JuliCA, Certification Practice Statement V. 4

Version	Effective Date	Description of Changes	Author / Approved By
1.0	1 October 2021	Initial release of CP and CPS	TendaWorld Ltd / CA Team
2.0		Updates to align with internal policies and initial audit preparation	TendaWorld Ltd / CA Team
3.0	20 March 2025	Minor revisions and addition of embedded policies (Data Protection, Incident Response, Business Continuity and Disaster Recovery Plan.)	TendaWorld Ltd / CA Team
4.0	27 March 2026	Major update to fully align CP and CPS with RFC 3647 and Kenya E-CSP Compliance Audit Checklist · Strengthened Publication & Repository Responsibilities (Section 2) · Added detailed Certificate Revocation and Suspension procedures (Section 4.9) · Fixed all broken/malformed external links and removed template artifacts · Updated subscriber rights and privacy references	Christina Wanjiku Wood / Chris Daniels Ohabo/ Duncan Mang'are (Data Protection Officer & Managing Director/ Project Manager)

Contents

Contents

1. INTRODUCTION

1.1. Overview

The JuliCA Public Key Infrastructure ("JuliCA PKI"), has been established by Tendaworld Ltd to enable reliable and secure identity authentication, and to facilitate the preservation of confidentiality and integrity of data in electronic transactions. This document is issued by JuliCA to identify the practices and procedures that JuliCA employs in issuing certificates from its Certificate Authorities within the JuliCA PKI.

1.2. Document name and identification

This document is the JuliCA Certification Practice Statement ("CPS"). It has been published in response to JuliCA's Certificate Policy and sets forth the practices that JuliCA has adopted to implement the provisions made therein.

1.3. PKI participants

1.3.1. Certification authorities

The term Certification Authority (CA) is an umbrella term that refers to all entities authorized to issue, manage, revoke, and renew certificates. Moreover it can refer to the infrastructure and key material from which such an entity issues and signs certificates.

This CPS covers all certificates issued and signed by JuliCA.

1.3.2. Registration authorities

Registration Authorities (RAs) are entities that approve and authenticate requests to obtain, renew,or revoke Certificates. RAs are generally responsible for identifying and authenticating Applicants for Certificates, verifying their authorization to request Certificates, approving individuals, entities, and/or devices to be named in Certificates, and authorizing and/or requesting a CA to issue, renew,or revoke a Certificate to an individual, entity or device.

All RA functions for JuliCA listed in this CPS will be performed by JuliCA.

1.3.3. Subscribers

Subscribers use JuliCA certificates to support their transactions and communications.

A Subscriber is an individual or organization for whom JuliCA has issued a Certificate on the basisof a Certificate Application. JuliCA may allow Applicants to submit a Certificate Application through the product of a JuliCA Affiliate or directly through an appropriate API. OV certificates include the name of the Subscriber as part of the subject of the certificate.

All Subscribers are required to enter into an agreement that, with respect to each JuliCA Certificate issued to them as a Subscriber, obligates them to:

- Make true representation at all times to JuliCA regarding information in the Certificate and other identification and authentication information requested by JuliCA.
- Maintain possession and control of the Private Key corresponding to the Public Key in the Certificate at all times.
- Implement appropriate security measures to protect their Private Key corresponding to the Public Key included in the Certificate.
- Promptly inform JuliCA of a change to any information included in the Certificate or in the certificate application request.
- Promptly inform JuliCA of any suspected compromise of the Private Key.
- Immediately cease using the Certificate upon expiration of the Certificate, revocation of the Certificate, or in the event of any suspected compromise of the Private Key.
- Use Certificates exclusively for legal purposes and in accordance with this CPS. and in accordance with this CPS.

1.3.4. Relying parties

A Relying Party is any individual or entity that acts in reliance on a JuliCA Certificate to verify a digital signature and/or decrypt an encrypted document or message. Relying Parties may include JuliCA and JuliCA Affiliates, as well as unaffiliated individuals or entities.

1.3.5. Other participants

Not applicable.

