Purpose: This **Certificate Policy ("CP")** applies to the products and services of **Impression Signatures (Pty) Ltd ("Impression")**. Primarily this pertains to the issuance and lifecycle management of Certificates including validity checking services. This CP may be updated from time to time as outlined in Section 1.5 *Policy Administration*. The latest version may be found on the Impression Repository at https://www.impression-signatures.com/pages/legal.

This CP addresses areas of policy and practice such as, but not limited to, technical requirements, security procedures, personnel and training needs, which are required to meet industry best practices for Certificate lifecycle management as issued by the **Certificate Authority ("CA")**. This CP addresses the additional procedures that are not contained in the CA's CP or **("Master CP")** and discloses, where applicable, the relevant sections of the CA's CP that Impression is contracted to follow.

This CP is final and binding between Impression Signatures (Pty) Ltd, a company with registered office at 1st Floor, Howick Close Building, Waterfall Office Park, Midrand, South Africa, 1686 and registration number 2015/285088/07, (hereinafter referred to as **"Impression"**), and the Subscriber and/or Relying Party, who uses, relies upon or attempts to rely upon certification services made available by the Registration and Certification Authorities referring to this CP.

For Subscribers, this CP becomes effective and binding by accepting a Subscriber Agreement. For Relying Parties, this CP becomes binding by relying upon a Certificate issued under this CP. In addition, Subscribers are required by the Subscriber Agreement to inform their Relying Parties that the CP is itself binding upon those Relying Parties.

Document History:

Version	Release Date	Author(s)	Status & Description
1.0	25/09/2019	Andrew Papastefanou	First Version

1. Introduction

1.1. Impression is a certified regional partner of **GMO GlobalSign Ltd ("GS")**, a WebTrust and eIDAS-certified **certificate authority ("GS CA")** who is part of an international network of **Trusted Third Parties ("TTP's")** following established procedures to issue digital certificates to public and private entities.

1.2. **Registration Authorities ("RA")** and **Local Registration Authorities ("LRA")** are accredited to interact with both the subscriber and GS to deliver **Public Key Infrastructure ("PKI")** services to the end-user. RA/LRA organisations perform one or more of the following functions:

1.2.1. Accept, evaluate, approve or reject the registration of certificate applications.
1.2.2. Register subscribers for GS certification services.
1.2.3. Manage stages of the identification of subscribers as assigned by GS according to the type of certificate to be issued, including face-to-face identification or equivalent.
1.2.4. Use official, notarised or other required documentation to evaluate a subscriber application, in compliance with the requirements of the ECT Act.
1.2.5. Following approval of an application, notify GS to issue a certificate.
1.2.6. Initiate the process to revoke a certificate and request a certificate revocation from GS.

1.3. For the purposes of accreditation with the **South African Accreditation Authority ("SAAA")** for issuing **Advanced Electronic Signatures ("AES")** as defined by the **Electronic Communications and Transactions Act 25 of 2002 ("ECT Act")**, Impression has been designated as an RA/LRA of GS.

1.4. Impression acts locally within its own geographical context, complying with local laws and regulations whilst operating under the supervision of GS and within their framework of approved practices and procedures and in accordance with the **CA/Browser Forum Baseline Requirements (the "Baseline Requirements").**

1.5. The latest version of the Master CP may be found on the GS Repository at https://www.globalsign.com/repository. This CP will specifically reference the applicable sections of the latest version of the Master CP which is checked for relevance as new versions are made available.

1.6. **If at any time GS in its sole discretion determines that Impression is not appropriately performing any delegated functions described herein, GS may remove Impression as an RA/LRA.**

2. Overview

2.1. The ECT Act provides for the recognition of AES that are used for the purposes of authentication, signature and/or non-repudiation. Impression extends upon the Master CP to ensure compliance with the requirements of the ECT Act and accreditation regulations. The Certificate types defined in this CP are the following:

2.1.1. Timestamping: A Certificate to authenticate time sources.

2.1.2. **Adobe Approved Trust List ("AATL")**: A Certificate of medium hardware assurance for use with Adobe AATL and Microsoft Office documents.

