or the CA itself. The policy can be obtained from NITA-U.

9.4.2 Information Treated as Private
As stipulated in **CPS Part** 9.3

9.4.3 Information Not Deemed Private
As stipulated in **CPS Part** 9.3

9.4.4 Responsibility to Protect Private Information
As stipulated in **CPS Part** 9.3

9.4.5 Notice and Consent to Use Private Information
As stipulated in **CPS Part** 9.3

9.4.6 Disclosure Pursuant to Judicial or Administrative Circumstances
POS DIGICERT may disclose private information if required by law or regulation without providing notice to the subscribers.

9.4.7 Other Information Disclosure Circumstances
POS DIGICERT independent third-party RAs under a CA, Resellers, and Co-marketers may disclose information provided to POS DIGICERT such RA, Reseller or Co-marketer, by an Applicant, a Subscriber, or a Relying Party upon request of such Applicant, Subscriber, or Relying Party.
If a Certificate is revoked by a CA, a serial number will be included in the Certificate Revocation List entry for the revoked Certificate.

9.5 Intellectual Property Rights
Subscribers, users of this CPS, and parties covered in **CPS Part** 1.3 are not to reverse engineer, decompile or attempt to reverse engineer or decompile the technologies including encryption algorithms employed by POS DIGICERT in providing the CA services to subscribers. Unless otherwise stated, the following property-ownership relationships are assumed to be in force:

- Public key - public keys are the personal property of the holders of the corresponding private key. Public keys may be distributed freely due to the nature of its usage;

- Private key - private keys are the personal property of the subscribers. Subscribers are individually responsible for the security of the private key;

- Certificates - certificates are the private property of POS DIGICERT. Certificates shall only be reproduced in a publicly accessible repository with the prior permission of POS DIGICERT. Should the certificate be reproduced in a non-publicly accessible repository, no part of the certificate must be omitted; and

- CPS - this CPS remains as the sole private property of POS DIGICERT. Reproduction of this CPS requires the prior permission of POS DIGICERT.

9.6 Representations and Warranties
9.6.1 CA Representations and Warranties
By issuing certificates POS DIGICERT makes certain representations to the subscriber and to the subsequent parties relying on the certificates. POS DIGICERT makes no representations or guarantees, which includes but is not limited to, the accuracy, integrity, reliability, completeness, fitness for a particular purpose or the authenticity of the information contained within the digital certificate. POS

DIGICERT shall not be liable to any person for any liabilities, damages or claims whatsoever in respect of any loss suffered, economic or otherwise, whether consequential, direct or indirect, resulting from the person's reliance on such information. POS DIGICERT makes no further representations and provides no further guarantees of any kind whatsoever to any person regarding the identity of the subscriber to whom POS DIGICERT has issued a certificate to the extent that such identity has been verified in the manner set out within this CPS. In addition, subscribers must maintain full responsibility to ensure that their private key is not compromised, stolen, modified or used in an unauthorised manner. The subscribers assume this responsibility upon transmission of the key from POS DIGICERT (if the subscriber did not generate the key). In this respect, POS DIGICERT will not guarantee that the receiving party is the subscriber in person. POS DIGICERT will only guarantee that the private key was transmitted to an address, whether electronic or otherwise, or to a natural person, designated by the subscriber as being the address or the natural person through which he will receive the private key. POS DIGICERT will not be liable in any way for damages suffered, whether directly or indirectly, as a result of a person's reliance that the private key was transmitted to the actual intended party. The subscribers may delegate to another person the responsibilities to prevent compromise, theft, modification, or unauthorised use of the private key. However, this does not negate the delegator of his responsibilities as outlined in the above paragraphs. By accepting a certificate issued by POS DIGICERT, the subscriber acknowledges and represents the following to POS DIGICERT and to persons relying on the information contained within the certificate throughout the validity period of the certificate (until such time that the certificate is revoked, suspended or expired):

a) all information contained in the certificate is true to the best of the subscriber's knowledge to the extent that any changes to the information is not made known to POS DIGICERT or has been made known to POS DIGICERT but has not been amended by POS DIGICERT due to an unreasonable time frame or reasons beyond the control of POS DIGICERT;