1.4. Certificate usage

1.4.1. Appropriate certificate uses

Appropriate Certificate uses under this CPS are all uses for the purpose of authentication, using digital signatures, encryption and access control which are consistent with the key usage extension fields of the respective Certificate and are not in violation of the CP, this CPS, applicable law or any agreement made between the Subscriber and JuliCA.

1.4.2. Prohibited certificate uses

Certificates are not proof of the trustworthiness or honesty of the subscriber nor do they indicate the subscriber's compliance with any law. By issuing a certificate JuliCA merely confirms that it has used reasonable means to verify the information in the certificate before it was issued.

Certificates issued under this CPS are not intended and may not be used for any application requiring fail-safe performance such as (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage.

JuliCA certificates may not be used for man-in-the middle purposes or where usage is prohibited by law.

1.5. Policy administration

1.5.1. Organization administering the document

The JuliCA Policy Authority is responsible for the drafting, maintenance, and interpretation of this Certification Practice Statement.

1.5.2. Contact person

Tendaworld Ltd

Merchant square,
Riverside drive Nairobi,
Kenya

+254721138882

Chris Daniel Ohabo

For security issues, such as vulnerability reports or external reports of key compromise, please contact mail@tenda.world.

To notify JuliCA of a CA service outage or report a suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates, please contact mail@tenda.world

If you request a Certificate revocation, please add "Revocation request" and the domain name, IP address or certificate serial number into the subject line of your email.

1.5.3. Person determining CPS suitability for the policy

The Communications Authority of Kenya determines the suitability and applicability of this CPS.

1.5.4. CPS approval procedures

JuliCA may change this CPS as deemed necessary. Changes that in the judgment of JuliCAwill have no or only a minimal effect on Participants in the JuliCA PKI, may be made without notification. Changes, that in the judgment of JuliCA will have a significant impact on Participants in the JuliCA PKI, will be made with prior notice to such Participants.

A new version of the CPS will become effective fifteen (15) days after it has been published, and will supersede all previous versions and will be binding on all Participants in the JuliCA PKI from that point forward.

1.6. Definitions and acronyms

See appendix A.

1.6.1. Conventions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",

"SHOULD",
"SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in these Requirements SHALL be interpreted in accordance with RFC 2119.

2. PUBLICATION AND REPOSITORY RESPONSIBIL-ITIES

2.1. Repositories

JuliCA maintains a secure publicly accessible Repository which comprises its root certificates, its current CP and CPS, Subscriber Agreements, Relying Party Agreements, and the most recent revocation information for certificates it has issued.

Additionally JuliCA publishes all non-constrained Subordinate CA Certificates and all Cross Certificates it issues including a link to the CPS under which they were issued.

JuliCA represents that it will adhere to the latest version of the CP published in the Repository.

2.2. Publication of certification information

The following items are published in the repository:

• The Certificate Policy (CP) and Certification Practice Statement (CPS), including all versions and change history;

• CA certificates and subordinate CA certificates;

• Certificate Revocation Lists (CRL) and/or OCSP responses;

• Current version of the CP/CPS with change history.

2.3. Time or frequency of publication

The CP and CPS are published within 30 days of any material change and are promptly notified to the User Community.

CRLs are published at least every 24 hours (or more frequently if required).

Certificates are published immediately upon issuance.

2.4. Access controls on repositories

The Repository is publicly available. JuliCA operates physical and logical security controls to protect the repository from unauthorized modification or deletion.
The repository is read-only for the public, Subscribers, and Relying Parties. Write access is strictly restricted to authorised JULICA personnel and is subject to formal change management, dual control, and approval procedures.

Repository Location: https://repository.tendaworld.com
All documents are available under the "Legal & Policy Documents" section of the repository.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

3.1.1. Types of names

OV Certificates contain an X.501 distinguished name in the Subject name field, and incorporate the following attributes:

- Country (C)
- Organization (O)
- Organizational Unit (OU)
- State or Province (ST)
- Locality (L)
- Common Name (CN)

DV Certificates contain an X.501 distinguished name in the Subject name field, and incorporate the following optional attributes:

- Common Name (CN)

Both OV and DV certificates also incorporate the Subject Alternative Name (SAN) extension, which must contain the value of CN from the Subject (if present), and may contain other names that apply to the subject.