2.1.3. Intermediate signing for AATL: An intermediate CA that enters the GS hierarchy.

2.1.4. Timestamping for Adobe **Certified Document Services ("CDS")**: A Certificate to authenticate time sources.

2.1.5. Test Digital Certificate for Adobe CDS: A Certificate for test or demonstration purposes which does not require hardware Assurance.

2.1.6. AES: SAAA accredited and ECT compliant certificates used for providing electronic signatures that extend AATL requirements.

3. Document Name & Identification

3.1. Refer to Master CP, section 1.2

4. PKI Participants

4.1. Refer to Master CP, section 1.3 and subsections

4.2. RA/LRA Specific Requirements for AES: GS/Impression will delegate the verification of the Individual Identity to an RA/LRA under the condition that this RA/LRA meet the verification requirements as set by ECT Act and accreditation regulations.

4.3. This condition is considered to be met in the following scenarios:

4.3.1. The RA/LRA passes an audit to confirm that the Subscriber information is properly authenticated, following the relevant "Verification" sections in Impression's CP and CPS for AES.

4.3.2. Impression shall monitor adherence to its CP and CPS by the delegated LRA by performing ongoing quarterly audits against a randomly selected sample of at least the greater of one (1) certificate or one percent (1%) of the AES verified by the delegated LRA in the period beginning immediately after the last sample was taken.

4.3.3. Most organizations will perform an in-person (or equivalent) identification of their employees, agents or contractors. These organizations may act as a LRAs for Impression with regards to the identity verification of their employees, contractors or agents. In this case, there will be an agreement between Impression and the organization, and Impression, along with their auditors, will perform a security assessment of employee identification procedures. Certificates issued using this specific LRA type contain the organization information in the Certificate.

5. Certificate Usage

5.1. Refer to Master CP, section 1.4 and subsections

6. Policy Administration

6.1. Organisation administering the policy: Requests for information on the compliance of RAs and Issuing CAs with accreditation schemes as well as any other inquiry associated with this CP should be addressed to:
AES Policy Committee – Impression Signatures (Pty) Ltd
1st Floor, Howick Close Building,

Waterfall Office Park
1686
Email: aes@impression.cloud
Tel: +27 (0) 87 405 6220

6.2. Certificate Problem Report: Subscribers, Relying Parties, Application Software Suppliers, and other third parties may report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates by sending email to aes@impression.cloud. Impression may or may not revoke in response to this request.

6.3. Person/s Determining CP Suitability for the Policy: The **AES Policy Committee ("APC")** determines the suitability and applicability of the CP and the conformance of a CPS to this CP based on the results and recommendations received from a Qualified WebTrust Auditor.

6.3.1. In an effort to maintain credibility and promote trust in this CP and better correspond to accreditation and legal requirements, the APC shall review this CP at least annually and may make revisions and updates to policies as it sees fit or as required by other circumstances.

6.3.2. Any updates become binding for all Certificates that have been issued or are to be issued upon the date of the publication of the updated version of this CP.

6.3.3. The SAAA will be notified in writing at least 30 days before any substantive changes become effective.

6.4. CP Approval Procedures: The APC reviews and approves any changes to the CP. The updated CP is reviewed against the CPS in order to check for consistency. CP changes are also added on an as-needed basis.

6.4.1. Upon approval of a CP update by the APC, the SAAA are notified in writing of any substantive changes. Thirty (30) days later, the new CP is published in the Impression Repository at https://www.impression-signatures.com/pages/legal.

6.4.2. The updated version is binding upon all Subscribers including the Subscribers and parties relying on Certificates that have been issued under a previous version of the CP.

7. Definitions

7.1. In addition to the definitions contained herein, refer to Master CP, section 1.6

8. Publication & Repository Responsibilities

8.1. Refer to Master CP, section 2.0 and subsections

9. Identification & Authentication

9.1. Naming: Refer to Master CP, section 3.1 and subsections

9.2. Initial Identity Verification: Impression may perform identification of the using any legal means of communication or investigation necessary to identify the individual.

