Idently
Certificate Policy

Date: April 28th, 2021

Version: v.1.0

Table of Contents

Document History

Version	Release Date	Status & Description
V1.0	28/04/2021	First Version

Acknowledgments

1.0 Introduction

This Certificate Policy (CP) applies to the products and services of Idently Systems Limited and affiliated entities ("Idently"). Primarily, this pertains to the issuance and lifecycle management of Certificates including validity checking services. Idently may also provide additional services such as timestamping. 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 Idently group company repository https://www.idently.com/repository. (*Alternative languages versions may be available to aid Relying Parties and Subscribers in their understanding of this CP, however, in the event of any inconsistency, the English version shall control).*

A CP is a "named set of rules that indicates the applicability of a Digital Certificate to a particular community and/or class of application with common security requirements." This CP 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 policy according to the structure of RFC 3647, the topic may not necessarily apply to services of Idently. These sections have 'No stipulation' appended. Where necessary, additional information is presented in subsections to the standard structure. 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 Idently's practices and procedures.

This CP aims to comply with the requirements of:

- Browsers' root programs
- RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003
- WebTrust Principles and Criteria for Certification Authorities
- The Kenya Information And Communications (Electronic Certification And Domain Name Administration) Regulations, 2010

This CP conforms to current versions of the requirements:

- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements" or "BR")
- CA/Browser Forum Network and Certificate System Security Requirements

published at http://www.cabforum.org. If there is any inconsistency between this document and the Requirements above, the Requirements take precedence over this document.

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. This CP applies to all Certificates issued by Idently including its Root Certificates and any chaining services to third party Subordinate/Issuing CAs. Root Certificates are used to manage Certificate hierarchies through the creation of one or more Subordinate CAs that may or may not be controlled directly by the same entity that manages the Root Certificate itself.

This CP is applicable to the Subscriber and/or Relying Party, who uses, relies upon or attempts to rely upon certification services made available by the Certification Authority referring to this CP.

The English version of this CP is the primary version. In the event of any conflict or inconsistency between the English CP and any localized or translated version, the provisions of the English version shall prevail.

1.1 Overview

This CP applies to the complete Idently hierarchy of Idently and all Certificates that it issues either directly through its own systems or indirectly through its Dedicated Issuing CA™ *(Previously known as Root Sign)* program including self-signed Root Certificates and Key Pairs. The purpose of this CP is to present Idently's practices and procedures in managing Root Certificates and Issuing CAs in order to demonstrate compliance with formal industry accepted accreditations such as WebTrust. Additionally, eIDAS Regulation (Regulation (EU)N910/2014) ("eIDAS") and eIDAS (UK Legislation) and The Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 ("UK eIDAS") provide for the recognition of Electronic Signatures that are used for the purposes of authentication or nonrepudiation. In this regard, Idently operates within the scope of the applicable sections of the Law when delivering its services. Trust services for the United Kingdom are operated by and provided through GMO Idently LTD., an affiliate entity of Idently.

This CP sets out the objectives, roles, responsibilities and practices of all entities involved in the lifecycle of Certificates issued under this CP. In simple terms, a CP states *"what is to be adhered to,"* setting out an operational rule framework for products and services.

A Certification Practice Statement (CPS) complements this CP and states, *"how the Certification Authority adheres to the Certificate Policy."* A CPS provides an end user with a summary of the processes, procedures and overall prevailing conditions that the Issuing CA *(i.e. the entity which provides the Subscriber its Certificate)* will use in creating and managing such Certificates. Likewise, Idently Dedicated Issuing CA Subscribers who themselves become an *Issuing CA* maintain their own Certificate Practice Statement applicable to products and services they offer.

In addition to this CP and the CPS, Idently maintains additional documented policies which address such issues as:

- Business continuity and disaster recovery
- Security policy
- Personnel policies
- Key management policies
- Registration procedures

Additionally, other relevant documents include:

- The Idently Warranty Policy that addresses issues on insurance;
- The Idently Privacy Policy on the protection of personal data; and
- The Idently Certification Practice Statement that addresses the methods and rules by which Certificates are delivered for the domain of the Idently top roots.

All applicable Idently policies are subject to audit by authorised third parties which Idently highlights on its public facing web site via a WebTrust Seal of Assurance. Additional information can be made available upon request.

1.1.1 Certificate Naming

The exact names of the Idently Certificates that are governed by this CP are:

Idently Public Root CA Certificates

- <TBC>

Idently Public Non-TLS Root CA Certificates

- <TBC>

The Root Certificates above are Public, WebTrust-audited certificates that are configured for non-TLS use, to cater to Idently's various product offerings. Idently actively promotes the inclusion of the Root Certificates above in hardware and software platforms that are capable of supporting Certificates and associated cryptographic services according to the specified Idently use case and applicable hardware/software trust bits. Where possible, Idently will seek to enter into a contractual agreement with platform providers to ensure effective Root Certificate life cycle management. However, Idently also actively encourages platform providers at their own discretion to include Idently Root Certificates without contractual obligation.

Idently Non-public Root CA Certificates

- <TBC>

Idently actively promotes the inclusion of the Root Certificates above into hardware and software platforms that are capable of supporting Certificates and associated cryptographic services. Where possible, Idently will seek to enter into a contractual agreement with platform providers to ensure effective Root Certificate lifecycle management. However, Idently also actively encourages platform providers at their own discretion to include Idently Root Certificates without contractual obligation.

Dedicated Issuing CA is a Idently service, which allows third party Issuer CAs to chain to one of the Idently Certificates.

Dedicated Issuing CA TPM is the Idently service which allows third party Issuing CAs to chain to one of the Idently Trusted Platform Module Root Certificates above.

Certificates allow entities that participate in an electronic transaction to prove their identity to other participants or sign data digitally. By means of a Certificate, a Certification Authority provides confirmation of the relationship between a named entity (Subscriber) and its Public Key. For Dedicated Issuing CA CA's, the purpose of entering the Idently hierarchy is to enhance trust in an Issuer CA's own hierarchy, as well as providing greater functionality within third party applications such as web browsers. It is the duty of any Dedicated Issuing CA Issuer CA to assess the value of the Idently services at any point in time and act accordingly.

The process to obtain a Certificate includes the identification, naming, authentication and registration of an Applicant as well as aspects of Certificate management such as the issuance, revocation and expiration. By means of this policy, Idently provides confirmation of the identity of the Subject of a Certificate by binding the Public Key the Subscriber uses through the issuance of a Certificate. An entity in this instance might include an end user or another Certification Authority. Idently makes available Certificates that can be used for non-repudiation/contentCommitment, encryption and authentication. The use of these Certificates can be further limited to a specific business or contractual context or transaction level in support of a warranty policy or other limitations imposed by the applications that Certificates are used in.

Idently accepts comments regarding this CP addressed to the address stated in Section 1.5, *Policy Administration.*

1.1.2 Additional requirements for Dedicated Issuing CA Issuer CAs

This CP also addresses the Dedicated Issuing CA program for authorized Issuing CAs. Entering the Idently hierarchy is carried out through a CA chaining program that Idently makes available to interested parties under the Dedicated Issuing CA brand. Dedicated Issuing CA Certificates are typically:

- Issued by Idently to a third-party Issuing CA that meets the contractual, audit and policy requirements of Idently Dedicated Issuing CA services with regard to operational practices and technical implementation;
- Issued only to enterprise in-house CAs to issue SSL and/or S/MIME Certificates for use under their own brand to their own target audience;
- Provide allowance for additional Certificate types as required to provide lifecycle management such as but not limited to key escrow Certificates and OCSP signing Certificates;
- Not allowed to be used for code signing Certificates; and
- Constrained to specific domains for either SSL and/or S/MIME usage to protect both the third party and Idently hierarchy.

Idently expressly forbids the use of chaining services for MITM (Man in the Middle) SSL/TLS deep packet inspection.

1.2 PKI Participants

1.2.1 Certification Authorities ("Issuer CAs")

A Certification Authority (CA)'s primary responsibility is to perform tasks related to Public Key Infrastructure (PKI) functions such as Certificate lifecycle management, Subscriber registration, Certificate issuance, Certificate renewal, Certificate distribution and Certificate revocation. Certificate status information may be provided using a Repository in the form of a Certificate Revocation List (CRL) distribution point and/or Online Certificate Status Protocol (OCSP) responder. A Certification Authority may also be described by the term *"Issuing Authority" or "Issuer CA"* to denote its purpose of issuing Certificates at the request of a Registration Authority (RA) from a Subordinate CA which may or may not be managed by Idently (i.e. a Dedicated Issuing CA Issuing CA).

The Idently Policy Authority, which is composed of members of the Idently management team and appointed by its Board of Directors, is responsible for maintaining this Certificate Policy relating to all Certificates in the Idently hierarchy. Through its Policy Authority, Idently has ultimate control over the lifecycle and management of the Idently Root CA and any subsequent Subordinate CAs including Dedicated Issuing CA Issuing CAs belonging to the hierarchy.

Henceforth and for ease of reference all CAs issuing Certificates in accordance with this CP (including Idently) shall be referred to as Issuing CAs.

Issuing CAs ensure the availability of all services relating to the management of Certificates issued. Appropriate publication is necessary to ensure that Relying Parties obtain notice or knowledge of revoked Certificates. Issuing CAs provide Certificate status information using a Repository in the form of a CRL distribution point and/or OCSP responder as indicated within the Certificate properties.

1.2.2 Registration Authorities

In addition to identifying and authenticating Applicants for Certificates, an RA may also initiate or pass along revocation requests for Certificates and requests for renewal and re-key of Certificates.

Issuing CAs may act as a Registration Authority for Certificates they issue in which case they are responsible for:

- Accepting, evaluating, approving or rejecting the registration of Certificate applications;
- Registering Subscribers for certification services;
- Providing systems to facilitate the identification of Subscribers (according to the type of Certificate requested);
- Using officially notarised or otherwise authorised documents or sources of information to evaluate and authenticate an Applicant's application;
- Requesting issuance of a Certificate via a multi-factor authentication process following the approval of an application; and
- Initiating the process to revoke a Certificate from the applicable Idently Subordinate CA or partner Subordinate CA.

Third party Issuing CAs who enter into a contractual relationship with Idently may operate their own RA and authorize the issuance of Certificates. Third parties must comply with all the requirements of this CP and the terms of their contract which may also refer to additional criteria as recommended by the CA/B Forum. RAs may implement more restrictive vetting practices if their internal policy dictates.

In order to issue certain Certificate types, RAs may need to rely on Certificates issued by third party Certification Authorities or other third-party databases and sources of information Such as government national identity cards such as passwords, eID, and drivers licenses. Where the RA

relies on Certificates issued by third party Certification Authorities, Relying Parties are advised to review additional information by referring to such third party's CPS.

Issuing CAs may designate an Enterprise RA to verify Certificate Requests from the Enterprise RA's own organization. In Enterprise RA, the Subscriber's organization shall be validated and predefined, and shall be constrained by system configuration.

1.2.3 Subscribers

Subscribers of Issuing CAs are either directly reliant on the Issuing CA to issue end entity Certificates from a hierarchy managed by the Issuing CA or they are third parties that seek to be issued with an Issuing CA capable of issuing additional Certificates to their own PKI hierarchy. Subscribers are either Legal Entities or natural persons that successfully apply for and receive a Certificate to support their use in transactions, communications and the application of Digital Signatures. In some cases, individuals are not able to obtain certain Certificate types.

A *Subscriber*, as used herein, refers to both the Subject of the Certificate and the entity that contracted with the Issuing CA for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an *Applicant*.

End entity Subscribers:

- Have ultimate authority over the Private Key corresponding to the Public Key that is listed in a Subscriber's Certificate. A Subscriber may or may not be the Subject of a Certificate (For example, machine or role-based Certificates issued to firewalls, routers, servers or other devices used within an organization).

Dedicated Issuing CA Subscribers:

- Set the framework of providing certification services with the CA hierarchy for the benefit of the Subject mentioned in a Certificate;
- Accept and implement the contractual, audit and policy requirements of Idently Dedicated Issuing CA services with regard to operational practices and technical implementation:
- Can only be enterprise in-house PKIs. No public PKI services are allowed; and
- Idently reserves the right to technically constrain the breadth of a domain through the use of subordination (For example, RFC 5280 dNSName Name Constraints).

Natural persons can be listed as the Subject of the following Certificates:

- **Personal**
- **Professional**

Natural or Department / role based legal persons within an Organizational context can be listed as the Subject of the following Certificates:

- **Professional**
- **Organization**

Legal Entities created through all recognized forms of incorporation or government entities can be listed as the Subject of the following Certificates:

- **Organization**
- **Timestamping**

Legal Entities or self-employed professionals can be listed as the Subject of the following Certificates:

- **Organization**

RFC822 email addresses may be listed as the Subject of the following Certificates.

- **Personal**

1.2.4 Relying Parties

Business partners of a Dedicated Issuing CA partner that receive S/MIME Certificates issued by the Dedicated Issuing CA Subscriber's CA are effectively Subscribers and Relying Parties at the same time.

To verify the validity of a Certificate, Relying Parties must always refer to Issuing CA revocation information which is usually presented in the applicable end entity Certificate and appropriate chain of Certificates.

1.2.5 Other Participants

Other participants include bridge CAs and CAs that cross certify Issuing CAs to provide trust among other PKI communities.

1.3 Certificate Usage

A Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Certificates are used in commercial environments as a digital equivalent of an identification card.

1.3.1 Appropriate Certificate Usage

End entity Certificate use is restricted by using Certificate extensions on key usage and extended key usage. End entity Certificate use is restricted by the key usage and extended key usage values.