b) the subscriber promises to notify POS DIGICERT as soon as practicable of changes to the information contained in the certificate;

c) the private key of the subscriber has not been compromised, stolen, modified, or used in an unauthorised manner and the subscriber has taken necessary steps to prevent these from happening;

d) the private key of the subscriber is not to be used in any manner other than its intended use as described in **CPS Part** 4.5;

e) digital signatures created by the subscriber are used for legal purposes (within the context of applicable local laws) and subject to the terms and conditions within this CPS; and

f) digital signatures created by the subscriber are signed with the private key that corresponds to the public key listed in the certificate.

9.6.2 RA Representations and Warranties

POS DIGICERT may outsource the function to several appointed RAs. Prior to appointment of RAs, the RAs need to sign up contract with POS DIGICERT to ensure that they are compliance to the procedures. The primary roles of RAs are as follows:

- certificate issuance;
- certificate renewal;
- certificate revocation;
- verification of applicants; and
- other functions that related to certification services that commissioned by POS DIGICERT.

RA also must observe the rules in this CPS and carry out registration functions as mandated. RA must accept only those applications with verified and accurate information. RA shall issue receipt slips to applicant. RA should clearly state the reasons if the application is rejected.

9.6.3 Subscriber Representations and Warranties

As Stipulated in **CPS Part** 4.5

9.6.4 Relying Party Representations and Warranties
As Stipulated in **CPS Part** 4.5

9.6.5 Representations and Warranties of Other Participants
POS DIGICERT's repository function is obliged to publish all the valid certificates and CRL as scheduled.

9.7 Disclaimers of Warranties
As stipulated in **CPS Part** 9.6.

9.8 Limitations of Liability
9.8.1 CA Liability
Additional terms, conditions or other representations whether oral or in written form by POS DIGICERT or its employees, agents or persons claiming to be its employees or agents will not increase the scope POS DIGICERT's liability contained within this CPS except where POS DIGICERT expressly provides for it. POS DIGICERT shall only be liable for the issued certificates to an amount not exceeding the following:

Class of certificate	**Reliance limit/ Liability Cap**
Class 2	USD25,000.00 (Enhanced) Up to USD25,000 (Sub CA)

The reliance limit on each certificate shall be the same regardless of the number of digital signatures, transactions, or claims related to such certificate. In the event the liability cap is exceeded, the available liability cap shall be apportioned first to the earliest claims to achieve final dispute resolution, unless otherwise ordered by a court of competent jurisdiction. In no event shall POS DIGICERT be obligated to pay more than the aggregate liability cap for each certificate, regardless of the method of apportionment among claimants to the amount of liability cap. POS DIGICERT will not be liable to any party whosoever for any damages suffered whether directly or indirectly as a result of terminating its services. Subscribers are liable for any form of misrepresentation of information contained in the certificate to relying parties even though the information has been verified by POS DIGICERT. Verification does not provide a one hundred percent guarantee of accuracy. This is due to the reason that facts may change over time or could have been fraudulently created and only through a detailed investigation (which shall be beyond the scope of the CA / RA due to time and cost constraints) shall the deception be detected. In line with section 76 (a) ESA 2011, POS DIGICERT shall not be liable for any loss caused by reliance on a false or forged digital signature of a subscriber, if, with respect to the false or forged digital signature, POS DIGICERT has complied with the requirements of this Act.

9.8.2 RA Liability
RAs shall subject to the same liabilities as applicable to POS DIGICERT, as listed in CPS Part 9.8.1 should there be any violation of provision in the CPS that may cause damage to the subscribers.

9.9 Indemnities
POS DIGICERT assumes no financial responsibility for improperly used certificates, CRLs, etc.

9.10 Term and Termination
9.10.1 Term
This CPS remains effective on POS DIGICERT website online repository until replaced with a new version.

9.10.2 Termination
This CPS remains effective on POS DIGICERT website online repository until get the notification changes and amendments which produce with a new version.

9.10.3 Effect of Termination and Survival
POS DIGICERT will communicate the effect of the termination of its CPS via POS DIGICERT Repository.