9.3. Method to Prove Possession of a Private Key: Refer to Master CP, section 3.2.1

9.4. Private Key Protection: Impression will generate and store subscriber private keys on a **Federal Information Processing Standards ("FIPS")** Publication 140-2 Level 3 compliant **Hardware Security Module ("HSM")** which complies with the following requirements:

9.4.1. Certificate applicants have their identity verified and consent before their private key is generated, demonstrated through an auditable process.

9.4.2. Applicants accept and sign a subscriber agreement before their certificate is generated from a corresponding signing request generated from their private key.

9.4.3. A subscriber's key can never be directly accessed, only activated indirectly to sign data through a minimum two-factor authentication mechanism under the sole control of the subscriber, selecting from two of the following **National Institute of Standards and Technology ("NIST")** recognised factors:

9.4.3.1. Something a person has – possession of a device under the sole control of the subscriber. Examples are a **One-Time-Pin ("OTP"), Unstructured Supplementary Service Data ("USSD")** sent to a mobile phone, smartcards, hardware or software based

cryptographic tokens or a mobile communication device managed by a **Mobile Device Management ("MDM")** solution.

9.4.3.2. Something a person is – fingerprint, iris, facial recognition or equivalent biometric evidence.

9.4.3.3. Something a person knows – knowledge of information known only to the subscriber such as a pin or password.

9.4.4. Impression can never access the subscriber's private key nor activate it without their sole express permission and consent.

9.4.5. Subscriber organisations and LRAs can elect to use Impression's HSM directly or provide their own HSM as long as the minimum private key protection requirements are met.

9.4.6. Impression has no access to the private key storage on the HSM and signing occurs using aliases

9.5. Authentication of Organization Identity: Refer to Master CP, section 3.2.2 and subsections

9.6. Authentication of Individual Identity: Refer to Master CP, section 3.2.3 and subsections

9.6.1. AES Certificates: Upon the verification and approval of an organizational profile and assignment of certificate content by GS, Impression shall serve as RA/LRA for the subscriber content. Impression will be entitled to accept subscriber applications for the issuance of AES certificates. Impression authenticates the Identity of Individual Subscribers according to the following methods:

9.6.1.1. In-person identity verification: The following information will be gathered and verified during an application by a natural person:

9.6.1.1.1. An electronic copy of the applicant's passport, **South African ("SA") identity ("ID")** card or SA barcoded green ID book. The identity of the subscriber will be verified in a face-to-face interview with the enrolment officer by comparison with the photo identification. The original identity document will also be checked for validity and that it is not counterfeit.

9.6.1.1.2. A completed electronic application form containing the subscriber's detail's to be verified.

9.6.1.1.3. A completed subscriber agreement signed with a handwritten signature in the presence of the authorized enrolment officer.

9.6.1.1.4. The following information will be gathered during a certificate renewal application by a natural person:

9.6.1.1.4.1. An active and valid AES certificate.

9.6.1.1.4.2. An updated and verified subscriber agreement signed with 9.6.1.1.3

9.6.1.2. Video identity verification: The following information will be gathered and verified during an application by a natural person:

9.6.1.2.1. An electronic copy of the applicant's passport, SA ID card or SA barcoded green ID book. The identity of the subscriber will be verified in a face-to-face interview with the enrolment officer by comparison with the photo identification. The original identity document will also be checked for validity and that it is not counterfeit through an automated comparison process with services made available through the **Home Affairs National Identification System ("HANIS")** that will also return the photo identification of the applicant.

9.6.1.2.2. A completed electronic application form containing the Subscriber's detail's to be verified.

9.6.1.2.3. A completed subscriber agreement signed with a handwritten signature in the presence of the authorized enrolment officer.

9.6.1.2.4. This method requires that the Subscriber has access to an internet-enabled device, a working webcam or other video-equipment and a working microphone and sound-system. Liveness and presence of the natural person is detected through a series of unique challenges completed by the user on video.