3.1.2. Need for names to be meaningful

Domain names included in the CN or SAN attributes must identify one or more specific hosts. JuliCA may issue wildcard Certificates, which identify a set of hosts, as well as Certificates which identify an IP Address.

3.1.3. Anonymity or pseudonymity of subscribers

Subscribers are not permitted to use pseudonyms.

3.1.4. Rules for interpreting various name forms

No stipulation.

3.1.5. Uniqueness of names

The CN attribute in root Certificates identifies the publisher and is unique.

3.1.6. Recognition, authentication, and role of trademarks

Certificate Applicants are prohibited from requesting certificates that contain content which infringes on the intellectual property and commercial rights of others. JuliCA does not determine whether Certificate Applicants have intellectual property rights in the name used in a Certificate Application nor does JuliCA resolve any dispute concerning the ownership of a domain name or

trademark. JuliCA may reject any Certificate Application and revoke any Certificate because of such a dispute.

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

The Certificate Applicant must prove ownership of the private key by providing a PKCS #10 compliant certificate signing request, or a cryptographically equivalent proof.

3.2.2. Authentication of organization and domain identity

3.2.2.1. Identity

For OV Certificates, the Applicant's identity and its address are validated by using one of the following:

1. A Government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation Letter.

3.2.2.2. DBA/Tradename

JuliCA does not include DBA/Tradenames into Certificates. OV Certificates include the company name of the Subscriber.

3.2.2.3. Verification of Country

See Section 3.2.2.1.

3.2.2.4. Validation of Domain Authorization or Control

Prior to issuing a Certificate, JuliCA validates that the Applicant has control over each FQDN listed in the Certificate by using at least one of the methods listed below.

3.2.2.4.6 Agreed-Upon Change to Website Confirming that a Random Value or Request Token is present at a well-known location at the Authorization Domain Name via HTTP/HTTPS over an Authorized Port.

3.2.2.4.7 DNS Change Confirming that a Random Value or Request Token generated by JuliCA is present either in a DNS CNAME, TXT or CAA record for the FQDN.

3.2.2.4.10 TLS Using a Random Number Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value within a Certificate on the Au- thorization Domain Name which is accessible by the CA via TLS over an Authorized Port.

Where the use of the methods listed above is not feasible, JuliCA may use the methods described in Sections 3.2.2.4.2, 3.2.2.4.3 BR as an alternative.

In addition, JuliCA may supplement its validation procedure with checks against internal data sources.

3.2.2.5. Authentication of an IP Address

IP address authentication is performed in accordance with the procedures set out in Subsections 2 and 3 of Section 3.2.2.5 BR.

For each IP Address listed in a Certificate, JuliCA confirms that, as of the date of Certificate issuance, the Applicant has control over the IP Address by:

1. Obtaining documentation of IP address assignment from the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC);or
2. Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name under Section 3.2.2.4 BR.

3.2.2.6. Wildcard Domain Validation

JuliCA has established and follows a documented procedure that determines if a wildcard character in a CN or subjectAltName of type DNS-ID occurs in the first label position to the left of a "reg- istry-controlled" label or "public suffix". If a wildcard falls within the label immediately to the left of a registry-controlled or public suffix, JuliCA refuses issuance unless the applicant proves its rightful control of the entire Domain Namespace.

3.2.2.7. Data Source Accuracy and Validity Periods

All data sources are evaluated for reliability, accuracy, and for their protection from alteration and falsification before they are used for I&A purposes.

Data sources are revalidated in accordance with the following terms.

- Legal existence and identity of Applicant - 825 days;
- Domain name - 825 days;
- Authority of Applicant - 825 days.

3.2.2.8. CAA Records

JuliCA's policy on checking CAA records is stated in Section 4.2.4.

3.2.3. Authentication of individual identity

JuliCA does not issue OV Certificates to natural persons.

3.2.4. Non-verified Subscriber Information

JuliCA does not verify the following subscriber information:

- Organizational Unit (OU);
- Organization-specific information not used for identification purposes;

- Other information designated as non-verified in the certificate.

3.2.5. Validation of Authority

JuliCA uses a reliable method of communication with the Applicant or its representative.