Subordinate CA Certificates issued under the Dedicated Issuing CA program can be used to issue Certificates for transactions that require:

- Authentication;
- Assurance about the identity of a remote device; and
- Encryption

Additional uses are specifically designated once they become available to end entities. Unauthorised use of Certificates may result in the voiding of warranties offered by Idently to Subscribers and their Relying Parties.

1.3.2 Prohibited Certificate Usage

Certificate use is restricted by using Certificate extensions on key usage and extended key usage. Any usage of the Certificate inconsistent with these extensions is not authorised. Certificates are not authorised for use for any transactions above the designated reliance limits that have been indicated in the Idently Warranty Policy.

Certificates do not guarantee that the Subject is trustworthy, operating a reputable business or that the equipment into which the Certificate has been installed is free from defect, malware or virus. In the case of code signing, Certificates do not guarantee that signed code is free from bugs or vulnerabilities.

Certificates issued under this CP may not be used:

- For any application requiring fail safe performance
- For any application or mechanism where issues with the certificate could cause a safety risk (e.g. human or environmental risk)
- Where prohibited by law

1.4 Policy Administration

1.4.1 Organization Administering the Document

Requests for information on the compliance of Issuing CAs with accreditation schemes as well as any other inquiry associated with this CP should be addressed to:

CA Governance Policy Authority
Idently Systems Limited
Four Greenway, 2nd Floor,
Westlands Road, Nairobi.
Tel: + 254 734467635
Email: legal@Idently.com

1.4.2 Contact Person

General Inquiries

Idently Systems, ATTN. Legal Practices,
Four Greenway, 2nd Floor,
Westlands Road, Nairobi.
Tel: + 254 734467635
Email: legal@Idently.com

URL: https://www.idently.com

Certificate Problem Report

Anti-Malware Organizations, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may report suspected Private Key Compromise, Certificate misuse, Certificates used to sign Suspect Code, Takeover Attacks, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates by sending email to:

report-abuse@Idently.com

Idently may or may not revoke in response to this request. See section 4.9.5 for detail of actions performed by Idently for making this decision.

1.4.3 Person Determining CP Suitability for the Policy

Idently CA Governance Policy Authority determines the suitability and applicability of this CP and the conformance of a CPS to this CP based on the results and recommendations received from a Qualified Auditor.

In an effort to maintain credibility and promote trust in this CP and better correspond to accreditation and legal requirements, Idently CA Governance Policy Authority 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. 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.

1.4.4 CP Approval Procedures

Idently CA Governance Policy Authority reviews and approves any changes to the CP. Upon approval of a CP update by Idently CA Governance Policy Authority, the new CP is published in the Idently Repository at https://www.idently.com/repository.

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.

1.5 Definitions and Acronyms

Any terms used but not defined herein shall have the meaning ascribed to them in the Baseline Requirements and/or the Kenya Electronic and Digital Signature Laws.

Adobe Approved Trust List (AATL): A document signing certificate authority trust store created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 9.0

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity.

Anti-Malware Organization: An entity that maintains information about Suspect Code and/or develops software used to prevent, detect, or remove malware.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Legal Entity is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual Certificate Request.

Application Software Supplier: A supplier of Internet browser software or other Relying Party application software that displays or uses Certificates and incorporates Root Certificates.

Attestation Letter: A letter attesting that Subject Identity Information is correct.

Business Entity: Any entity that is not a Private Organization, Government Entity, or noncommercial entity as defined in the EV Guidelines. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.

CDS (Certified Document Services): A document signing architecture created by the Adobe Root CA policy authority implemented from Adobe PDF Reader version 6.0.

Certificate: An electronic document that uses a digital signature to bind a Public Key and an identity.

Certificate Authority Authorization (CAA): The CAA record is used to specify which Certificate authorities are allowed to issue Certificates for a domain.

Certificate Beneficiaries: The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate, all Application Software Suppliers with whom Idently has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier, and all Relying Parties who reasonably rely on a Valid Certificate.

Certificate Data: Certificate Requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which the CA has access.

Certificate Management Process: Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Policy: A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Problem Report: A complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Request: Communications described in Section 10 of the Baseline Requirements requesting the issuance of a Certificate.

Certificate Revocation List: A regularly updated timestamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.

Certification Practice Statement: One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Common CA Database (CCADB): A certificate repository run by Mozilla, where all publicly trusted root and issuing certificates are listed.

Compromise: A violation of a security policy that results in loss of control over sensitive information.

Country: Either a member of the United Nations OR a geographic region recognized as a sovereign nation by at least two UN member nations.

Cross Certificate: A Certificate that is used to establish a trust relationship between two Root CAs.

Digital Signature: To encode a message by using an asymmetric cryptosystem and a hash function such 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 initial message has been altered since the transformation was made.

DNS CAA Email Contact: The email address defined in Appendix B.1.1. of the Baseline Requirements.

DNS TXT Record Email Contact: The email address defined in Appendix B.2.1. of the Baseline Requirements.

DNS TXT Record Phone Contact: The phone number defined in Appendix B.2.2. of the Baseline Requirements.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record, or as obtained through direct contact with the Domain Name Registrar.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Name System: An Internet service that translates *Domain Names* into IP addresses.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the "owner" of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the "Registrant" by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii)

a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

Electronic Seal: Data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity;

Electronic Signature: Data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign

Enterprise PKI (EPKI): A Idently product for organizations to manage the full lifecycle of Microsoft Window's trusted digital IDs, Adobe Approved Trust List, and Adobe Certified Document Services, including issuing, reissuing, renewing, and revoking.

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization or its subsidiaries. An Enterprise RA may also authorize issuance of client authentication Certificates to partners, customers, or affiliates wishing to interact with that organization.

Expiry Date: The "Not After" date in a Certificate that defines the end of a Certificate's Validity Period.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

Idently Certificate Center (idCC): A cloud-based certificate management system through which customers and partners may purchase and manage Certificates from Idently.

Global Positioning System (GPS): A U.S.-owned utility that provides users with positioning, navigation, and timing (PNT) services.

Governmentally Accepted Form of ID: A physical or electronic form of ID issued by the local country/state government or a form of ID that the local government accepts for validating identities of Individuals for its own official purposes.

Government Entity: A government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a Country, or political subdivision within such Country (such as a state, province, city, county, etc.).

Hash (e.g. SHA1 or SHA256): An algorithm that maps or translates one set of bits into another (generally smaller) set in such a way that:

- A message yields the same result every time the algorithm is executed using the same message as input.
- It is computationally infeasible for a message to be derived or reconstituted from the result produced by the algorithm.
- It is computationally infeasible to find two different messages that produce the same hash result using the same algorithm.

Hardware Security Module (HSM): A type of secure crypto processor targeted at managing digital keys, accelerating crypto processes in terms of digital signings/second and for providing strong authentication to access critical keys for server applications.

Internal Server Name: A server name (which may or may not include an Unregistered Domain Name) that is not resolvable using the public DNS.

Incorporate by Reference: To make one document a part of another by identifying the document to be incorporated, with information that allows the recipient to access and obtain the incorporated message in its entirety, and by expressing the intention that it be part of the incorporating message.

Such an incorporated message shall have the same effect as if it had been fully stated in the message.

Incorporating Agency: In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the entity is registered (e.g., the government agency that issues certificates of formation or incorporation). In the context of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Individual: A natural person.

Internationalized Domain Name (IDN): An internet domain name containing at least one language-specific script or alphabetic character which is then encoded in punycode for use in DNS which accepts only ASCII strings.

IP Address: A 32-bit or 128-bit label assigned to a device that uses the Internet Protocol for communication.

IP Address Contact: The person(s) or entity(ies) registered with an IP Address Registration Authority as having the right to control how one or more IP Addresses are used.

IP Address Registration Authority: The Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC).

Issuing CA: In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Jurisdiction of Incorporation: In the context of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.

Key Compromise: A Private Key is said to be Compromised if its value has been disclosed to an unauthorized person, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person may discover its value.

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a Country's legal system.

Network Time Protocol (NTP): A networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

Object Identifier (OID): A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables Relying Party application software to determine the status of an identified Certificate. See also OCSP Responder.

Place of Business: The location of any facility (such as a factory, retail store, warehouse, etc.) where the Applicant's business is conducted.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Private Organization: A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure (PKI): A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key cryptography.

Publicly-Trusted Certificate: A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2 (Identity/ Qualifications of Assessor).

Qualified Government Information Source: A database maintained by a Government Entity.

Qualified Government Tax Information Source: A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals.

Qualified Independent Information Source: A regularly updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information.

Registered Domain Name: A Domain Name that has been registered with a Domain Name Registrar.

Registration Authority (RA): Any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA may assist in the Certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

Relying Party: Any natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such supplier merely displays information relating to a Certificate.

Repository: An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response.

Root CA: The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

SSL Certificate: Certificates intended to be used for authenticating servers accessible through the Internet.

Subject: The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

Subject Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the commonName field.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Subscriber: A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber Agreement or Terms of Use.

Subscriber Agreement: An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Takeover Attack: An attack where a Signing Service or Private Key associated with a Code Signing Certificate has been compromised by means of fraud, theft, intentional malicious act of the Subject's agent, or other illegal conduct.

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the Baseline Requirements when the Applicant/Subscriber is an Affiliate of the CA.

Trusted Platform Module (TPM): A hardware cryptographic device which is defined by the Trusted Computing Group. https://www.trustedcomputinggroup.org/specs/TPM.

Trusted Third Party: A service provider with a secure process used for individual identity verification based on Governmentally Accepted Form(s) of ID, or whose service itself is considered to generate a Governmentally Accepted Form of ID.

Trustworthy System: Computer hardware, software, and procedures that are: reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialist: Someone who performs the information verification duties specified by the Baseline Requirements.

Validity Period: The period of time measured from the date when the Certificate is issued until the Expiry Date.

WebTrust Program for CAs: The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities.

WebTrust Seal of Assurance: An affirmation of compliance resulting from the WebTrust Program for CAs.

Wildcard Certificate: A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate.

WHOIS Lookup: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

X.400: The standard of the ITU-T (International Telecommunications Union-T) for E-mail.

X.500: The standard of the ITU-T (International Telecommunications Union-T) for Directory Services.

X.509: The standard of the ITU-T (International Telecommunications Union-T) for Certificates.

AATL	Adobe Approved Trust List
API	Application Programming Interface
ARL	Authority Revocation List (A CRL for Issuing CAs rather than end entities)
CA	Certification Authority
CAA	Certificate Authority Authorization
CCADB	Common CA Database
ccTLD	Country Code Top-Level Domain
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
EIR	Electric Industry Registry
EKU	Extended Key Usage
EPKI	Enterprise PKI
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
idCC	Idently Certificate Center
GPS	Global Positioning System
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
ITU	International Telecommunications Union
LRA	Local Registration Authority
NCA	National Competent Authority
NIST	(US Government) National Institute of Standards and Technology
NTP	Network Time Protocol
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PSP	Payment service provider
QGIS	Qualified Government Information Source
QGTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
RA	Registration Authority
RFC	Request for Comments
S/MIME	Secure MIME (Multipurpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
VAT	Value Added Tax

2.0 Publication and Repository Responsibilities

2.1 Repositories

The Issuing CA shall publish all CA Certificates and Cross Certificates issued to and from the Issuing CA, revocation data for issued Certificates, CP, CPS, and Relying Party agreements and Subscriber Agreements in Repositories. The Issuing CA shall ensure that revocation data for issued Certificates and its Root Certificate are available through a Repository 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled downtime that does not exceed 0.5% annually.

All parties who are associated with the issuance, use or management of Issuing CA Certificates are hereby notified that Issuing CAs may publish submitted information on publicly accessible directories for the provision of Certificate status information.

Issuing CAs may refrain from making publicly available certain sensitive and/or confidential documentation including security controls, operating procedures, and internal security policies. These documents are, however, made available to Qualified Auditors as required during any WebTrust audit performed on Idently.

Country specific web sites and translations of this CP and other public documentation may be made available by Issuing CAs for marketing purposes, however the repositories for all Idently public facing documentation are https://www.idently.com/repository and https://www.idently.com/corporate-policies and in the event of any inconsistency, the English version shall control.

2.2 Publication of Certificate Information

Idently publishes its CP, CPS, Subscriber Agreements, and Relying Party agreements at https://www.idently.com/repository. The CP and CPS include all the material required by RFC 3647, and are structured in accordance with RFC 3647.

2.3 Time or Frequency of Publication

CA Certificates are published in a Repository via support pages as soon as possible after issuance. CRLs for end entity Certificates are updated every 24 hours and are valid for 7 days. CRLs for CA Certificates are issued at least every 3 months and within 24 hours if a CA Certificate is revoked. Each CRL includes a monotonically increasing sequence number for each CRL issued.

Idently reviews its CP and CPS at least annually and makes appropriate changes so that Idently operation remains accurate, transparent and complies with external requirements listed in the "*Acknowledgements*" section of this document. Idently closely monitors CA/Browser Forum ballots and updates to the Requirements and implements updates to Idently operations in a timely manner. New or modified versions of this CP, the CPS, Subscriber Agreements, or Relying Party agreements are published within seven days after being digitally signed by the CPS Idently CA Governance Policy Authority using an Adobe AATL PDF signing Certificate with appropriate timestamp.

2.4 Access Controls on Repositories

Issuing CA shall make its Repository publicly available in a read-only manner and implement logical and physical controls to prevent unauthorized write access to such Repositories. In the case of Idently, the integrity and authenticity of its public documentation is maintained through the use of Digital Signatures applied to PDF documents.