9.6.1.2.5. The physical presence of the natural person can be augmented by adding the NIST categories of authentication factors. Impression accepts the following authentication factors as proof of physical presence:

9.6.1.2.5.1. At least one inherent factor (Something the person is); OR

9.6.1.2.5.2. Multifactor with at least one factor in each of the following categories:

9.6.1.2.5.2.1. Possession-based (Something the person has).

9.6.1.2.5.2.2. Knowledge-based (Something the person knows).
9.6.1.2.6. The following information will be gathered during a certificate renewal application by a natural person:
9.6.1.2.6.1. An active and valid AES certificate.
9.6.1.2.6.2. An updated and verified subscriber agreement signed with 9.6.1.1.3

9.7. Non-Verified Subscriber Information: Refer to Master CP, section 3.2.4

9.8. Validation of Authority: Refer to Master CP, section 3.2.5
9.8.1. AES Certificates: Verification of the authenticity of the individual Applicant's request with the methods listed in section 9.6.1

9.9. Criteria for Interoperations: Refer to Master CP, section 3.2.6

9.10. Authentication of Domain Names: refer to Master CP, section 3.2.7 and subsections

9.11. Authentication of Email Addresses: refer to Master CP, section 3.2.8

10. Identification & Authentication for Re-Key Requests

10.1. Refer to Master CP, section 3.3 and subsections
10.1.1. AES Certificate Rekey: Impression doesn't allow for AES re-key and will require a revocation and new Certificate issuance.

11. Identification & Authentication for Revocation Requests

11.1. Refer to Master CP, section 3.4

12. Certificate Lifecycle Operational Requirements

12.1. Certificate Application: Refer to Master CP, section 4.1 and subsections

12.2. Certificate Application Processing: Refer to Master CP, section 4.2 and subsections

12.3. Certificate Issuance: Refer to Master CP, section 4.3 and subsections

12.4. Certificate Acceptance: Refer to Master CP, section 4.4 and subsections

12.5. Keypair and Certificate Usage: Refer to Master CP, section 4.5 and subsections

12.6. Certificate Renewal: refer to Master CP, section 4.6 and subsections
12.6.1. AES Certificate Renewal: Impression doesn't allow for AES renewal and will require a new Certificate issuance.

12.7. Certificate Re-Key: refer to Master CP, section 4.7 and subsections
12.7.1. AES Certificate Rekey: Impression doesn't allow for AES re-key and will require a revocation and new Certificate issuance.

12.8. Certificate Modification: refer to Master CP, section 4.8 and subsections

12.9. Certificate Revocation and Suspension: refer to Master CP, section 4.9 and subsections
12.9.1. Suspension: Impression does not support certificate or private key suspension for AES certificates

12.10. Certificate Status Services: refer to Master CP, section 4.10 and subsections

12.11. End of Subscription: refer to Master CP, section 4.11

12.12. Key Escrow and Recovery: refer to Master CP, section 4.12 and subsections

13. Facility, Management &

13.1. Impressions Certificate Management Process MUST include:
13.1.1. Physical security and environmental controls;

Operational Controls

13.1.2. System integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
13.1.3. Network security and firewall management, including port restrictions and IP address filtering;
13.1.4. User management, separate trusted-role assignments, education, awareness, and training; and
13.1.5. Logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

13.2. Impression's security program includes an annual Risk Assessment that:
13.2.1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
13.2.2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
13.2.3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that Impression has in place to counter such threats.

13.3. Based on the Risk Assessment, Impression develops, implements, and maintains a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

13.4. The security plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan also takes into account available technology and the cost of implementing the specific measures and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

13.5. Physical Controls: Refer to Master CP, section 5.1 and subsections
13.5.1. Impression's infrastructure supplier maintains physical and environmental security policies for systems used for Certificate issuance and management which cover physical access control, natural disaster protection, fire safety factors, failure of supporting utilities (e.g. power, telecommunications), structure collapse, plumbing leaks, protection against theft, breaking & entering, and disaster recovery. Controls are implemented to avoid loss, damage or compromise of assets and interruption to business activities and theft of information and information processing facilities.