The authority of Certificate Applicants to request Certificates on behalf of an organization is verified during the validation of the Applicant's identity.

JuliCA may allow Applicants to specify in writing the individuals who may request Certificates on its behalf. Where such a specification has been made, JuliCA does not accept certificate requests that are outside this specification but will upon written request provide the Applicant a list of its authorized certificate requesters.

3.2.5.1 Verification of Domain Name Ownership

For OV certificates, all domain names to be included in a Certificate must be owned by JuliCA or a JuliCA Affiliate. An OV Certificate will not be issued for domain names which do not meet this requirement.

3.2.6. Criteria for Interoperation

All Cross Certificates that identify a JuliCA as the Subject are listed in the Repository, providedthat JuliCA has arranged for or accepted the establishment of the trust relationship.

3.3. Identification and Authentication for Re-key Requests

I&A procedures for re-key requests are the same as for initial Certificate applications. See Section 3.2.2.

3.3.1. Identification and Authentication for Routine Re-key

See Section 3.2.2.

3.3.2. Identification and Authentication for Re-key after Revocation

Not applicable.

3.4. Identification and Authentication for Revocation Request

Appropriate identification and authentication procedures are followed when evaluating requests for Certificate Revocation. If revocation is requested by the subscriber, identification and authentication is performed in accordance with Section 3.2. For revocation requests made by a member of JuliCA's Information Security team, identification and authentication is not required.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate Application

4.1.1. Who can submit a certificate application

Applications for an OV Certificate may be submitted by a representative employed by or contracted by, and authorized to act on behalf of, the applicant organization. In addition, applications fora DV Certificate can be submitted by any person through JuliCA's ACME request workflow or through a JuliCA product that offers a certificate request function.

JuliCA maintains an internal database of all previously revoked Certificates and previously rejected certificate requests. That database is used to identify subsequent suspicious certificate requests.

4.1.2. Enrollment process and responsibilities

Applicants seeking to obtain a JuliCA Certificate must submit to JuliCA a certificate application including a certificate request and provide at a minimum, the following:

- The Public Key to be included in the Certificate (if the Subscriber has generated its own Key Pair);
- The fully qualified domain names and/or IP addresses to be included in the Certificate;
- The identity of the Subscriber to be named as the Subject in the Certificate (if the Certificate is to include Subscriber Information);
- An executed Subscriber Agreement, which may be electronic;
- Any other relevant information that JuliCA requests.

One certificate request may be used for multiple Certificates to be issued to the same Applicant.

By executing the Subscriber Agreement, Subscribers warrant that all of the information contained in the certificate request is correct.

4.2. Certificate application processing

JuliCA performs the applicable certificate validation procedures and as required verifies the completeness, accuracy and authenticity of the information provided by the Applicant prior to issuing a Certificate. The procedures include:

- Verifying that the Applicant is permitted to obtain a Certificate under the relevant stipulations of the CP and this CPS.
- Verifying that the Applicant has provided a well-formed, valid CSR, containing a valid signature;
- Obtaining a Public Key from the Applicant;
- Verifying that the Applicant has executed the Subscriber Agreement;
- Validating that the requested Certificate meets the requirements in Sections 3.1.1 - 3.1.5;
- Performing the validation procedures set out in Section 3.2 and the relevant Subsections in so far as they apply to the type of the requested Certificate.

4.2.1. Performing identification and authentication functions

JuliCA performs identification and authentication functions during the Certificate application pro-

cess and during the Certificate re-key process.

Certificate Applications are not approved unless JuliCA has obtained all necessary information as specified in Section 4.1.2. If missing information cannot be readily obtained from a trusted internal data source, JuliCA may ask the Applicant to provide the required information in an alternative form.

Data obtained for identification and authentication purposes from a trusted third party source, is confirmed with the Applicant before it is used.

JuliCA maintains procedures to identify High Risk Certificate Requests that require additional verification activity prior to their approval. This includes maintaining an internal database of all Certificates that have previously been revoked and all certificate requests that have been rejected due to suspected phishing or other fraudulent usage or concerns. This information is used during identification and authentication to identify suspicious certificate requests.