3.0 Identification and Authentication

Issuing CAs maintain documented practices and procedures to authenticate the identity and/or other attributes of the Applicant.

Issuing CAs use approved procedures and criteria to accept applications from entities seeking to become part of the CAs hierarchy, either as Subordinate CA seeking chaining services or as an RA, Enterprise RA or as an end entity Subscriber.

Issuing CAs must authenticate the requests of parties wishing to perform revocation of Certificates under this CP.

3.1 Naming

3.1.1 Types of Names

To identify a Subscriber, Issuing CAs shall follow naming and identification rules that include types of names assigned to the Subject, such as X.500 distinguished names RFC-822 names and X.400 names. Where DNs (Distinguished Names) are used, CNs (Common Names) must respect name space uniqueness and must not be misleading. RFC2460 (IP version 6) or RFC791 (IP version 4) addresses may be used.

3.1.2 Need for Names to be Meaningful

When applicable, Issuing CAs shall use distinguished names to identify both the Subject and issuer name of the Certificate. When User Principal Names (UPN) are used, they must be unique and accurately reflect organizational structures.

3.1.3 Anonymity or Pseudonymity of Subscribers

Issuing CAs may issue end entity anonymous or pseudonymous Certificates provided that such Certificates are not prohibited by applicable policy and name space uniqueness is preserved.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished names in Certificates are interpreted using X.500 standards and ASN.1 syntax. See RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in Certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5 Uniqueness of Names

Issuing CAs may enforce uniqueness within the DN or by requiring that each Certificate include a unique non-sequential serial number with at least 20 bits of entropy.

3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers may not request Certificates with any content that infringes the intellectual property rights of another entity. This CP does not require that an Applicant’s right to use a trademark be verified. However, Issuing CAs may reject any applications or require revocation of any Certificate that is part of a dispute.

3.2 Initial Identity Validation

Issuing CAs may perform identification of the Applicant or for services including CA chaining services using any legal means of communication or investigation necessary to identify the Legal Entity or Individual.

Issuing CAs may use the result of a successful Subject DN initial identity validation process to create alternative product offerings by effectively combining elements of previously verified information with alternative, newly verified, information. A suitable account based challenge response mechanism must be used to authenticate any previously verified information for any returning Applicant provided that the re-verification requirements of Section 3.3.1 are complied with.

3.2.1 Method to Prove Possession of Private Key

No stipulation

3.2.2 Authentication of Organization Identity

For all Certificates that include an organization identity, Applicants are required to indicate the organization's name and registered or trading address. The legal existence, legal name, legal form (where included in the request or part of the legal name in the jurisdiction of incorporation) and provided address of the organization must be verified and any methods used must be highlighted in the CPS.

The authority of the Applicant to request a Certificate on behalf of the organization must be verified in accordance with Section 3.2.5.

3.2.2.1 Local Registration Authority Authentication

For accounts that allow the concept of a Local Registration Authority, Issuing CAs and RAs may set authenticated organizational details in the form of a *Profile.* Suitably authenticated account administrators acting in the capacity of a Local Registration Authority must authenticate Individuals affiliated with the organization and/or any sub-domains owned or controlled by the organization. (Whilst LRA's are able to authenticate Individuals under contract, all Domain Names to be authenticated must have previously had the appropriate higher-level Domain Name pre-authorized and authenticated in compliance with this CP and the Baseline Requirements).

3.2.2.2 Machine, Device, Department, and Role based Certificate Authentication

Issuing CAs must ensure that requests for machine, device, department, or role-based Certificates are authenticated either by a RA, acting on behalf of the CA, or an LRA that is contractually obligated to the Issuing CA/RA to ensure that machine, device, department, or role-based names relating to the organization and its business are accurate and correct.

3.2.3 Authentication of Individual identity

Issuing CAs or RAs shall authenticate Individuals depending upon the class of Certificate as indicated below.

3.2.3.1 Class 2

The Applicant is required to demonstrate control of certain identity attributes included in the request, such as his/her email address or domain name to which the Certificate relates if included in the Certificate Request.

The Applicant may also be required to submit a legible copy of a valid government issued national identity document or photo ID (driver's license, military ID or equivalent). A suitable non-government issued identity document or photo ID may also be required for additional proof. Idently verifies to a reasonable level of assurance that the copy of the ID matches the requested name and that other Subject information such as Country and/or state and locality fields are correct.

Idently may also authenticate the Applicant's identity through one of the following methods:

1. Performing a telephone challenge/response to the Applicant using a telephone number from a reliable source; or
2. Performing a fax challenge/response to the Applicant using a fax number from a reliable source; or
3. Performing an email challenge/response to the Applicant using an email address from a reliable source; or
4. Performing a postal challenge to the Applicant using an address obtained from a reliable source; or
5. The Applicant's seal impression (in jurisdictions that permit their use to legally sign a document) is included with any application received in writing.

For AATL, the options are defined as follows. Please note that these options are also available for other Class 2 products:

1. Receiving an attestation from an appropriate notary or Trusted Third Party that they have verified the individual identity based on a Governmentally Accepted Form of ID.
2. In the case of individuals affiliated with an organization: obtaining an executed declaration of identity of the individual that includes at least one unique biometric identifier of the individual (such as a fingerprint or handwritten signature). In this executed declaration of identity, an authorized representative of the Organization mentioned in the certificate confirms having seen the individual, reviewed the individual's photo ID, and confirm that the individual's identity information in the certificate requests matches the information contained in the reviewed photo ID. Idently confirms the document's authenticity directly with the authorized representative of the organization using contact information confirmed using a Qualified Independent Information Source or a Qualified Government Information Source or any other method.
3. In the case of individuals affiliated with an organization, Idently may rely on attestations from the approved Local RA. Refer to 3.2.3.3 in case of a Class 2 Certificate requested through an EPKI or an MSSL profile.
4. Receiving an attestation from an organization to validate the identities of its own end customers based on a verification of a Governmentally Accepted Form of ID, while the organization maintains a secure auditable trail of these verifications.
5. Other verifications in line with the verification of individuals for Qualified Certificates.

Idently may request further information from the Applicant. Other information and/or methods may be utilized in order to demonstrate an equivalent level of confidence.

If an email address is to be included in the Certificate Request, Idently or LRA shall verify the validity and ownership of that email address

.

3.2.3.2 Class 3

The Applicant is required to submit a legible copy of a valid government issued national identity document or photo ID (drivers licence, military ID or equivalent). A suitable non-government issued identity document or photo ID may also be required for additional proof. Issuing CAs are required to verify to a reasonable level of assurance that the copy of the ID matches the requested name and that other Subject information such as Country and/or state and locality fields are authenticated.

Issuing CA or RAs are also required to authenticate the Applicant's authority to represent the organization wishing to be named as the Subject in the Certificate, using reliable means of communication, verified by Idently as a reliable way of communicating with the Applicant.

Further information may be requested from the Applicant or the Applicant's organization. Other information and/or methods may be utilized in order to achieve an equivalent level of confidence.

3.2.3.3 Local Registration Authority Authentication

For pre-vetted Organization accounts that allow the concept of a Local Registration Authority, Issuing CAs and RAs may set authenticated organizational details in the form of a *Profile.* Certificates issued within these accounts are populated with data fields from the profile. Suitably authenticated account administrators acting in the capacity of a Local Registration Authority must authenticate individuals affiliated with the organization.

3.2.4 Non-Verified Subscriber Information

Issuing CAs must validate all information to be included within the Subject DN of a Certificate or clearly indicate within their CPS and within the issued Certificate itself any exceptions that may apply to specific product types or services offered. Issuing CAs may use the Subject:organizationalUnitName as a suitable location to identify non-verified Subscriber information to Relying Parties or to provide any specific disclaimers/notices. In the case of individuals, a unique identifier such as mobile number may be used in conjunction with the individual's legal name.

- For all Certificate types where the Issuing CA can explicitly identify a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity the Issuing CA must verify the information and may therefore omit a disclaimer notice.
- For all Certificate types where the Issuing CA cannot explicitly verify the identity, e.g. a generic term such as "Marketing," then the Issuing CA may omit the disclaimer that this item is classified as non-verified Subscriber information as described herein.

3.2.5 Validation of Authority

Personal Certificates	Verification that the Applicant has control over the email address to be listed within the Certificate through a challenge response mechanism.
Professional Certificates	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over any email address included. For Certificates issued through an EPKI account, the Authority of the Local Registration Authority will be verified at the time of the setup of the profile.
Organization Certificates	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over any email address included. For Certificates issued through an EPKI account, the Authority of the Local Registration Authority will be verified at the time of the set-up of the profile.
S/MIME certificates	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over any email address included.

Timestamping Certificates	Verification through a reliable means of communication with the organization's Applicant.
AATL and CDS	Verification through a reliable means of communication with the organization or individual Applicant together with verification that the Applicant has control over the email address if an email address is requested to be included in the Certificate. For Certificates issued through an EPKI account, the Authority of the Local Registration Authority will be verified at the time of the setup of the profile.
Dedicated Issuing CA	Verification through a reliable means of communication with the organization's Applicant and verification of all elements included within 'Name Constraints' which may include top level e-mail domain/sub domain names or domain names as detailed in section 3.2.6.

Alternative to any reliable means of communication with the organization, the authority can be confirmed using either:

- an advanced electronic signature (or higher) or seal which includes the name of the organization, its parent, subsidiary or affiliate, or
- an advanced electronic signature (or higher) of a confirmed employee or agent of the organization.

3.2.6 Criteria for Interoperation

As per 2.1.

3.2.7 Authentication of Domain Name

For all SSL Certificates, the Applicant's ownership or control of all requested Domain Name(s) and IP address must be verified with methods to achieve this in accordance with the Baseline Requirements section 3.2.2.4 and must be detailed within the CPS.

Further information may be requested from the Applicant, and other information and/or methods may be utilized to achieve an equivalent level of confidence.

3.2.8 Authentication of Email addresses

Idently must uses the following methods to confirm that the Applicant has control of or right to use email addresses:

1. Having the Applicant demonstrate control over the requested email address by sending a Random Value to the requested email address and then receiving a confirming response utilizing the Random Value; or
2. Having the Applicant demonstrate control over or right to use the FQDN using one of the Domain Validation processes listed in Section 3.2.7.1 of the Idently Certification Practice Statement. Once verified, an Enterprise RA can issue certificates containing email addresses under that FQDN.
3. The RA enters into a contractual agreement with the entity requesting the End Entity certificate to be signed according to the requirements in the applicable certificate policy.

3.3 Identification and Authentication for Re-key Requests

Issuing CAs may support re-key requests from Subscribers prior to the expiry of the Subscriber's existing Certificate. Issuing CAs may also support re-issue at any time during the lifetime of the Certificate.

3.3.1 Identification and Authentication for Routine Re-key

- **Personal Certificates** Username and password required with re-verification every 9 years.
- **Professional Certificates** Username and password required with re-verification every 9 years or client authentication with a current unexpired and unrevoked Certificate.
- **Organization Certificates** Username and password required with re-verification every 6 years.
- **Timestamping Certificates** Not supported.
- **CA for AATL Certificates** Username and password required with re-verification every 6 years.
- **PDF Signing for Adobe CDS** Not supported
- **Dedicated Issuing CA** Not supported
- **S/MIME Certificates** Username and password required with re-verification every 6 years.

3.3.2 Identification and Authentication for Reissuance after Revocation

After a Certificate has been revoked, the Subscriber is required to go through the initial registration process described elsewhere in this CP to obtain a new Certificate.
After a Certificate has been revoked, the Subscriber is required to request a new certificate and will be subject to an initial validation as specified in section 3.2.

3.3.3 Re-verification and Revalidation of Identity When Certificate Information Changes

If at any point any Subject name information embodied in a Certificate is changed in any way, the identity proofing procedures outlined in this requirement must be re-performed and a new Certificate issued with the validated information.

Issuer CAs must not re-key a Certificate without additional authentication if doing so would allow the Subscriber to use the Certificate beyond the limits described above.

3.3.4 Identification and Authentication for Re-key After Revocation

A routine re-key after revocation is not supported. Re-key after revocation of a Certificate requires the Subscriber to follow the initial validation process that was previously completed to allow the initial issuance of the Certificate.

3.4 Identification and Authentication for Revocation Request

All revocation requests must be authenticated by the Issuing CA. Revocation requests from Subscribers may be granted following a suitable challenge response such as logging into an account with a username and password, or proving possession of unique elements incorporated into the Certificate, e.g. Domain Name or email address.

Issuing CAs may also perform revocation on behalf of Subscribers in accordance with the requirements of the applicable Subscriber Agreement. Examples of reasons for revocation include a breach of the Subscriber Agreement or non- payment of applicable fees.

4.0 Certificate Life Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Issuing CAs shall maintain their own blocklists for individuals from whom or entities from which they will not accept Certificate applications. Blocklists may be based on historic certificates issued or other sources. In addition, other external sources such as government denied lists or internationally recognized denied persons lists which are applicable to the jurisdictions in which the Issuing CA operates may be used to screen unwanted Applicants.

