Purpose: This document outlines the business processes and practices of Impression with regards to its digital certificate lifecycle and management solution that supports Advanced Electronic Signatures in South Africa.

Copyright notice: This document and any new versions of this document are the property of Impression Signatures (Pty) Ltd ("Impression"). No part of this document may be reproduced or transmitted without the express permission of Impression. Enquiries can be directed to aes@impression.cloud.

1. Introduction

1.1. **Impression Signatures (Pty) Ltd ("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. **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. Education, experience and trustworthiness

2.1. Impression staff who have been delegated the RA/LRA functions shall meet the following minimum criteria:

2.1.1. a minimum of two (2) years studies leading directly to a university degree and/or two (2) years' experience in digital certification or equivalent;
2.1.2. have not been convicted of a serious crime;
2.1.3. will undergo a criminal and credit worthiness background check.

3. Records Retention

3.1. 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.

3.2. 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.

3.3. Impression shall ensure that the records are deleted after the expiry of the seven (7) years.

4. Compliance with CP and CPS

4.1. Impression must comply with its **Certificate Policy ("CP")** and **Certification Practice Statement ("CPS")** which GS has previously verified complies with their own CP, CPS and the Baseline Requirements, available for viewing/download from https://www.impression-signatures.com/pages/legal

5. Audit

5.1. 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.

5.1.1. Audits and inspections will be conducted by GS or an independent certified public accountant or consultant selected by GS.

5.1.2. GS will provide thirty (30) days' notice to Impression prior to the start of the audit or inspection.

5.1.3. Impression will provide reasonable access to the relevant records and facilities.

5.1.4. The auditors will have the ability to copy Impression's records for audit evidence.

5.2. 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.

5.3. 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

6. Personal Data Protection

6.1. 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.

7. Confidentiality

7.1. Impression shall treat as confidential, shall not use for any purpose other than as set forth in this Charter, and shall not disclose or transmit to any third party:

7.1.1. any documentation or other materials that are marked as "Confidential"; and

7.1.2. any information concerning GS procedures, or any documentation used in connection with the certificate management process.

7.2. Confidential Information as described in 7.1.1 shall not include:

7.2.1. 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);

7.2.2. any information that is independently developed by Impression without use of or reference to information from GS; or

7.2.3. is required by law, regulatory agency or court order to be disclosed by Impression.

7.3. Impression is required to ensure that RA/LRA's it appoints are bound by confidentiality obligations at least as stringent as those stated herein.

8. Limitation of Liability

8.1. **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.**

9. Certificate Configuration

9.1. PKI Trust Hierarchy

9.1.1. Root: cn=GlobalSign CA for AATL - SHA384 - G4, o=GlobalSign nv-sa, c=BE

9.1.2. Issuing Authority: cn=GlobalSign CA 4 for AATL, o=GlobalSign nv-sa, c=BE

9.1.3. RA/LRA: Impression performing registration authority duties

9.1.4. LRA: Delegated face-to-face or equivalent identity verification and document gathering

9.2. Certificate Type and Content

9.2.1. Type: X.509

9.2.2. GS Subscriber Content: o=Organisation Name, l=City, st=Province, c=Country, serialnumber=Certificate Serial Number

9.2.3. RA/LRA Subscriber Content: cn=Subscriber First and Last Name, e=Subscriber Email, ou=Organisational Unit

9.2.4. Validity: One (1), two (2) or three (3) years

9.2.5. Timestamp Embedded: http://aatl-timestamp.globalsign.com/tsa/

9.2.6. CRL: http://crl.globalsign.com/gs/gsaatl4sha2g4.crl

9.2.7. OCSP: http://ocsp.globalsign.com/gsaatl4sha2g4

9.3. Certificate Purpose

9.3.1. 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.

10. Private Key Protection

10.1. 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:

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

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

10.1.3. 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:

10.1.3.1. 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.

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

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

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

10.1.5. 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.

10.1.6. *** delegated auth process ***

11. Transport Security

11.1. Communication of digital certificate lifecycle events and transmission of subscriber information between LRAs, Impression and GS will be protected by:

11.1.1. **Internet Protocol ("IP")** address whitelisting;

11.1.2. **Transport Layer Security ("TLS")** encrypted endpoints;

11.1.3. **Application Programming Interface ("API")** keys that are unique per subscriber organisation and environment and;

11.1.4. Profile username and passwords provisioned to identity vetted RA/LRA administrators

12. Application Process

12.1. Upon the verification and approval of an organisational profile and assignment of certificate content as per 9.2.2 by GS, Impression shall serve as RA/LRA for the subscriber content as per 9.2.3. Impression will be entitled to accept subscriber applications for the issuance of AES certificates.