4.2.2. Approval or rejection of certificate applications

JuliCA only considers Certificate applications for which all required subscriber information has been provided and validated. All other applications will be rejected.

Applications for subordinate CAs are not approved unless the CA in question will be operated by JuliCA or one of its affiliates and will be governed by the CP and this CPS.

4.2.3. Time to process certificate applications

Where JuliCA has entered into a written Service Level Agreement with the Applicant JuliCA will process certificate applications in accordance with the Service Level Objectives defined therein. Otherwise certificate applications will be processed within a reasonable timeframe.

4.2.4. Certificate Authority Authorization (CAA) records

JuliCA checks for a CAA record for each dNSName in the subjectAltName extension of the Certificate to be issued, according to the procedure in RFC 3467, following the processing instructions set down in RFC 3467 for any records found.

The following Issuer Domain Names in CAA “issue” or “issuewild” records are recognized as permitting JuliCA to issue:

If JuliCA issues, it does so within the TTL of the CAA record, or 8 hours, whichever is greater.

When processing CAA records, JuliCA processes the issue and issuewild property tags as specifiedin RFC 3467.

A Certificate is not issued if an unrecognized property has the critical flag set.
JuliCA may decide not to check for a CAA record:

- For certificates for which a Certificate Transparency pre-certificate was created and logged in at least two public logs, and for which CAA was checked;
- For certificates issued by a Technically Constrained Subordinate CA Certificate as set out in

Baseline Requirements Section 7.1.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant;

- When checking CAA records, a lookup failure is treated as permission to

issue if:

- the failure is outside the CA's infrastructure;
- the lookup has been retried at least once; and
- the domain's zone does not have a DNSSEC validation chain to the ICANN root.

JuliCA documents potential issuance that was prevented by a CAA record in sufficient detail to provide feedback to the CAB Forum on the circumstances.

CAA record checking results are logged in certificate lifecycle management event logs (see Section 5.4.1).

URL schemes in the iodef record other than mailto: or https: are not supported.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

Prior to issuing a Certificate JuliCA processes the Certificate Application and performs the required I&A procedures in accordance with this CPS. Once these procedures have been completed, the Certificate is generated and the appropriate key usage extension added.

Certificate Issuance by a root CA requires a CA Engineer to deliberately issue a direct command in order to perform the certificate signing operation.

4.3.2. Notification to subscriber by the CA of issuance of certificate

After issuing the Certificate, JuliCA will notify the Applicant via email or an alternate means of communication and will provide the Applicant with appropriate instructions on how to obtain the Certificate. Delivery of the Certificate will be made via a designated JuliCA service.

4.4. Certificate acceptance

4.4.1. Conduct constituting certificate acceptance

The Subscriber indicates acceptance of a Certificate by obtaining it.

By accepting a Certificate, the Subject agrees to be bound by the continuing responsibilities, obligations and duties imposed by the Subscriber Agreement and this CPS, and represents and warrants that:

- To its knowledge no unauthorized person has had access to the Private Key associated with the Certificate;

- The information it has supplied during the registration process is truthful and to the extent applicable, has been accurately and fully published within the certificate;

- It will at all times retain control of the Private Key corresponding to the Public Key listed in the Certificate;
- It will immediately inform JuliCA of any event that may invalidate or otherwise diminish the integrity of the Certificate, such as known or suspected loss, disclosure, or other compromiseof its Private Key associated with its Certificate.

4.4.2. Publication of the certificate by the CA

JuliCA publishes the CA certificates in the Repository.

4.4.3. Notification of certificate issuance by the CA to other entities

JuliCA may notify the public of the issuance of a certificate by submitting it to one or more publicly accessible Certificate Transparency logs.

4.5. Key pair and certificate usage

4.5.1. Subscriber private key and certificate usage

See Section 9.6.3, provisions 2. and 4.

4.5.2. Relying party public key and certificate usage

No stipulation.

4.6. Certificate Re-issuance

4.6.1. Circumstance for certificate renewal

Certificate renewal is the process whereby a new Certificate with an updated validity period is created for an existing Key Pair.

As a general rule, JuliCA does not offer Certificate renewal. Whenever a JuliCA Certificate expires, the Subscriber is required to generate request a new Certificate in accordance with this CPS.