4.1.2 Enrolment Process and Responsibilities

Issuing CAs shall maintain systems and processes that sufficiently authenticate the Applicant's identify for all Certificate types that present the identity to Relying Parties. Applicants should submit sufficient information to allow Issuing CAs and RAs to successfully perform the required verification. Issuing CAs and RAs shall protect communications and securely store information presented by the Applicant during the application process.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

Issuing CAs shall maintain systems and processes to sufficiently authenticate the Applicant's identify in in compliance with its CPS. Initial identity validation shall be performed by an Issuing CAs validation team or by Registration Authorities under contract as set forth in Section 3.2 of this CP. All communications shall be securely stored along with all information presented directly by the Applicant during the application process. Future identification of repeat Applicants and subsequent authentication checks may be addressed using single (username and password) or multi-factor (Certificate in combination with username/password) authentication principles.

Idently shall validate each server FQDN in publicly trusted SSL Certificates against the domain's CAA records. Idently's CAA issuer domain is "Idently.com." If a CAA record exists that does not list Idently.com as an authorized CA, Idently shall not issue the certificate.

4.2.2 Approval or Rejection of Certificate Applications

Issuing CAs shall reject applications for Certificates where validation of all items cannot successfully be completed.
Assuming all validation steps can be completed successfully following appropriate best practice techniques Issuing CAs shall generally approve the Certificate Request. Issuing CAs may reject applications including for the following reasons:

- Based on potential brand damage to Idently in accepting the application.
- For Certificates from Applicants who have previously been rejected or have previously violated a provision of a Subscriber Agreement.

Issuing CAs are under no obligation to provide a reason to an Applicant for rejection of a Certificate Request.

Issuing CA shall not issue publicly trusted SSL Certificates to internal server name or reserved IP addresses.

4.2.3 Time to Process Certificate Applications

Issuing CAs shall ensure that all reasonable methods are used in order to process and evaluate Certificate applications.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Certificate issuance by Idently Root CA requires an authorized Trusted Role member from Idently to deliberately issue a direct command for the Root CA to perform a Certificate signing operation.

Issuing CAs shall communicate with any RA accounts capable of causing Certificate issuance using multi-factor authentication. RAs directly operated by the Issuing CA or RAs contracted by the Issuing CA to perform validation shall ensure that all information sent to the CA is verified and authenticated in a secure manner.

4.3.2 Notifications to Subscriber by the CA of Issuance of Certificate

The Issuing CA shall notify the Subscriber of the issuance of a Certificate in a convenient and appropriate way based on information submitted during the enrolment process.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Issuing CAs shall inform the Subscriber that s/he may not use the Certificate until the Subscriber has reviewed and verified the accuracy of the data incorporated into the Certificate. To avoid this being an open-ended stipulation, Issuing CAs may set a time limit by when the Certificate is deemed to be accepted.

4.4.2 Publication of the Certificate by the CA

Issuing CAs may publish a Certificate by sending the Certificate to the Subscriber and/or publishing in a suitable Repository, including to Certificate Transparency Logs.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

RAs, local RA, partners/resellers, Idently and other entities may be informed of the issuance if they were involved in the initial enrolment.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

All Subscribers must protect their Private Key taking care to avoid disclosure to third parties. Issuing CAs must maintain a suitable Subscriber Agreement which highlights the obligations of the Subscriber with respect to Private Key protection. Private Keys must only be used as specified in the appropriate key usage and extended key usage fields as indicated in the corresponding Certificate. Where it is possible to make a back-up of a Private Key, Subscribers must use the same level of care and protection attributed to the live Private Key. At the end of the useful life of a Private Key, Subscribers must securely delete the Private Key and any fragments that it has been split into for the purposes of backup.

In the case of Idently's Digital Signing Service, and with the consent of the Subscriber, Idently shall host, secure, and manage short-lived Certificates and their corresponding Private Keys.

4.5.2 Relying Party Public Key and Certificate Usage

Issuing CAs must describe the conditions under which Certificates may be relied upon by Relying Parties within their CPS including the appropriate mechanisms available to verify Certificate validity (e.g. CRL or OCSP). Issuing CAs must also offer a Relying Party agreement to Subscribers the content of which should be presented to the Relying Party. Relying Party must accept and act in

accordance with the Relying Party Agreement prior to reliance upon a Certificate from the Issuing CA. Relying Parties should use the information to make a risk assessment and as such are solely responsible for performing the risk assessment prior to relying on the Certificate or any assurances made.

Software used by Relying Parties should be fully compliant with X.509 standards including best practice for chaining decisions around policies and key usage.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

Certificate renewal is defined as the production of a new Certificate that has the same details as a previously issued Certificate and the same Public Key. Issuing CAs that support renewal must identify the products and services under which renewals can be accepted. An Issuing CA may renew a Certificate so long as:

- The original Certificate to be renewed has not been revoked;
- The Public Key from the original Certificate has not been blocklisted for any reason; and
- All details within the Certificate remain accurate and no new or additional validation is required.

Issuing CAs may renew Certificates which have either been previously renewed or previously rekeyed (subject to the points above). The original Certificate may be revoked after renewal is complete; however, the original Certificate must not be further renewed, re-keyed or modified.

4.6.2 Who May Request Renewal

An Issuing CA may accept a renewal request provided that it is authorized by the original Subscriber through a suitable Certificate lifecycle account challenge response. A Certificate signing request is not mandatory, however if one is used then it must contain the same Public Key.

4.6.3 Processing Certificate Renewal Requests

An Issuing CA may request additional information before processing a renewal request.

4.6.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As per 4.4.1

4.6.6 Publication of the Renewal Certificate by the CA

As per 4.4.2

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

Certificate re-key is the process in which a subscriber can obtain a new certificate to replace an old certificate that:

- Contains the same information (identity, domains etc.) as the old certificate,
- Has the same expiry date (notAfter date) as the old certificate,
- Contains a different public key as the old certificate.

If a Certificate is re-keyed prior to the 'Not After' date, and the new certificate is given the same 'Not After' date as the old certificate, this process is referred to as Certificate re-issue.

Issuing CAs that support re-keying must identify the products and services under which re-keys can be accepted. An Issuing CA may re-key a Certificate as long as:

- The original Certificate to be re-keyed has not been revoked;
- The new public key has not been blocklisted for any reason; and
- All details within the Certificate remain accurate and no new or additional validation is required.

Issuing CAs may re-key Certificates which have either been previously renewed or previously rekeyed (subject to the points above). The original Certificate may be revoked after re-key is complete; however, the original Certificate must not be further renewed, re-keyed or modified.

4.7.2 Who May Request Certification of a New Public Key

An Issuing CA may accept a re-key request provided that it is authorized by either the original Subscriber, or an organization administrator who retains responsibility for the Private Key on behalf of a Subscriber through a suitable Certificate lifecycle account challenge response. A Certificate signing request is mandatory with any new Public Key.

4.7.3 Processing Certificate Re-Keying Requests

An Issuing CA may request additional information before processing a re-key or re-issue request and may re-validate the Subscriber subject to re-verification of any previously validated data. In the case of a reissuance, authentication through a suitable challenge response mechanism is acceptable.

4.7.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per 4.4.1

4.7.6 Publication of the Re-Keyed Certificate by the CA

As per 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification

Certificate modification is defined as the production of a new Certificate that has details which differ from a previously issued Certificate. The new modified Certificate may or may not have a new Public Key and may or may not have a new 'Not After' date.

- Issuing CAs shall treat modification in the same was a 'New' issuance.
- Issuing CAs may modify Certificates that have either been previously renewed or previously re-keyed. The original Certificate may be revoked after modification is complete, however, the original Certificate must not be further renewed, re-keyed or modified.

4.8.2 Who May Request Certificate Modification

As per 4.1

4.8.3 Processing Certificate Modification Requests

As per 4.2

4.8.4 Notification of New Certificate Issuance to Subscriber

As per 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate

As per 4.4.1

4.8.6 Publication of the Modified Certificate by the CA

As per 4.4.2

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

Certificate revocation is a process whereby the serial number of a Certificate is effectively blocklisted by adding the serial number and the date of the revocation to a Certificate Revocation List (CRL). The CRL itself will then be digitally signed with the same Private Key which originally signed the Certificate to be revoked. Adding a serial number to the CRL allows Relying Parties to establish that the lifecycle of a Certificate has ended. Issuing CAs may remove serial numbers once a Certificate has normally expired to promote more efficient CRL file size management, except for CodeSigning certificates (10 years after expiry). Prior to performing a revocation, Issuing CAs will verify the authenticity of the revocation request.

Idently may revoke any Certificate at its sole discretion.

Revocation of a Subscriber Certificate is performed within twenty-four (24) hours under the following circumstances:

1. The Subscriber requests in writing (to Idently which provided the Certificate) that they wish to revoke the Certificate;

2. The Subscriber notifies Idently that the original Certificate Request was not authorized and does not retroactively grant authorization;
3. Idently obtains reasonable evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;
4. Idently is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys);
5. Idently obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

Revocation of a Subscriber's Certificate should be performed within twenty-four (24) hours and is performed within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements for algorithm type and key size of the Baseline Requirements, as specified in Sections 6.1.5 and 6.1.6;
2. Idently obtains evidence that the Certificate was misused;
3. Idently receives notice or otherwise becomes aware that the Subscriber violated any of its material obligations under the Subscriber Agreement or Terms of Use;
4. Idently is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
5. Idently is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
6. Idently receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
7. Idently is made aware that the Certificate was not issued in accordance with the Baseline Requirements or Idently's CP or CPS;
8. Idently determines that any of the information appearing in the Certificate is not accurate or is misleading;
9. Idently's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless Idently has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by Idently's CP and/or CPS;
11. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/B Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time);
12. Idently receives notice or otherwise becomes aware of any circumstance indicating that use of the email address in the certificate is no longer legally permitted;
13. the CA private key used in issuing the certificate is suspected to have been compromised;
14. Idently ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;

Revocation of a Subscriber Certificate may also be performed within a commercially reasonable period of time under the following circumstances:

1. The Subscriber or organization administrator requests revocation of the Certificate through a idCC account which controls the lifecycle of the Certificate;
2. The Subscriber requests revocation through an authenticated request to Idently's support team or Idently's Registration Authority;
3. Idently receives notice or otherwise becomes aware that the Subscriber has been added as a denied party or prohibited person to a blocklist, or is operating from a prohibited destination under the laws of Idently's jurisdiction of operation;
4. Following the request for cancellation of a Certificate;
5. If a Certificate has been re-issued, Idently may revoke the previously issued

Certificate;

6. Under certain licensing arrangements, Idently may revoke Certificates following expiration or termination of the license agreement; and
7. Idently determines the continued use of the Certificate is otherwise harmful to the business of Idently or third parties. When considering whether Certificate usage is harmful to a third party's business or reputation, Idently will consider, amongst other things, the nature and number of complaints received, the identity of the complainant(s), relevant legislation in force, responses to the alleged harmful use by the Subscriber; If Microsoft, in its sole discretion, identifies a certificate whose usage or attributes are determined to be contrary to the objectives of the Dedicated Issuing CA Program, Microsoft will notify Idently and request that it revoke the certificate. Idently will either revoke the certificate or request an exception from Microsoft within 24 hours of receiving Microsoft's notice. Microsoft will review submitted material and inform Idently of its final decision to grant or deny the exception at its sole discretion. In the event that Microsoft does not grant the exception, Idently will revoke the certificate within 24 hours of the exception being denied.
8. Death of a Subscriber.

Revocation of a Subordinate CA Certificate is performed within seven (7) days under the following circumstances:

1. The Subordinate CA requests in writing to the Idently entity which provided the Subordinate CA Certificate or the authority detailed in Section 1.5.2 of this CP, that Idently revoke the Certificate;
2. The Subscriber notifies the Issuing CA that the original Certificate Request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains reasonable evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements for algorithm type and key size of the Baseline Requirements as specified in Sections 6.1.5 and 6.1.6;
4. Idently obtains evidence that the Certificate was misused;
5. Idently is made aware that the Certificate was not issued in accordance with or that the Subordinate CA has not complied with the Baseline Requirements or applicable CP or CPS;
6. Idently determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under the Baseline Requirements expires or is revoked or terminated, unless the issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Revocation is required by the Issuing CA's CP and/or CPS;
10. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/B Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

Issuing CAs that cross sign other Issuing CAs may revoke the Issuing CA if the cross signed Issuing CA no longer meets the contractual terms and conditions of the agreement between the two parties.

4.9.2 Who Can Request Revocation

Issuing CAs and RAs will accept authenticated requests for revocation. Authorization for revocation shall be accepted if the revocation request is received from either the Subscriber or an affiliated organization named in the Certificate. Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports to notify Idently of a suspected

reasonable cause to revoke a Certificate. Issuing CAs may also at their own discretion revoke Certificates including Certificates that are issued to other cross signed Issuing CAs.

4.9.3 Procedure for Revocation Request

Due to the nature of revocation requests and the need for efficiency, Issuing CAs and RAs may provide automated mechanisms for requesting and authenticating revocation requests; for example, through an account which issued the Certificate that is requested to be revoked. RAs may also provide manual backup processes in the event that automated revocation methods are not possible.

Issuing CAs and RAs will record each request for revocation and authenticate the source, taking appropriate action to revoke the Certificate if the request is authentic and approved.

Once revoked, the serial number of the Certificate and the date and time shall be added to the appropriate CRL. CRL reason codes may be included. CRLs may be published immediately or they may be published as defined within the Issuing CA's CPS.

Issuing CAs and RAs shall prepare methods for Subscribers, Relying Parties, Application Software Suppliers, and other third parties to submit a Certificate Problem Report. Issuing CAs and RAs may or may not revoke in response to this request. See section 4.9.5 for detail of actions required for Issuing CAs and RAs for making this decision.