12.2. The following information will be gathered and verified during an application by a natural person:

12.2.1. An electronic copy of the applicant's passport, South African ID card or South African 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.

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

12.2.3. A completed subscriber agreement signed in the presence of the authorised enrolment officer.

12.3. The following information will be gathered during a certificate renewal application by a natural person:
12.3.1. An active and valid AES certificate.
12.3.2. An updated and verified subscriber agreement signed with 12.3.1.

13. Lifecycle Events

13.1. Issuance and Acceptance:
13.1.1. The LRA will transmit the completed information to Impression who will upon performing the requisite validation, create a private key as per section 10 and issue a **Certificate Signing Request ("CSR")** to GS who will sign the request according to the hierarchy defined in 9.1.
13.1.2. The signed public certificate returned is known as the AES and is published
13.1.3. The RA/LRA are informed via the Impression API on the outcome of the subscriber's application
13.1.4. The subscriber is notified and shall check the content of their AES and unless otherwise informed, Impression shall deem the information contained on the certificate correct and the AES accepted by the subscriber.

13.2. Verification and Reliance:
13.2.1. Documents and transactions signed with the AES can be checked for validity by checking the revocation status on the GS **Certificate Revocation List ('CRL")** and **Online Certificate Status Protocol ("OCSP")** responders.
13.2.2. **Portable Document Format ("PDF")** documents signed with the AES will also display document integrity, **Timestamp Authority ("TSA")** as well as **Long Term Validation ("LTV")** indicators on standards compliant PDF readers.

13.3. Name Changes:
13.3.1. Name changes result in the **Common Name ("cn")** attribute of the certificate changing which is a key identity attribute that is verified during the subscriber application process. The subscriber would therefore need to complete a new application under the new name and present their updated identity documentation.
13.3.2. Upon a successful name change application, the previous certificate and associated key issued are revoked and a new key pair is issued.

13.4. Revocation:
13.4.1. The following circumstances would result in revocation:
13.4.1.1. A request from the subscriber to revoke their certificate
13.4.1.2. Changes in information contained on the certificate, such as name
13.4.1.3. Subscriber abuse of their digital certificate
13.4.1.4. Subscriber suspected of fraudulent activity
13.4.1.5. Compromise of the subscriber's private key, Impression's private key or GS private key
13.4.1.6. A subscriber's breach of their subscriber agreement
13.4.1.7. Non-payment of fees to Impression or GS
13.4.1.8. Issue or use of a digital certificate that is not in line with the Impression CPS and CP
13.4.1.9. Upon receipt of a certified death certificate of a subscriber
13.4.1.10. Expiry of the superior certificates in the PKI hierarchy
13.4.1.11. Any other reason that Impression reasonably believes that the integrity, security or trustworthiness of Impression certificates.
13.4.2. Upon verifying that the revocation reasons are valid, an RA/LRA may request Impression to revoke a subscriber's key and certificate
13.4.3. Impression will request GS to revoke the certificate and if possible, cancel the associated certificate license for re-use, if the revocation occurs within seven (7) days of first issue.
13.4.4. GS will publish a revocation entry on the GS public CRL and OCSP
13.4.5. Impression will notify the subscriber and the LRA that the revocation request have been completed, via email.

13.5. Suspension:
13.5.1. Impression nor GS support certificate or private key suspension

13.6. Certificate renewal before expiry:

13.6.1. Automated renewal can be completed by the subscriber by ensuring they complete a renewal request and sign an updated and verified subscriber agreement with their existing, valid AES. Renewal can be completed up to three (3) months before expiry and Impression will notify the subscriber when their renewal period has started.

13.7. Certificate renewal post expiry, name change and revocation:

13.7.1. In the case of a name change, revocation or certificate expiry, the subscriber will need to start a new and complete application process. In all these cases, the certificate and the private key were revoked and are no longer usable.

14. Termination

14.1. Should Impression be removed as an RA/LRA of GS, the following termination process shall apply:

14.1.1. All stakeholders, including LRAs, SAAA, WebTrust, GS and Impression will be informed of GS intention to cancel the RA/LRA agreement

14.1.2. GS and Impression must agree on the sequence of events resulting in the termination

14.1.3. GS and Impression must agree on the most appropriate timing of the termination

14.1.4. 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.

14.1.5. Impression will ensure that all information is deleted after seven (7) years.