13.6. Procedural Controls: Impression ensures that all operators and administrators including Vetting Agents are acting in the capacity of a trusted role. Trusted roles are such that no conflict of interest is possible, and the roles are distributed such that no single person can circumvent the security of the RA system.
13.6.1. Impression may subscribe Certificates for Impression affiliate companies, or persons identified in association with these companies (as a Subject). Impression affiliate companies include Impression's parent and subsidiary companies, as well and other companies that share a same parent company as Impression.
13.6.2. Trusted roles include but are not limited to the following:
13.6.2.1. Developer: Responsible for development of RA systems.
13.6.2.2. Security Officer/Head of Information Security: Overall responsibility for administering the implementation of the RA's security practices;
13.6.2.3. Vetting Agents: Responsible for validating the authenticity and integrity of data to be included within Certificates via a suitable RA system and approve the generation/revocation/suspension of Certificates;
13.6.2.4. Infra System Engineer: Authorized to install, configure and maintain the RA systems used for Certificate lifecycle management;
13.6.2.5. Infra Operator: Responsible for operating the RA systems on a day to day basis. Authorized to perform system backup / recovery, viewing / maintenance of RA system archives and audit logs;

13.6.2.6. Auditor: Authorized to view archives and audit logs of the RA Trustworthy Systems;
13.6.3. Number of Persons Required per Task: Refer to Master CP, section 5.2.2
13.6.4. Identification and Authentication for Each Role: Before appointing a person to a trusted role, Impression performs a background check. Each role described above is identified and authenticated in a manner to guarantee that the right person has the right role to support the RA.
13.6.5. Roles Requiring Separation of Duties: Impression enforces role separation procedurally. Individual RA personnel are specifically assigned to the roles defined in Section 13.6.2 above. Roles requiring a separation of duties include:
13.6.5.1. Those performing approval of the generation, revocation and suspension of certificates;
13.6.5.2. Those performing installation, configuration and maintenance of the RA systems;
13.6.5.3. Those performing duties related to cryptographic key life cycle management (e.g., key component custodians);
13.6.6. Those performing RA systems development.

13.7. Personnel Controls:
13.7.1. Qualifications, Experience, and Clearance Requirements:
13.7.1.1. Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor, Impression verifies the identity and trustworthiness of such person.
13.7.1.2. Impression employs a sufficient number of personnel that possess the expert knowledge, experience and qualifications necessary for the offered services, as appropriate to the job function.
13.7.1.3. Impression staff who have been delegated the RA/LRA functions shall meet the following minimum criteria:
13.7.1.3.1. a minimum of two (2) years studies leading directly to a university degree and/or two (2) years' experience in digital certification or equivalent;
13.7.1.3.2. have not been convicted of a serious crime;
13.7.1.3.3. will undergo a criminal and credit worthiness background check.
13.7.1.3.4. have been provided with training material to identify the validity of photo identity documents and detect counterfeits
13.7.2. Background Check Procedures:
13.7.2.1. All Impression personnel in trusted roles are free from conflict of interests that might prejudice the impartiality of the RA operations. Impression does not appoint to a trusted role any person who is known to have a conviction for a serious crime or another offence if such conviction affects his/her suitability for the position. Personnel do not have access to the trusted functions until any necessary checks are completed and results analyzed, provided such checks are permitted by the jurisdiction in which the person will be employed. All persons filling trusted roles shall be selected on the basis of loyalty, trustworthiness, and integrity, and shall be subject to background investigation where permitted by law.
13.7.2.2. Any use of information revealed by background checks by Impression shall be in compliance with applicable laws of the jurisdiction where the person is employed.
13.7.3. Training Requirements:
13.7.3.1. Impression provides all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the RA's Certificate Policy and/or Certification Practice Statement) and the common threats to the information verification process (including phishing and other social engineering tactics).
13.7.3.2. Impression maintains records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.
13.7.4. Retraining Frequency and Requirements:
13.7.4.1. All personnel in Trusted Roles maintain skill levels consistent with Impression's training and performance programs.
13.7.4.2. Individuals responsible for trusted roles are aware of changes in the RA operations, as applicable. Any significant change to the operations has a training (awareness) plan, and the execution of such plan is documented.