4.9.4 Revocation Request Grace Period

For all other certificates, the revocation request grace period is the time available for a Subscriber to take any necessary actions themselves in order to request revocation of a suspected Key Compromise, use of a weak key or discovery of inaccurate information within an issued Certificate. Issuing CAs should allow Subscribers a maximum of 48 hours to take appropriate action to revoke or take appropriate action on behalf of Subscribers.

4.9.5 Time Within Which CA Must Process the Revocation Request

Issuing CAs shall begin investigating Certificate Problem Reports within twenty-four (24) hours of receipt of the report.

All revocation requests for end entity Certificates, both those generated automatically via user accounts and those initiated by the Issuing CA itself, must be processed within a maximum of 30 minutes of receipt.

Issuing CAs that cross sign other CAs should process a revocation request within 24 hours of a confirmation of Compromise and an ARL should be published within 12 hours of any off-line ARL key ceremony.

Issuing CAs and RAs shall maintain 24 x 7 ability to respond internally to a high-priority Certificate Problem Report through report abuse channel and, where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint. Issuing CAs and RAs shall begin investigation procedures for a suspected Key Compromise or misuse of a Certificate within 24 hours of receipt of the report.

Issuing CAs and RAs shall decide whether revocation or other action is warranted based on at least following criteria:

- The nature of the alleged problem;
- The number of reports received about a particular Certificate or Subscriber;
- The entity making the complaint; and
- Relevant legislation.

4.9.6 Revocation Checking Requirements for Relying Parties

Prior to relying on a Certificate, Relying Parties must validate the suitability of the Certificate to the purpose intended and ensure the Certificate is valid. Relying Parties will need to consult CRL or OCSP information for each Certificate in the chain as well as validating that the Certificate chain itself is complete. This may include the validation of Authority Key Identifier (AKI) and Subject Key Identifier (SKI). Issuing CAs may include all applicable URLs within the Certificate to aid Relying Parties in performing the revocation checking process.

4.9.7 CRL Issuance Frequency

All Issuing CAs must meet the requirements of the Baseline Requirements and the EV Guidelines (if applicable).

For the status of Subscriber Certificates:
If the CA publishes a CRL, then the CA SHALL update and re-issue CRLs at least once every seven days, and the value of the nextUpdate field MUST NOT be more than ten days beyond the value of the thisUpdate field.

For the status of Subordinate CA Certificates:
If the Subordinate CA contains a CDP, the CA SHALL update and re-issue CRLs at least (i) once every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field MUST NOT be more than twelve months beyond the value of the thisUpdate field.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the repository within a commercially reasonable time after generation.

4.9.9 On-Line Revocation/Status Checking Availability

Issuing CAs that support OCSP responses in addition to CRLs shall provide response times no longer than 10 seconds under normal network operating conditions.

Issuing CAs' OCSP responses shall conforms to RFC6960 and/or RFC5019. OCSP responses shall be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. OCSP signing Certificate must contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 On-Line Revocation Checking Requirements

OCSP responders operated by the CA SHALL support the HTTP GET method, as described in RFC 6960 and/or RFC 5019.

The validity interval of an OCSP response is the difference in time between the thisUpdate and nextUpdate field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

For the status of Subscriber Certificates:

1. OCSP responses MUST have a validity interval greater than or equal to eight hours.
2. OCSP responses MUST have a validity interval less than or equal to ten days.
3. For OCSP responses with validity intervals less than sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate.

4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then the CA SHALL update the information provided via an Online Certificate Status Protocol at least eight hours prior to the nextUpdate, and no later than four days after the thisUpdate.

For the status of Subordinate CA Certificates:

- The CA shall update information provided via an OCSP Responder (i) at least every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate.

OCSP Responders that receive a request for status of a Certificate that has not been issued, shall not respond with a "good" status for such Certificates. OCSP Responders for CAs which are not Technically Constrained, in line with Section 7.1.5, shall not respond with a "good" status for such Certificates.

Issuing CA shall require OCSP requests to contain the following data:

- Protocol version
- Service request
- Target Certificate identifier

4.9.11 Other Forms of Revocation Advertisements Available

If the Subscriber Certificate is for a high-traffic FQDN, Issuing CA may choose to rely on stapling, in accordance with RFC4366, to distribute its OCSP responses. In this case, Issuing CA shall ensure that the Subscriber “staples” the OCSP response for the Certificate in its TLS handshake. Issuing CA shall enforce this requirement on the Subscriber contractually through the Subscriber Agreement or Terms of Use, or by technical review measures implemented by the CA.

4.9.12 Special Requirements Related to Key Compromise

Issuing CAs and related Registration Authorities shall use commercially reasonable methods to inform Subscribers that their Private Key may have been Compromised. This includes cases where new vulnerabilities have been discovered or where the Issuing CA at their own discretion decides that evidence suggests a possible Key Compromise has taken place. Where Key Compromise is not disputed Issuing CAs shall revoke Issuing CA Certificates or Subscriber end entity Certificates and publish a revised CRL within 24 hours.

4.9.13 Circumstances for Suspension

Certificate suspension is only allowed for Client certificates. Certificate suspension is not allowed for any other types of end entity Certificates. Certificate suspension is strictly forbidden for SSL Certificates.

4.9.14 Who Can Request Suspension

Issuing CAs and RAs shall accept authenticated requests for suspension. Authorization for suspension shall be accepted if the suspension request is received from either the Subscriber or an affiliated organization named in the Certificate. Issuing CAs may also at their own discretion suspend Certificates including Certificates that are issued to other cross signed Issuing CAs.

4.9.15 Procedure for Suspension Request

Due to the nature of suspension requests and the need for efficiency, Issuing CAs and RAs may provide automated mechanisms for requesting and authenticating suspension requests; for example, through an account which issued the Certificate that is requested to be suspended. RAs may also provide manual backup processes in the event that automated suspension methods are not possible. Issuing CAs and RAs will record each request for suspension and authenticate the source, taking appropriate action to suspend the Certificate if the request is authentic and approved.

Once suspended, the serial number of the Certificate and the date and time shall be added to the appropriate CRL. CRL reason code “on hold” will be included. CRLs may be published immediately or they may be published as defined within the Issuing CA’s CPS.

4.9.16 Limits on Suspension Period

There are no limits on the Certificate suspension period.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Issuing CAs shall provide a Certificate status service either in the form of a CRL distribution point or an OCSP responder or both. For Code Signing Certificates and Qualified Certificates that include a cRLDistributionPoints extension, Issuing CAs shall not remove revocation entries on CRL or OCSP until 10 years after the Expiry Date of the revoked Certificate. For other Certificate types, Issuing CAs shall not remove revocation entries on CRL or OCSP until after the Expiry Date of the revoked Certificate.

4.10.2 Service Availability

Issuing CAs shall maintain 24x7 availability of Certificate status services and may choose to use additional content distribution network cloud based mechanisms to aid service availability. Issuing CAs shall maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 Operational Features

No stipulation

4.11 End of Subscription

Subscribers may end their subscription to Certificate services by having their Certificate revoked or naturally letting it expire. Where Issuing CAs have issued Issuing CAs capable of end entity issuance contracts between parties must be maintained unless revocation is used to terminate the contract.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

CA Private Keys are never escrowed. An Issuing CA that offers key escrow services to Subscribers may escrow Subscriber Private Keys. Any Private Keys that are escrowed must be held in at least the same level of security as when the Key Pair was originally created.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation

5.0 Facility, Management, and Operational Controls

5.1 Physical Controls

Issuing CAs shall have 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 should be implemented to avoid loss, damage or Compromise of assets and interruption to business activities and theft of information and information processing facilities.

5.1.1 Site Location and Construction

Issuing CAs shall ensure that critical and sensitive information processing facilities are housed in secure areas with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage and interference, and the protections provided should be commensurate with the identified risks in risk analysis plans.

5.1.2 Physical Access

Issuing CAs shall ensure that the facilities used for Certificate life cycle management are operated in an environment that physically protects the services from Compromise through unauthorized access to systems or data. An authorized employee should always accompany any unauthorized person entering a physically secured area. Physical protections should be achieved through the creation of clearly defined security perimeters (i.e. physical barriers) around the systems hosting the CA operations. No parts of the CA premises shall be shared with other organizations within this perimeter.

5.1.3 Power and Air Conditioning

Issuing CAs should ensure that the power and air conditioning facilities are sufficient to support the operation of the CA system.

5.1.4 Water Exposures

Issuing CAs should ensure that the CA system is protected from water exposure.

5.1.5 Fire Prevention and Protection

Issuing CAs should ensure that the CA system is protected with a fire suppression system.

5.1.6 Media Storage

Issuing CAs should ensure that any media used is securely handled to protect it from damage, theft and unauthorized access. Media management procedures should be protected against obsolescence and deterioration of the media within a defined period of time. Records are required to be retained. All media should be handled securely in accordance with requirements of the information asset classification scheme and media containing sensitive data must be securely disposed of when no longer required.

5.1.7 Waste Disposal

Issuing CAs should ensure that all media used for the storage of information is declassified or destroyed in a generally accepted manner before being released for disposal.

5.1.8 Off-Site Backup

Issuing CAs should ensure that full system backups of the Certificate issuance system are sufficient to recover from system failures and are made periodically, as defined in the Issuing CA's CPS. Back-up copies of essential business information and software must be taken regularly. Adequate back-up facilities must be provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans. At least one full backup copy must be stored at an offsite location (at a location separate from the Certificate issuance equipment). Backups should be stored at a site with physical and procedural controls commensurate to that of the operational facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Issuing CAs should ensure that all operators and administrators including Validation Specialists 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 CA system.

Idently may subscribe certificates for Idently affiliate companies, or persons identified in association with these companies (as a subject). Idently affiliate companies includes Idently's parent and subsidiary companies, as well and other companies that share a same parent company as Idently.

Trusted roles include but are not limited to the following:

- **Developers:** Responsible for development of CA systems.
- **Security Manager:** overall responsibility for administering the implementation of the CA's security practices, cryptographic key life cycle management functions (e.g., key component custodians);
- **Administrator:** approval of the generation, revocation and suspension of certificates;
- **System Engineer:** installation, configuration and maintenance of the CA systems, viewing and maintenance of CA system archives and audit logs;
- **Operator:** day-to-day operation of CA systems and system backup and recovery;
- **Key Manager:** cryptographic key life cycle management functions (e.g., key component custodians).

5.2.2 Number of Persons Required per Task

Issuing CAs shall state the number of persons required per task within their CPS. The goal is to guarantee the trust for all CA services (Key Pair generation, Certificate generation, and revocation) so that any malicious activity would require collusion. Where multiparty control is required, at least one of the participants shall be an Administrator. All participants shall serve in a trusted role as defined in Section 5.2.1 above.

5.2.3 Identification and Authentication for Each Role

Before appointing a person to a trusted role, Issuing CAs shall run 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 CA. The CPS should describe the mechanisms that are used to identify and authenticate people appointed to trusted roles.

5.2.4 Roles Requiring Separation of Duties

Issuing CAs shall enforce role separation either by the CA equipment or procedurally or by both means.

Individual CA personnel are specifically designated to the roles defined in Section 5.2.1 above

Roles requiring a separation of duties include:

- Those performing approval of the generation, revocation, and suspension of certificates. (Validation Specialists)
- Those performing installation, configuration, and maintenance of the CA systems. (Infra system engineer)
- Those with overall responsibility for administering the implementation of the CA's security practices. (Security Officer)
- Those performing duties related to cryptographic key life cycle management (e.g., key component custodians). (CA activation data holders)
- Those performing CA systems development. (Developers)
- Those performing CA systems auditing (Infra Operator, Auditor)

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor, Issuing CA shall verify the identity and trustworthiness of such person.

Issuing CAs shall employ a sufficient number of personnel that possess the expert knowledge, experience and qualifications necessary for the offered services, as appropriate to the job function. Issuing CA personnel should fulfil the requirement of *expert knowledge, experience and qualifications* through formal training and education, actual experience, or a combination of the two. Trusted roles and responsibilities, as specified in the Issuing CA's CPS, are documented in job descriptions. Issuing CA personnel (both temporary and permanent) have job descriptions defined from the view point of separation of duties and least privilege, determining position sensitivity based on the duties and access levels, background screening and employee training and awareness. Issuing CA personnel shall be formally appointed to trusted roles.

5.3.2 Background Check Procedures

All Issuing CA personnel in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the CA operations. The Issuing CA shall not appoint to a trusted role any person who is known to have a conviction for a serious crime or another offence, is 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 analysed, 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.

Any use of information revealed by background checks by the Issuing CA shall be in compliance with applicable laws of jurisdiction where the person is employed.

5.3.3 Training Requirements

Issuing CA shall provide all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common

threats to the information verification process (including phishing and other social engineering tactics), and the Baseline Requirements.

Issuing CA maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

Issuing CA documents that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

Issuing CA requires all Validation Specialists to pass an examination provided by the CA on the information verification requirements outlined in the Baseline Requirements.

5.3.4 Retraining Frequency and Requirements

All personnel in Trusted Roles shall maintain skill levels consistent with Idently's training and performance programs.

Any significant change to the operations shall have a training (awareness) plan with at least annual training on information security, and the execution of such plan shall be documented.

5.3.5 Job Rotation Frequency and Sequence

Issuing CAs should ensure that any change in the staff will not affect the operational effectiveness of the service or the security of the system.

5.3.6 Sanctions for Unauthorized Actions

Appropriate disciplinary sanctions shall be applied to personnel violating provisions and policies within the CP, CPS or CA related operational procedures.

5.3.7 Independent Contractor Requirements

Contractor personnel employed for Issuing CA operations must be subjected to the same process, procedures, assessment, security control and training as permanent CA personnel.