9.11 Individual Notices and Communications with Participants

Severance or merger may result in changes to the scope, management and/or operations of POS DIGICERT. In such an event, this CPS shall require modifications as well. Changes to the operations will occur consistent with the administrative requirements stipulated in **CPS Part** 9.12. In either event, the DNs of all POS DIGICERT's subscribers within the current scope of POS DIGICERT's PKI will likely to be changed too, resulting in the need to update keys for those subscribers.

9.12 Amendments

9.12.1 Procedure for Amendment

POS DIGICERT reserves the right to amend this CPS at any time (prospectively and not retroactively). Amendments to the CPS will be made available either as an amended version of the CPS or retrospectively can be posted in the Notices section of POS DIGICERT's web site at the following URL www.posdigicert.com.my under the Repository Section. These amendments shall supersede any conflicting provisions of the referenced version of the CPS.

This CPS can be obtained:

- in an electronic form via POS DIGICERT's website www.posdigicert.com.my under the Repository Section.
- the electronic copy of this CPS is currently available in PDF format only.

To maintain integrity of this document, the web-based version of the CPS must be viewed using SSL-enabled browsers, e.g. Mozilla Firefox version 3.0 and above, or Microsoft Internet Explorer 7 and above.

9.12.2 Notification Mechanism and Period

From time to time POS DIGICERT may make changes to its practices in order to improve its services. Some of these changes may require an amendment to the CPS. These updates will be posted at POS DIGICERT's web site at URL www.posdigicert.com.my under the Repository Section. The amendments will become enforceable automatically within fourteen (14) working days of this CPS being made available at the POS DIGICERT's web site unless POS DIGICERT explicitly states otherwise or issues a notice of withdrawal prior to the end of the fourteen (14) day period.

9.12.3 Circumstances Under Which OID must be changed

Should POS DIGICERT deem that the amendments to the specifications could affect the acceptability of the certificates for specific purposes, the amendments will be notified to the users of the certificates by updating the CPS.

9.13 Dispute Resolution Provisions

Within the POS DIGICERT domain, disputes between subscribers, one of which acts in the role of a subscriber and the other which acts in the role of a relying party, or between subscribers and POS DIGICERT, will initially be reported to POS DIGICERT for dispute resolution.

9.14 Governing Law

This CPS complies with the Ugandan Law, namely, the ESA and the ESR.

9.15 Compliance with Applicable Law

POS DIGICERT is responsible for ensuring compliance with the applicable legislation stated under **CPS Part** 9.14.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Every RA involved in Certificate issuance shall obligate to comply with this CPS and applicable industry Guidelines. POS DIGICERT will also require its Subscriber and Relying Parties to accept agreements.

9.16.2 Assignment

Entities operating under this CPS must not assign their rights or obligations without the prior written consent of POS DIGICERT.

9.16.3 Severability
If any provision of this CPS is found invalid or unenforceable by a competent court or tribunal, amendment will be made and agreed in such manner as to correspond to the original intention of the parties.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)
As stipulated in **CPS Part** 9.13

9.16.5 Force Majeure
POS DIGICERT shall not be liable for any losses, costs, expenses, liabilities, damages, or claims arising out of or related to delays in performance or from failure to perform its obligations if such failure or delay is due to circumstances beyond POS DIGICERT's reasonable control, including without limitation, acts of any governmental body, war, insurrection, sabotage, embargo, fire, flood, strike or other, interruption of or delay in transportation, unavailability of interruption or delay in telecommunications or third party services.

9.17 Other Provisions
9.17.1 Fiduciary Relationships
Nothing contained in this CPS, or in any Subscription Agreement shall be deemed to constitute POS DIGICERT as the fiduciary, partner, agent, trustee, or legal representative of any Applicant, Subscriber, Relying Party or any other person, entity, or organization or to create any fiduciary relationship between the POS DIGICERT and any Subscriber, Applicant, Relying Party or any other person, entity, or organization, for any purpose whatsoever. Nothing in the CPS, or in any Subscription Agreement shall confer on any Subscriber, Applicant, Relying Party, or any other third party, any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf of the POS DIGICERT.

(end of document)