13.7.4.3. Impression provides information security and privacy training at least once a year to all employees
13.7.5. Job Rotation Frequency and Sequence:
13.7.5.1. Impression ensures that any change in the staff will not affect the operational effectiveness of the service or the security of the system.
13.7.6. Sanctions for Unauthorized Actions:
13.7.6.1. Appropriate disciplinary sanctions are applied to personnel violating provisions and policies within this CP, the CPS or RA related operational procedures.
13.7.6.2. The disciplinary code is distributed to Impression staff annually
13.7.7. Independent Contractor Requirements:
13.7.7.1. Contractor personnel employed for Impression operations are subject to the same process, procedures, assessment, security control and training as permanent RA personnel.
13.7.8. Documentation Supplied to Personnel:
13.7.8.1. Impression makes available to its personnel this CP, any corresponding CPS and any relevant statutes, policies or contracts. Other technical, operational and administrative documents (e.g., administrator manuals, user manuals, etc.) are provided in order for the trusted personnel to perform their duties.
13.7.8.2. Documentation is maintained identifying all personnel who received training and the level of training completed.

13.8. Audit Logging Procedures: refer to Master CP, section 5.4 and subsections

13.9. Records Archival: refer to Master CP, section 5.5 and subsections
13.9.1. Impression shall retain all documentation relating to certificate requests and the verification thereof, and all certificates and revocation thereof, for at least seven (7) years after any certificate based on that documentation ceases to be valid, as required by the ECT Act.
13.9.2. Impression shall retain any audit logs generated for at least seven (7) years and shall make these audit logs available to GS or its auditors upon request.
13.9.3. Impression shall ensure that the records are deleted after the expiry of the seven (7) years.

13.10. Key Changeover: refer to Master CP, section 5.6

13.11. Compromise and Disaster Recovery: refer to Master CP, section 5.7 and subsections

13.12. CA or RA Termination: refer to Master CP, section 5.8 and subsections
13.12.1. Should Impression be removed as an RA/LRA of GS, the following termination process shall apply:
13.12.1.1. All stakeholders, including LRAs, SAAA, WebTrust, GS and Impression will be informed of GS intention to cancel the RA/LRA agreement
13.12.1.2. GS and Impression must agree on the sequence of events resulting in the termination
13.12.1.3. GS and Impression must agree on the most appropriate timing of the termination
13.12.1.4. Impression must ensure that SAAA and GS have access to all identity verification and digital certificate lifecycle management information for a period of seven (7) years.
13.12.1.5. Impression will ensure that all information is deleted after seven (7) years.

14. Technical Security Controls

14.1. Key Pair Generation and Installation: Key Pair Generation
14.1.1. CA Key Pair Generation: refer to Master CP, section 6.1.1.
14.1.2. Subscriber Key Pair Generation: For Subscriber AES keys generated by Impression, Key generation is performed in a secure cryptographic device that meets FIPS 140-2 using key generation algorithm and key size as specified in Master CP, Section 6.1.5 and 6.1.6.
14.1.3. Impression also rejects a certificate request if it has a known weak Private Key.
14.1.4. Impression does not generate key pairs for other certificate types

14.2. Private Key Delivery to Subscriber: refer to Master CP, section 6.1.2
14.2.1. Impression stores the private key of the Subscriber's AES on their behalf on a secure cryptographic HSM, where the key's usage is under the sole control of the Subscriber as per section 9.4
14.2.2. Impression does not store key pairs for other certificate types.

14.3. Public Key Delivery to CA: refer to Master CP, section 6.1.3

14.4. CA Public Key Delivery to Relying Parties: refer to Master CP, section 6.1.4

14.5. Key Sizes: refer to Master CP, section 6.1.5

14.6. Public Key Parameters Generation and Quality Checking: refer to Master CP, section 6.1.6

14.7. Key Usage Purposes (as per X.509 v3 Key Usage Field): refer to Master CP, section 6.1.7

14.8. Private Key Protection and Cryptographic Module Engineering Controls: refer to Master CP, section 6.2 and subsections

14.9. Other Aspects of Key Pair Management:
14.9.1. Public Key Archival: Impression archives Public Keys from AES Certificates.
14.9.2. Certificate Operational Periods and Key Pair Usage Periods: Impression AES Certificates and renewed Certificates have a maximum Validity Period of three (3) years
14.9.2.1. Key Pair usage period can have up to the same Validity Period as Certificate Validity Period.
14.9.2.2. Certificates signed by a specific CA must expire before the end of that Key Pair's operational period.
14.9.2.3. Impression and GS comply with the Baseline Requirements with respect to the maximum Validity Period. In the event that a Subscriber's Certificate has a reduced validity period, subsequent reissues may be used to regain that lost validity period.