5.3.8 Documentation Supplied to Personnel

Issuing CA should make 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.

Documentation is maintained identifying all personnel who received training and the level of training completed.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit log files shall be generated for all events relating to the security and services of the Issuing CA. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

Issuing CA shall record details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. Issuing CA shall make these records available to its Qualified Auditor as proof of the CA's compliance with associated CA audit scheme stipulated in introduction.

Issuing CA shall record at least the following events:

CA certificate and key lifecycle events, including:

- Key generation, backup, storage, recovery, archival, and destruction;
- Certificate requests, renewal, and re-key requests, and revocation;
- Approval and rejection of certificate requests;
- Cryptographic device life cycle management events; and
- Generation of Certificate Revocation Lists and OCSP entries;
- Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.

Subscriber Certificate life cycle management events, including:

- Certificate requests, renewal, and re-key requests, and revocation;
- All verification activities stipulated in this CP;
- Approval and rejection of Certificate Requests;
- Issuance of Certificates; and
- Generation of Certificate Revocation Lists and OCSP entries.

Security events, including:

- Successful and unsuccessful PKI system access attempts;
- PKI and security system actions performed;
- Security profile changes;
- Installation, update and removal of software on a Certificate System;
- System crashes, hardware failures, and other anomalies;
- Firewall and router activities; and
- Entries to and exits from the CA facility.

Log entries includes the following elements;

1. Date and time of entry;
2. Identity of the person making the journal entry; and
3. Description of the entry.

5.4.2 Frequency of Processing Log

Audit logs should be reviewed periodically for any evidence of malicious activity and following each important operation.

5.4.3 Retention Period for Audit Log

Issuing CA shall retain any audit logs generated for at least ten years. Issuing CA shall make these audit logs available to Qualified Auditor upon request.

5.4.4 Protection of Audit Log

The events must be logged in a way that they cannot be deleted or destroyed (except for transfer to long term media) for any period of time that they are retained.

The events must be logged in a manner to ensure that only individuals with authorized trusted access are able to perform any operations regarding their profile without modifying integrity, authenticity and confidentiality of the data.

The records of events must be protected in a manner to prevent alteration and detect tampering.

The records of events must be date stamped in a secure manner that guarantees, from the date of creation of the record to the end of the archive period that there is a trusted link between the event and the time of its realisation.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries must be backed-up in a secure location (for example, a fire proof safe), under the control of an authorized trusted role, and separated from their component source generation. Audit log backup should be protected to the same degree as originals.

5.4.6 Audit Collection System

The audit log collection systems may be an internal component. Audit processes must be initiated at system start up and may finish only at system shutdown. The audit collection system should ensure the integrity and availability of the data collected. If necessary, the audit collection system should protect the data confidentiality. In the case of a problem occurring during the process of the audit collection the Issuing CAs must determine whether to suspend Issuing CA operations until the problem is solved, duly informing the impacted asset owners.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Issuing CA shall perform annual risk assessments that:

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 Process;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the Issuing CA has in place to counter such threats.

Issuing CA shall also perform regular vulnerability assessment and penetration testing covering all CA assets related to Certificate issuance, products and services. Assessments focus on internal and external threats that could result in unauthorized access, tampering, modification, alteration or destruction of the Certificate issuance process.

5.5 Records Archival

5.5.1 Types of Records Archived

Issuing CAs and RAs archive records with enough detail to establish the validity of a signature and of the proper operation of the CA system.

5.5.2 Retention Period for Archive

Issuing CA shall retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least the retention period defined by the WebTrust and/or Kenya Electronic and Digital Signature Laws for the Certificate type.

5.5.3 Protection of Archive

The archives should be created in such a way that they cannot be deleted or destroyed (except for transfer to long term media) within the period of time for which they are required to be held. Archive protections should ensure that only authorized trusted access is able to make operations without modifying integrity, authenticity and confidentiality of the data. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site.

5.5.4 Archive Backup Procedures

Archive backups are made which are either of the online Idently system or the offline system.

5.5.5 Requirements for Timestamping of Records

If a timestamping service is used to date the records, it must comply with the requirements defined in Section 6.8. Irrespective of timestamping methods, all logs must have must have data indicating the time at which the event occurred.

5.5.6 Archive Collection System (Internal or External)

The archive collection system complies with the security requirements defined in Section 5.3.

5.5.7 Procedures to Obtain and Verify Archive Information

Media storing of Issuing CA archive information are checked upon creation. Periodically, statistical samples of archived information are tested to check the continued integrity and readability of the information.

Only authorized Issuing CA equipment, trusted role and other authorized persons are allowed to access the archive.

5.6 Key Changeover

Issuing CAs may periodically changeover Key material for Issuing CAs in accordance with Section 6.3.2. Certificate Subject information may be modified and Certificate profiles may be altered to adhere to new best practices. Private Keys used to sign previous Subscriber Certificates shall be maintained until such time as all Subscriber Certificates have expired.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Issuing CAs shall establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing resources, software and/or data that could disturb or Compromise the Issuing CA services. Issuing CAs should carry out risk assessments to evaluate business risk and determine the necessary security requirements and operational procedures to be taken as a consequence of its disaster recovery plan. This risk analysis is regularly reviewed and revised if necessary *(threat evolution, vulnerability evolution, etc.).* This business continuity is included in the scope of the audit process as described in Section 8 to validate which operations should be first restored after a disaster and the recovery plan.
Issuing CA personnel that serve in a trusted role and operational role should be specially trained to operate according to procedures defined in the disaster recovery plan for business critical operations.

If an Issuing CA detects a potential hacking attempt or another form of Compromise, it should perform an investigation in order to determine the nature and the degree of damage. Otherwise, the Issuing CA should assess the scope of potential damage in order to determine if the CA or RA system needs to be rebuilt, if only some Certificates need to be revoked, and/or if a CA hierarchy needs to be declared as Compromised. The CA disaster recovery plan should highlight which services should be maintained *(for example, revocation and Certificate status information)*

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

If any equipment is damaged or rendered inoperative, but the Private Keys are not destroyed, the operation should be re-established as quickly as possible, giving priority to the ability to generate Certificate status information according to the Issuing CA's disaster recovery plan.

5.7.3 Issuing CA Private Key Compromise Procedures

In the event an Issuing CA Private Key is Compromised, lost, destroyed, or suspected to be Compromised:

- The Issuing CA shall, after investigation of the problem, decide whether the Issuing CA Certificate should be revoked. If so, then:
  - All the Subscribers who have been issued a Certificate will be notified at the earliest feasible opportunity; and
  - A new Issuing CA Key Pair shall be generated, or an alternative existing CA hierarchy shall be used to create new Subscriber Certificates

5.7.4 Business Continuity Capabilities After a Disaster

The disaster recovery plan deals with the business continuity as described in Section 5.7.1. Certificate status information systems should be deployed so as to provide 24 hours per day, 365 days per year availability.

5.8 CA or RA Termination

When it is necessary to terminate an Issuing CA or RA activities, the impact of the termination must be minimized as much as possible in light of the prevailing circumstances and is subject to the applicable Issuing CA and/or Registration Authority Agreements. Issuing CAs must specify the procedures they will follow when terminating all or a portion of their Digital Certificate issuance and management operations. The procedures must, at a minimum:

- ensure that any disruption caused by the termination of an Issuing CA is minimised as much as possible;
- ensure that archived records of the Issuing CA are retained;
- ensure that prompt notification of termination is provided to Subscribers, Authorised Relying Parties, Application Software Providers, and other relevant stakeholders in Idently certificate lifecycles;
- ensure Certificate status information services are provided and maintained for the applicable period after termination, including, if applicable, transferring Certificate status information services to another GMO Internet Group entity;
- ensure that a process for revoking all Digital Certificates issued by an Issuing CA at the time of termination is maintained;
- notify all auditors; and
- notify other relevant Government and Certification bodies under applicable laws and related regulations

5.8.1 Successor Issuing Certification Authority

To the extent that it is practical and reasonable, the successor Issuing CA should assume the same rights, obligations, and duties as the terminating Issuing CA.

6.0 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

For Root CA Key Pairs, Idently shall performs following controls;

1. prepares and follows a Key Generation Script,
2. has a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process, and
3. has a Qualified Auditor issue a report opining that Idently followed its key ceremony script during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

In other CA Key Pairs, issuing CA shall performs following controls;

1. Generates the keys in a physically secured environment as described in Section 5.1 and 5.2.2. of Certificate Policy and/or Certification Practice Statement;
2. Generates the CA keys using personnel in trusted roles under the principles of multiple person control and split knowledge;
3. Generate the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's Certificate Policy and/or Certification Practice Statement;
4. Log its CA key generation activities; and
5. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certificate Policy and/or Certification Practice Statement and (if applicable) its Key Generation Script.

For Subscriber keys generated by issuing CA, Key generation must be performed in a secure cryptographic device that meets FIPS 140-2 using key generation algorithm and key size as specified in Section 6.1.5 and 6.1.6.

Issuing CA shall also reject a certificate request if it has a known weak Private Key.

Issuing CAs shall generate all issuing Key Pairs in a physically secure environment by personnel in trusted roles under, at least, dual control. External witnesses (Ideally an independent auditor who normally performs audits on a regular basis) should be present or the ceremony, as a whole, must be videotaped/recorded. Issuing CA key generation is carried out within a device which is at least certified to FIPS 140-2 level 3 or above.

Subscriber key generation by Idently is performed in a secure cryptographic device meeting FIPS 140-2 using key generation algorithm and key size as specified in Section 6.1.5 and 6.1.6.

6.1.2 Private Key Delivery to Subscriber

Issuing CAs that create Private Keys on behalf of Subscribers may do so only when sufficient security is maintained within the key generation process and any onward issuance process to the Subscriber. The cryptographic algorithms regarding Public/Private key generation (encryption, sign, cryptographic hash, RNG or PRNG etc.) were approved by FIPS, the Public/Private key generation algorithm is also specified in FIPS 186-4.

The generated Public/Private key is encrypted with PIN code which was provided by the Subscriber. The encrypted Public/Private key will be delivered in TLS session, authenticated by the password pre-registered by an administrator of the Subscriber.

As of March 1, 2018, Idently does not generate private keys for publicly trusted SSL Certificates.

6.1.3 Public Key Delivery to Certificate Issuer

Issuing CAs shall only accept Public Keys from RAs that have been protected during transit and have had the authenticity and integrity of their origin from the RA suitably verified. RA's shall only accept Public Keys from Subscribers in accordance with Section 3.2.1 of this CP.

6.1.4 CA Public Key Delivery to Relying Parties

Issuing CAs shall ensure that Public Key delivery to Relying Parties is undertaken in such a way as to prevent substitution attacks. This may include working with commercial browsers and platform operators to embed Root Certificate Public Keys into root stores and operating systems. Issuing CA Public Keys may be delivered by the Subscriber in the form of a chain of Certificates or via a Repository operated by the Issuing CA and referenced within the profile of the issued Certificate.

6.1.5 Key Sizes

Idently follows NIST Special Publication 800-133 Revision 2 (2020) - Recommendation for Cryptographic Key Generation - for recommended timelines and best practices in the choice of Key Pairs for Root CAs, Issuing CAs and end entity Certificates delivered to Subscribers. Any Subordinate CAs in the Dedicated Issuing CA program, outside of the direct control of Idently are contractually obligated to use the same best practices.

Idently selects from the following Key Sizes/Hashes for Root Certificates, Issuing CA Certificates, and end entity Certificates as well as CRL/OCSP Certificate status responders. These choices align with the Baseline Requirements and EV Guidelines:
SSL Certificates must meet Baseline Requirements Section 6.1.5 on algorithm type and key size.

6.1.6 Public Key Parameters Generation and Quality Checking

Issuing CAs shall generate Key Pairs in accordance with FIPS 186 and shall use reasonable techniques to validate the suitability of Public Keys presented by Subscribers. Known weak keys shall be tested for and rejected at the point of submission. Issuing CAs shall reference Baseline Requirements Section 6.1.6 on quality checking.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

Issuing CAs shall set key usage of Certificates depending on their proposed field of application via the v3 Key Usage Field for X.509 v3 (See Section 7.1).

Private Keys corresponding to Root Certificates shall not be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for OCSP Response verification.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Issuing CAs shall implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA Private Key outside the validated system or device specified above must consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the CA Private Key. Issuing CAs shall encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic Module Standards and Controls

Issuing CAs shall ensure that all systems signing Certificates and CRLs or generating OCSP responses use FIPS 140-2 level 3 as the minimum level of cryptographic protection. Issuing CAs that require Subscribers to use FIPS 140-2 level 2 or above systems for Private Key protection must contractually obligate the Subscriber to use such a system or provide a suitable mechanism to guarantee protection. This can be achieved, for example, through limitation to a suitable CSP (Cryptographic Service Provider) tied to a known FIPS compliant hardware platform as part of the enrolment process.

6.2.2 Private Key (n out of m) Multi-Person Control

Issuing CAs shall activate Private Keys for cryptographic operations with multi-person control (using CA activation data) performing duties associated with their trusted roles. The trusted roles permitted to participate in this Private Key multi-person controls are strongly authenticated (i.e. token with PIN code).

6.2.3 Private Key Escrow

Issuing CAs shall not escrow CA Private Keys for any reason.

6.2.4 Private Key Backup

Issuing CAs shall back up Private Keys under the same multi-person control as the original Private Key for disaster recovery plan purposes.

6.2.5 Private Key Archival

Issuing CAs shall not archive Private Keys and must ensure that any temporary location where a Private Key may have existed in any memory location during the generation process is purged.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Issuing CA Private Keys must be generated, activated, and stored in Hardware Security Modules. When Private Keys are outside of a Hardware Security Module (either for storage or transfer), they must be encrypted. Private Keys must never exist in plain text outside of a cryptographic module. If Idently becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the Idently shall revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7 Private Key Storage on Cryptographic Module

Issuing CAs shall store Private Keys on at least a FIPS 140-2 level 3 device.

6.2.8 Method of Activating Private Key

Issuing CAs are responsible for activating the Private Key in accordance with the instructions and documentation provided by the manufacturer of the hardware security module. Subscribers are responsible for protecting Private Keys in accordance with the obligations that are presented in the form of a Subscriber Agreement or Terms of Use.

6.2.9 Method of Deactivating Private Key

Issuing CAs shall ensure that Hardware Security Modules that have been activated are not left unattended or otherwise available to unauthorized access. During the time, an Issuing CA's

Hardware Security Module is on-line and operational it is only used to sign Certificates and CRL/OCSPs from an authenticated RA. When a CA is no longer operational, its Private Keys are removed from the Hardware Security Module.

6.2.10 Method of Destroying Private Key

Issuing CA Private Keys must be destroyed when they are no longer needed or when the Certificate to which they correspond have expired or are revoked. Destroying Private Keys requires Issuing CAs to destroy all associated CA secret activation data in the HSM in such a manner that no information can be used to deduce any part of the Private Key.

Private Keys generated by Idently are stored in idCC in PKCS#12 format until the Key Pairs are picked up by the Subscriber. When the Subscriber acknowledge the receipt of the Key Pair or when 30 days has passed after the key generation, the Subscriber Key Pair is automatically deleted from idCC.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Issuing CAs must archive Public Keys from Certificates.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Publicly Trusted Issuing CA Certificates and renewed Certificates shall have a maximum validity period of:

Type	Private Key Usage	Max Validity Period
Root Certificates	No stipulation	27 years
TPM Root Certificates	30 years	40 years
Publicly Trusted Sub-CAs/Issuer CAs	No stipulation	17 years
Dedicated Issuing CA	No stipulation	10 years
Personal/Professional/Organization Certificates	No stipulation	39 months
AATL End Entity Certificates	No stipulation	39 months
Timestamping Certificates	15 months	11 years
PDF Signing for Adobe CDS Certificates	No stipulation	39 months
Private Key Archival\Key Recovery Agent Certificates	No stipulation	5 years

Key pair usage period can have up to the same Validity Period as certificate Validity Period.

Certificates signed by a specific CA must expire before the end of that Key Pair's operational period.

Issuing CAs must comply with the Baseline Requirements with respect to the maximum validity period, in some cases thereby reducing the effective available Certificate term. In some cases, the maximum validity period may not be realized by the Subscriber in the event the current or future Baseline Requirements impose requirements on Certification Authorities relative to Certificate issuance that were not in place at the time the Certificate was originally issued, particularly in the case of a request for reissuance, e.g., additional requirements are included for identification and authentication for certain Certificate type, or maximum Validity Period is decreased.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Generation and use of Issuing CA activation data used to activate Issuing CA Private Keys shall be made during a key ceremony (Refer to Section 6.1.1). Activation data shall be generated automatically by the appropriate HSM and delivered to a shareholder who must be a person in trusted role. The delivery method must maintain the confidentiality and the integrity of the activation data.

6.4.2 Activation Data Protection

Issuing CA activation data must be protected from disclosure through a combination of cryptographic and physical access control mechanisms. Issuing CA activation data must be stored on smart cards.

6.4.3 Other Aspects of Activation Data

Issuing CA activation data must only be held by Issuing CA personnel in trusted roles.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions must be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The Issuing CA PKI components must include the following functions:

- Require authenticated logins for trusted role;
- Provide discretionary access control with least privilege;
- Provide security audit capability (protected in integrity);
- Prohibit object re-use;
- Require use of strong password policy;
- Require use of cryptography for session communication;
- Require trusted path for identification and authentication;
- Provide means for malicious code protection;
- Provide means to maintain software and firmware integrity;
- Provide domain isolation and partitioning different systems and processes; and
- Provide self-protection for the operating system.

For accounts capable of directly causing certificate issuance, Issuing CA shall enforce multifactor authentication.

6.5.2 Computer Security Rating

No Stipulation

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system development controls for the Issuing CA are as follows:

- Use software that has been designed and developed under a formal, documented development methodology;
- Hardware and software procured are purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase);

- Hardware and software are developed in a controlled environment, and the development processes are defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software;
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location;
- The hardware and software are dedicated to performing CA activities. There are no other applications, hardware devices, network connections, or component software installed which are not part of the CA operation;
- Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required to perform the CA operations are installed on the equipment and are obtained from sources authorized by local policy. Issuing CA hardware and software are scanned for malicious code on first use and periodically thereafter; and
- Hardware and software updates are purchased or developed in the same manner as original equipment; and are installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the Issuing CA system as well as any modifications and upgrades are documented and controlled by the Issuing CA management. There is a mechanism for detecting unauthorized modification to the Issuing CA software or configuration. A formal configuration management methodology is used for installation and on-going maintenance of the Issuing CA system. The Issuing CA software, when first loaded, is checked as being that supplied from the vendor, with no modifications, and is the version intended for use.

6.6.3 Life Cycle Security Controls

Issuing CA monitors the maintenance scheme requirements in order to maintain the level of trust of software and hardware that are evaluated and certified.

6.7 Network Security Controls

Issuing CA PKI components implement appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures include the use of security guards, firewalls, and filtering routers. Unused network ports and services are turned off. Any boundary control devices used to protect the network on which PKI equipment are hosted deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 Timestamping

All Issuing CA components are regularly synchronized with a time service such as an atomic clock or Network Time Protocol (NTP) service. A dedicated authority, such as a timestamping authority, may be used to provide this trusted time. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a CA Certificate;
- Revocation of a CA Certificate;
- Posting of CRL updates; and
- Issuance of Subscriber end entity Certificates.

Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events.

7.0 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Version Number(s)

Issuing CAs shall issue Certificates in compliance with X.509 Version 3.

7.1.2 Certificate Extensions

Issuing CAs shall issue Certificates in compliance with RFC 5280 and applicable best practice including compliance to the current Baseline Requirements sections 7.2.1.1 through 7.2.1.5. Criticality shall also follow best practice and where possible prevent unnecessary risks to Relying Parties when applied to name constraints.

7.1.3 Algorithm Object Identifiers

Issuing CAs shall issue Certificates with algorithms indicated by the following OIDs

SHA1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 5}
SHA256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
SHA384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 12}
SHA512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 13}

ECDSAWithSHA256	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 2}
ECDSAWithSHA384	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3}
ECDSAWithSHA512	{iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 4}
RSASSA-PSS	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsassa-pss(10)}

7.1.4 Name Forms

Issuing CAs shall issue Certificates with name forms compliant to RFC 5280 and section 7.1.4 of the Baseline Requirements.

7.1.5 Name Constraints

Issuing CAs may issue Subordinate CA Certificates with name constraints and mark as critical where necessary. When name constraints are NOT set on a Subordinate CA, such CA must be subject for full audit specified in section 8.0 of this document.

Idently may issue Subordinate CA Certificates with name constraints where necessary and mark as critical where necessary as part of the Dedicated Issuing CA program.

7.1.6 Certificate Policy Object Identifier

Idently follows Section 7.1.6 of Baseline Requirements.

7.1.7 Usage of Policy Constraints Extension

No stipulation

7.1.8 Policy Qualifiers Syntax and Semantics

Issuing CAs may issue Certificates with a policy qualifier to aid Relying Parties in determining applicability.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation

7.1.10 Serial Numbers

Each Issuing CA must issue certificates that include a unique (within the context of the Issuer Subject DN and CA certificate serial number) non-sequential Certificate serial number greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.2 CRL Profile

7.2.1 Version Number(s)

Issuing CAs shall issue Version 2 CRLs in compliance with RFC 5280.

7.2.2 CRL and CRL Entry Extensions

CRLs have the following extensions:CRL Number and Authority Key Identifier

7.3 OCSP Profile

Issuer CAs may operate an Online Certificate Status Profile (OCSP) responder in compliance with RFC 6960 or RFC 5019.

7.3.1 Version Number(s)

Issuing CAs shall issue Version 1 OCSP responses.

7.3.2 OCSP Extensions

No stipulation

8.0 Compliance Audit and Other Assessments

The policies within this CP encompass relevant portions of currently applicable PKI standards for the various vertical PKI industries in which Issuing CAs are required to operate.standards listed in Section 1.0.

8.1 Frequency and Circumstances of Assessment

Idently maintains its compliance with the WebTrus standards identified in Section 1.0 via a Qualified Auditor on an annual (WebTrust) and contiguous basis.

Dedicated Issuing CA CAs that are not constrained by dNSNameConstraints are audited for compliance to the applicable WebTrust standards.

8.2 Identity/Qualifications of Assessor

Applicable audits of Issuing CAs shall be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme such as stipulated in section 8.0 of this document;
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- Certified, accredited, licensed, or otherwise assessed as meeting the qualification requirements of auditors under the audit scheme;
- Bound by law, government regulation, or professional code of ethics; and
- Except in the case of an internal government auditing agency, maintains professional liability/errors & omissions insurance with policy limits of at least one million US dollars ($1,000,000) in coverage.

8.3 Assessor’s Relationship to Assessed Entity

Issuing CAs must choose an auditor/assessor who is completely independent from the Issuing CA.

8.4 Topics Covered by Assessment

The audit must meet the requirements of the audit scheme under which the assessment is being made. These requirements may vary as audit schemes are updated. An audit scheme will be applicable to the Issuing CA in the year following the adoption of the updated scheme.

8.5 Actions Taken as a Result of Deficiency

Issuing CAs, including cross signed Issuing CAs that are not technically constrained, must follow the same process if presented with a material non-compliance by external auditors and must create a suitable corrective action plan to remove the deficiency.

8.6 Communications of Results

Results of the audit must be reported to the Idently Policy Authority for analysis and resolution of any deficiency through a subsequent corrective action plan. The results could also be made available to any other appropriate entities that may be entitled to a copy of the results by law, regulation, or agreement. Copies of Idently's WebTrust for CAs audit reports can be found at: https://www.idently.com/repository.

8.7 Self-Audit

Issuing CA shall monitor its adherence to this Certificate Policy, Issuing CA's Certification Practice Statement and other external requirements specified in the "*Acknowledgements*" section and strictly control its service quality by performing self-audits on at least a quarterly basis against randomly selected samples of at least 3 percent of the Certificates issued.

9.0 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Issuing CAs may charge fees for Certificate issuance or renewal. Issuing CAs may also charge for re-issuance or re-key. Fees and any associated terms and conditions should be made clear to Applicants.

9.1.2 Certificate Access Fees

Issuing CAs may charge for access to any database which stores issued Certificates.

9.1.3 Revocation or Status Information Access Fees

Issuing CAs 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 Issuing CAs Certificate status infrastructure.

9.1.4 Fees for Other Services

Issuing CAs may charge for other additional services such as timestamping.

9.1.5 Refund Policy

Issuing CAs may offer a refund policy to Subscribers. Subscribers who choose to invoke the refund policy should have all issued Certificates revoked.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Idently maintains commercial general liability insurance with policy limits of at least one million US dollars ($1,000,000) in coverage and Errors and Omissions / Professional Liability insurance with a policy limit of at least one million US dollars ($1,000,000) in coverage. Idently's insurance policies include coverage for (1) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (2) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, patent, and trademark infringement), invasion of privacy, and advertising injury.

9.2.2 Other Assets

No stipulation

9.2.3 Insurance or Warranty Coverage for End Entities

Issuer CAs may offer a warranty policy to Subscribers.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Issuing CAs shall define the scope of confidential information within its CPS.

9.3.2 Information Not Within the Scope of Confidential Information

Any information not defined as confidential within the CPS shall be deemed public. Certificate status information and Certificates themselves are deemed public.

9.3.3 Responsibility to Protect Confidential Information

Issuing CAs shall protect confidential information. Issuing CAs shall enforce protection of confidential information through training and contracts with employees, agents, and contractors.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Issuing CAs shall protect personal information in accordance with a privacy policy published on a suitable Repository along with this CP.

9.4.2 Information Treated as Private

Issuing CAs shall treat all information received from Applicants that will not ordinarily be placed into a Certificate as private. This applies both to those Applicants who are successful in being issued a Certificate and those who are unsuccessful and rejected. Issuing CAs should periodically train all RA and vetting staff as well as anyone who has access to the information about due care and attention that must be applied.

9.4.3 Information Not Deemed Private

Certificate status information and any Certificate content is deemed not private.

9.4.4 Responsibility to Protect Private Information

Issuing CAs are responsible for securely storing private information in accordance with a published privacy policy document and may store information received in either paper or digital form. Any backup of private information must be encrypted when transferred to suitable backup media.

9.4.5 Notice and Consent to Use Private Information

Personal information obtained from Applicants during the application and enrolment process is deemed private and permission is required from the Applicant to allow the use of such information. Issuing CAs should incorporate the relevant provisions within an appropriate Subscriber Agreement including any additional information obtained from third parties that may be applicable to the validation process for the product or service being offered by the Issuing CA.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Issuing CAs may disclose private information without notice to Applicants or Subscribers where required to do so by law or regulation.