14.10. Activation Data: refer to Master CP, section 6.4 and subsections

14.11. Computer Security Controls: refer to Master CP, section 6.5 and subsections

14.12. Lifecycle Technical Controls: refer to Master CP, section 6.6 and subsections

14.13. Network Security Controls: refer to Master CP, section 6.7 and subsections
14.13.1. Communication of digital certificate lifecycle events and transmission of subscriber information between LRAs, Impression and GS will be protected by:
14.13.1.1. **Internet Protocol ("IP")** address whitelisting;
14.13.1.2. **Transport Layer Security ("TLS")** encrypted endpoints;
14.13.1.3. **Application Programming Interface ("API")** keys that are unique per subscriber organisation and environment and;
14.13.1.4. Profile username and passwords provisioned to identity vetted RA/LRA administrators

14.14. Timestamping: refer to Master CP, section 6.8 and subsections

15. Certificate, CRL and OCSP Profiles

15.1. Refer to Master CP, section 7.0 and subsections

15.2. PKI Trust Hierarchy
15.2.1. Root: cn=GlobalSign CA for AATL - SHA384 - G4, o=GlobalSign nv-sa, c=BE
15.2.2. Issuing Authority: cn=GlobalSign CA 4 for AATL, o=GlobalSign nv-sa, c=BE
15.2.3. RA/LRA: Impression performing registration authority duties
15.2.4. LRA: Delegated face-to-face or equivalent identity verification and document gathering

15.3. Certificate Type and Content

15.3.1. Type: X.509
15.3.2. GS Subscriber Content: o=Organisation Name, l=City, st=Province, c=Country, serialnumber=Certificate Serial Number
15.3.3. RA/LRA Subscriber Content: cn=Subscriber First and Last Name, e=Subscriber Email, ou=Organisational Unit
15.3.4. Validity: One (1), two (2) or three (3) years
15.3.5. Timestamp Embedded: http://aatl-timestamp.globalsign.com/tsa/
15.3.6. CRL: http://crl.globalsign.com/gs/gsaatl4sha2g4.crl
15.3.7. OCSP: http://ocsp.globalsign.com/gsaatl4sha2g4

15.4. Certificate Purpose: Certificates issued under the **Adobe Approved Trust List ("AATL")** can be used for Digital Signature (of both documents and transactions), Non-Repudiation (of both documents and transactions) and Email Protection and should not be used for illegitimate business purposes.

16. Compliance Audit and Other Assessments

16.1. Refer to Master CP, section 8.0 and subsections
16.1.1. GS may audit Impression's records and/or inspect its facilities to verify Impression's statements and compliance with this charter, including but not limited to any privacy or security requirements.
16.1.2. Audits and inspections will be conducted by GS or an independent certified public accountant or consultant selected by GS.
16.1.3. GS will provide thirty (30) days' notice to Impression prior to the start of the audit or inspection.
16.1.4. Impression will provide reasonable access to the relevant records and facilities.
16.1.5. The auditors will have the ability to copy Impression's records for audit evidence.
16.1.6. If the results of an audit report recommend remedial action, Impression shall implement corrective action within thirty (30) days of receipt of such audit report. Failure to remediate in that period may lead to the suspension or termination of the RA/LRA by GS.
16.1.7. Independent audits will also be conducted once per calendar year by an evaluator that has been appointed to the SAAA panel of auditors to ensure compliance with the ECT Act and Regulations