9.4.7 Other Information Disclosure Circumstances

No Stipulation.

9.5 Intellectual Property Rights

Issuing CAs shall not knowingly violate the intellectual property rights of third parties. Public and Private Keys remain the property of Subscribers who legitimately hold them. Issuing CAs retain ownership of Certificates however, they shall grant permission to reproduce and distribute Certificates on a non-exclusive, royalty free basis, provided that they are reproduced and distributed in full.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Issuing CAs use this CP and applicable Subscriber Agreements to convey legal conditions of usage of issued Certificates to Subscribers and Relying Parties. Participants that may make representations and warranties include Idently, RAs, Subscribers, Relying Parties, and any other participants as it might become necessary. All parties including the Issuing CA, any RAs and Subscribers warrant the integrity of their respective Private Key(s). If any such party suspects that a Private Key has been compromised they will immediately notify the appropriate RA.

Issuing CA represents and warrants to Certificate Beneficiaries, during the period when the Certificate is valid, Issuing CA has complied with its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate:

- **Right to Use Domain Name or IP Address:** That, at the time of issuance, Issuing CA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's Subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in Issuing CA's Certificate Policy and/or Certification Practice Statement (see Section 3.2);
- **Authorization for Certificate:** That, at the time of issuance, Issuing CA (i) operated a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in Issuing CA's Certificate Policy and/or Certification Practice Statement (see Section 3.2.5);
- **Accuracy of Information:** That, at the time of issuance, Issuing CA (i) operated a procedure for verifying all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute) was true and accurate; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in Issuing CA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.2, 3.2.3, 3.2.4);
- **No Misleading Information:** That, at the time of issuance, Issuing CA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in Issuing CA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.2, 3.2.3, 3.2.4);
- **Identity of Applicant:** That, if the Certificate contains Subject Identity Information, the CA (i) operated a procedure to verify the identity of the Applicant; (ii) followed the procedure when issuing and managing the Certificate; and (iii) accurately described the procedure in Issuing CA's Certificate Policy and/or Certification Practice Statement (see Sections 3.2.2, 3.2.3, 3.2.4);
- **Subscriber Agreement:** That, if Issuing CA and Subscriber are not Affiliates, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the Baseline Requirements or, if Issuing CA and Subscriber are Affiliates, the Applicant Representative acknowledged and accepted the Terms of Use (see Section 4.5.1);
- **Status:** The Issuing CA maintains a 24 x 7 publicly accessible Repository;
- **Revocation:** The Issuing CA will revoke the Certificate for any of the reasons specified in the Baseline Requirements (see Section 4.9.1);

9.6.2 RA Representations and Warranties

Issuing CAs require all RAs to warrant that they are in compliance with this CP and the relevant CPS and may choose to include additional representations within its CPS or RA agreement.

9.6.3 Subscriber Representations and Warranties

Subscribers and/or Applicants warrant that:

- **Accuracy of Information:** Subscriber will provide accurate and complete information at all times to Issuing CA, both in the Certificate Request and as otherwise requested by Issuing CA in connection with issuance of a Certificate;
- **Protection of Private Key:** Applicant shall take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key to be included in the requested Certificate(s) and any associated activation data or device, e.g. password or token;
- **Acceptance of Certificate:** Subscriber shall review and verify the Certificate contents for accuracy;
- **Use of Certificate:** Subscriber shall install an SSL Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
- **Reporting and Revocation:** Subscriber shall (a) promptly request revocation of the certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate; and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
- **Termination of Use of Certificate:** Subscriber shall promptly cease use of Private Key associated with the Public Key in the Certificate upon revocation of that Certificate;
- **Responsiveness:** Subscriber shall respond to Issuing CA's instructions concerning Compromise or Certificate misuse within forty-eight (48) hours; and
- **Acknowledgment and Acceptance:** Applicant acknowledges and accepts that Issuing CA is entitled to revoke the Certificate immediately if the Applicant violates the terms of the Subscriber Agreement or Terms of Use or if Issuing CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

9.6.4 Relying Party Representations and Warranties

A party relying on an Issuing CA's Certificate warrants to:

- Have the technical capability to use Certificates;
- Receive notice of the Issuing CA and associated conditions for Relying Parties;
- Validate an Issuing CA's Certificate by using Certificate status information (e.g. a CRL or OCSP) published by the issuing CA in accordance with the proper Certificate path validation procedure;
- Trust an Issuing CA's Certificate only if all information featured on such Certificate can be verified via such a validation procedure as being correct and up to date;
- Rely on an Issuing CA's Certificate, only as it may be reasonable under the circumstances; and
- Notify the appropriate RA immediately, if the Relying Party becomes aware of or suspects that a Private Key has been Compromised.

The obligations of the Relying Party, if it is to reasonably rely on a Certificate, are to:

- Verify the validity or revocation of the CA Certificate using current revocation status information as indicated to the Relying Party;

- Take account of any limitations on the usage of the Certificate indicated to the Relying Party either in the Certificate or this CP;
- Take any other precautions prescribed in the Issuing CA's Certificate as well as any other policies or terms and conditions made available in the application context a Certificate might be used.

Relying Parties must at all times establish that it is reasonable to rely on a Certificate under the circumstances taking into account circumstances such as the specific application context a Certificate is used in.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

Issuing CAs should make statements in their CPS that they do not warrant:

- The accuracy of any unverifiable piece of information contained in Certificates except as it may be stated in the relevant product description below in this CP and in a warranty policy, if available.
- The accuracy, authenticity, completeness, or fitness of any information contained in, free, test or demo Certificates.

9.8 Limitations of Liability

The total liability of the Issuing CA should be limited in accordance with any warranty policy and any limitations set forth in its CPS.

9.8.1 Exclusion of Certain Elements of Damages

Issuing CAs should make statements in their CPS to the effect that in no event (except for fraud or wilful misconduct) is the Issuing CA liable for:

- Any loss of profits;
- Any loss of data;
- Any indirect, consequential, or punitive damages arising from or in connection with the use, delivery, license, and performance or non-performance of Certificates or Digital Signatures;
- Any transactions or services offered or within the framework of this CP;
- Any other damages except for those due to reliance on the verified information in a Certificate, except for information featured on, free, test or demo Certificates; and
- Any liability incurred in any case if the error in such verified information is the result of fraud or wilful misconduct of the Applicant.

9.9 Indemnities

9.9.1 Indemnification by an Issuer CA

The Issuing CA's indemnification obligations must be set forth in its CPS, Subscriber Agreement, or Relying Party Agreement including any obligation to third party beneficiaries.

9.9.2 Indemnification by Subscribers

The Issuing CA shall include its indemnification requirements for Subscribers in the CPS and in its Subscriber Agreements.

9.9.3 Indemnification by Relying Parties

The Issuing CA shall include its indemnification requirements for Relying Parties in its CPS.

9.10 Term and Termination

9.10.1 Term

This CP remains in force until such time as communicated otherwise by Idently on its web site or Repository.

9.10.2 Termination

Notified changes are appropriately marked by an indicated version. Following publications, changes become applicable 30 days thereafter.

9.10.3 Effect of Termination and Survival

Issuing CAs should communicate the conditions and effect of this CP's termination via their appropriate Repository.

9.11 Individual Notices and Communications with Participants

Idently accepts notices related to this CP by means of digitally signed messages or in paper form. Upon receipt of a valid, digitally signed acknowledgment of receipt from Idently the sender of the notice deems its communication effective. The sender must receive such acknowledgment within twenty (20) business days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed as follows. Individuals communications made to Idently must be addressed to: legal@Idently.com or by post to Idently in the address provided in Section 1.4.2.

9.12 Amendments

9.12.1 Procedure for Amendment

This CP is reviewed at least annually and may be reviewed more frequently. All changes are reviewed and approved by the Idently CA Governance Policy Authority before insertion.

Changes to this CP are indicated by appropriate numbering.

9.12.2 Notification Mechanism and Period

Issuing CAs should post appropriate notice on their web sites of any major or significant changes to this CP as well as any appropriate period by when the revised CP is deemed to be accepted.

9.12.3 Circumstances Under Which OID Must be Changed

No stipulation

9.13 Dispute Resolution Procedures

Before resorting to any dispute resolution mechanism including adjudication or any type of alternative dispute resolution (including without exception mini-trial, arbitration, binding expert's

advice, co-operation monitoring and normal expert's advice) complaining parties agree to notify Idently of the dispute in an effort to seek dispute resolution.

Upon receipt of a dispute notice, Idently convenes a dispute committee that advises Idently management on how to proceed with the dispute. The dispute committee convenes within twenty (20) business days from receipt of a dispute notice. The dispute committee is composed by a counsel, a data protection officer, a member of Idently operational management and a security officer. The counsel or data protection officer chair the meeting. In its resolutions the dispute committee proposes a settlement to the Idently executive management. The Idently executive management may subsequently communicate the proposed settlement to the complaining party.

If the dispute is not resolved within twenty (20) business days after initial notice pursuant to CPS, parties submit the dispute to arbitration, in accordance with Kenya Law.

There will be three (3) arbitrators of whom each party proposes one while both parties of the dispute choose the third arbitrator. The place of the arbitration is Nairobi, Kenya and the arbitrators determine all associated costs.

9.14 Governing Law

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

Each party, including Idently partners, Subscribers and Relying Parties, irrevocably submit to the jurisdiction of the courts of Kenya.

9.15 Compliance with Applicable Law

Idently complies with applicable laws of Kenya. Export of certain types of software used in certain Idently public Certificate management products and services may require the approval of appropriate public or private authorities. Parties (including Idently, Subscribers and Relying Parties) agree to comply with applicable export laws and regulations as pertaining in Kenya.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

The Issuing CA will contractually obligate every RA involved with Certificate issuance to comply with this CP and all applicable Industry guidelines. No third party may rely on or bring action to enforce any such agreement.

9.16.2 Assignment

Entities operating under this CP must not assign their rights or obligations without the prior written consent of Idently.

9.16.3 Severability

If any provision of this CP, including limitation of liability clauses, is found to be invalid or unenforceable, the remainder of this CP will be interpreted in such manner as to affect the original intention of the parties.

Each and every provision of this CP that provides for a limitation of liability, is intended to be severable and independent of any other provision and is to be enforced as such.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

Idently may seek indemnification and attorneys' fees from a party for damages, losses and expenses related to that party's conduct. Idently's failure to enforce a provision of this CP does not waive Idently's right to enforce the same provisions later or right to enforce any other provisions of this CP. To be effective any waivers must be in writing and signed by Idently

9.16.5 Force Majeure

Idently 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 Idently'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

Third party Issuing CAs that want to subscribe to the Dedicated Issuing CA CA chaining service of Idently must adhere to this CP and all of its conditions. This adherence is implemented and verified through a number of legal and procedural controls and is verified through annual audits. Controls include, but are not limited to:

- Execution of a CA chaining agreement between the Dedicated Issuing CA Subscriber and Idently;
- Submission and publication of a CPS reviewed and acceptance by Idently and/or Idently auditors; and
- Submission of PKI infrastructure review by Dedicated Issuing CA Subscriber and acceptance by Idently and/or Idently auditors.

9.17.1 CA Chaining Agreement

The CA chaining Agreement includes the following terms and conditions:

- Use of Dedicated Issuing CA by Subscriber's enterprise and subsidiaries (50+% controlling interest) only;
- Non-commercial use only: Certificates issued are for own use, staff, and third parties affiliated with Subscriber for existing business use and processes only. Reselling is explicitly disallowed;
- Restriction of types of end entity Certificates: S/MIME, SSL client Certificates:
- Requirement of submission of CPS reviewed and accepted by Idently;
- Compliance with this CP;
- Submission of PKI Infrastructure review documenting physical, personnel, network, logical and operational controls in line with industry standards;
- Requirement of FIPS 140-2 level 3 or equivalent cryptographic modules for CA and Subordinate CA Private Key management;
- No cross-signing allowed;
- Enforcement of export controls for issued Certificates in compliance with US Export regulations;

- Acceptance of annual audits by Idently and/or Idently auditors;
- Ongoing requirement to notify Idently of material changes in CA environment as reported in the PKI infrastructure review and CPS; and
- Acceptance of Subscriber that Idently might publish Subscriber CA in a Idently repository.

If Idently and/or Idently auditors determine that the Dedicated Issuing CA Subscriber has breached the CA chaining agreement Idently may revoke the Subordinate CA Certificate.

9.17.2 PKI Infrastructure review

Execution of Dedicated Issuing CA Subscriber Agreement is subject to review and acceptance by Idently and/or Idently auditors of Subscriber PKI infrastructure review.
This review documents the Subscriber CA hierarchy and its security measures taken. It includes, but is not limited to, the following subjects:

- Logical security measures implemented – including personnel matters and separation of duty and dual control;
- Physical security measures implemented;
- Network security measures implemented;
- CA hierarchy implemented; and
- HSM type and serial numbers.

9.17.3 Subscriber CA implementation

Idently requires a mandatory test signing of a Subscriber CA with a Idently test CA. Idently test CA duplicates the Idently Root CA but it is identified as for testing purposes (CAT versus CA) and is not distributed to third party applications. Only after successful test signing is the Subscriber CA signed by Idently Root CA.

9.17.4 Ongoing requirements and audits

Subscriber must at all times adhere to its obligations. Subscriber has an ongoing duty to report to Idently and/or Idently auditors any changes previously reported in section. Idently will instruct its Qualified Auditors, as part of its own WebTrust for CA audit, to audit annually the requirements as stated above and will also obtain from an independent third-party offering web site scanning services a list of any publicly available domains to ensure compliance.