17. Other Business & Legal Matters

17.1. Fees:
17.1.1. Certificate Issuance or Renewal Fees: Impression charges fees for Certificate issuance and renewal. Impression does not charge for reissuance (re-key during the lifetime of the Certificate). Fees and any associated terms and conditions are made clear to Applicants both by the enrollment process and the subscriber agreement.
17.1.2. Certificate Access Fees: Impression may charge for access to any database which stores issued Certificates.
17.1.3. Revocation or Status Information Access Fees: Impression may charge additional fees to Subscribers who have a large Relying Party community and choose not to use OCSP stapling or other similar techniques to reduce the load on the Impression and GS Certificate status infrastructure.
17.1.4. Fees for Other Services: Impression may charge for other additional services such as timestamping.
17.1.5. Refund Policy: Impression offers a refund to Subscribers who cancel their order within seven (7) days of certificate issuance. Subscribers who choose to invoke the refund policy should have all issued Certificates revoked.

17.2. Financial Responsibility: Refer to Master CP, section 9.2 and subsections

17.3. Confidentiality of Business Information:
17.3.1. Scope of Confidential Information: The following items are classified as being confidential information and therefore are subject to reasonable care and attention by Impression staff including Vetting Agents and administrators:
17.3.1.1. Personal Information as detailed in Master CP, Section 9.4;
17.3.1.1.1. Personal data are data used to identify persons. Impression holds a database of the subscribers' personal data and is the holder of the personal data file and thus responsible for the use and protection of the data.

17.3.1.2. Audit logs from RA systems;
17.3.1.3. Internal Impression business process documentation including **Business Continuity Plans ("BCP")**
17.3.1.4. Audit Reports from an independent auditor as detailed in Master CP, Section 8.0; and
17.3.1.5. Any documentation or other materials that are marked as "Confidential";
17.3.2. Information Not Within the Scope of Confidential Information: Confidential Information shall not include:
17.3.2.1. any information that is available to the public or from sources other than GS (provided that such source is not subject to obligations of confidentiality with regard to such information);
17.3.2.2. any information that is independently developed by Impression without use of or reference to information from GS; or
17.3.2.3. is required by law, regulatory agency or court order to be disclosed by Impression.
17.3.3. Responsibility to Protect Confidential Information: Impression is required to ensure that RA/LRA's it appoints are bound by confidentiality obligations at least as stringent as those stated herein.
17.3.3.1. Impression protects confidential information through training and enforcement with employees, agents and contractors.

17.4. Privacy of Personal Information: Refer to Master CP, section 9.2 and subsections

17.5. Intellectual Property Rights: Impression does not knowingly violate the intellectual property rights of third parties. Public and Private Keys remain the property of Subscribers who legitimately hold them. GS retains ownership of Certificates; however, it grants permission to reproduce and distribute Certificates on a non-exclusive, royalty free basis, provided that they are reproduced and distributed in full.

17.6. Representations and Warranties: Refer to Master CP, section 9.6 and subsections

17.7. Disclaimers of Warranties: Refer to Master CP, section 9.7

17.8. **Neither GS, nor Impression, nor the employees, or directors of any of the foregoing entities shall be liable for (a) indirect or special damages and/or (b) loss of income or profit and/or (c) any other form of consequential damages howsoever arising and regardless of form or cause or action.**

17.9. Indemnities: Refer to Master CP, section 9.9 and subsections

17.10. Term & Termination:
17.10.1. Term: This CP remains in force until such time as communicated otherwise by Impression on its web site or Repository.
17.10.2. Termination: Notified changes are appropriately marked by an indicated version. Changes become effective immediately upon publication.
17.10.3. Effect of Termination and Survival: Impression will communicate the conditions and effect of this CP termination via the appropriate Repository.

17.11. Governing Law: This CP is governed, construed and interpreted in accordance with the laws of South Africa. This choice of law is made to ensure uniform interpretation of this CP, regardless of the place of residence or place of use of Impression Certificates or other products and services. The law of South Africa applies also to all Impression commercial or contractual relationships in which this CP may apply or quoted implicitly or explicitly in relation to Impression products and services where Impression acts as a provider, supplier, beneficiary receiver or otherwise.