4.6.2. Who may request renewal

Not applicable.

4.6.3. Processing certificate renewal requests

Not applicable.

4.6.4. Notification of new certificate issuance to subscriber

Not applicable.

4.6.5. Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6. Publication of the renewal certificate by the CA

Not applicable.

4.6.7. Notification of certificate issuance by the CA to other entities

Not applicable.

4.7. Certificate re-key

4.7.1. Circumstance for certificate re-key

JuliCA treats certificate re-key requests as requests for the issuance of a new Certificate.

4.7.2. Who may request certification of a new public key

See Section 4.1.1.

4.7.3. Processing certificate re-keying requests

See Section 4.2.

4.7.4. Notification of new certificate issuance to subscriber

See Section 4.3.2.

4.7.5. Conduct constituting acceptance of a re-keyed certificate

See Section 4.4.1.

4.7.6. Publication of the re-keyed certificate by the CA

See Section 4.4.2.

4.7.7. Notification of certificate issuance by the CA to other entities

See Section 4.4.3.

4.8. Certificate modification

JuliCA does not modify previously issued certificates. Any request for certificate modification will be treated as a request for the issuance of a new Certificate.

4.8.1. Circumstance for certificate modification

Not applicable.

4.8.2. Who may request certificate modification

See Section 4.1.1.

4.8.3. Processing certificate modification requests

See Section 4.2.

4.8.4. Notification of new certificate issuance to subscriber

See Section 4.3.2.

4.8.5. Conduct constituting acceptance of modified certificate

See Section 4.4.1.

4.8.6. Publication of the modified certificate by the CA

See Section 4.4.2.

4.8.7. Notification of certificate issuance by the CA to other entities

See Section 4.4.3.

4.9. Certificate revocation and suspension

4.9.1. Circumstances for revocation

Revocation of a certificate is to permanently end the operational period of the certificate prior to reaching the end of its stated validity period. JULICA CA will revoke a digital certificate if:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the Private Key associated with the certificate.
- The subscriber or JULICA CA has breached a material obligation under this CP/CPS.
- Either the subscriber's or JULICA CA 's obligations under this CP/CPS are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person's information is materially threatened or compromised.
- JULICA CA receives a lawful and binding order from a government or regulatory body to revoke the certificate.

There has been a modification of the information pertaining to the subscriber that is contained within the certificate. For Code-Signing Certificates, JULICA CA receives notice or otherwise becomes aware or suspects that information in the certificate is inaccurate or that someone has used the Code Signing Certificate to sign, publish or distribute spyware, Trojans, root kits, browser

hijackers, malware, or other content it deems harmful, malicious, hostile, deceptive or downloaded onto a user's system without their consent.

4.9.1.1. Reasons for Revoking a Subscriber Certificate

JuliCA will revoke a Subscriber Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that JuliCA revokes the Certificate;
2. The Subscriber notifies JuliCA that the original certificate request was not authorized and does not retroactively grant authorization;
3. JuliCA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or
4. JuliCA 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.

JuliCA will revoke a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
2. JuliCA obtains evidence that the Certificate was misused;
3. JuliCA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement;
4. JuliCA 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 arbi- trator 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. JuliCA is made aware that a Wildcard Certificate has been used to authenticate a fraudu-lently misleading subordinate Fully-Qualified Domain Name;
6. JuliCA is made aware of a material change in the information contained in the Certificate;
7. JuliCA is made aware that the Certificate was not issued in accordance with the BR, the CP or this CPS;
8. JuliCA determines or is made aware that any of the information appearing in the Certificateis inaccurate;
9. JuliCA's right to issue Certificates under the BR expires or is revoked or terminated, unless JuliCA has made arrangements to continue maintaining its CRL/OCSP Repository;
10. Revocation is required by the CP or this CPS; or
11. JuliCA is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

JuliCA will revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies JuliCA that the original certificate request was not authorized and does not retroactively grant authorization;
3. JuliCA obtains 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 of Sections 6.1.5 and 6.1.6;
4. JuliCA obtains evidence that the Certificate was misused;
5. JuliCA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with the CP or this CPS;
6. JuliCA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. JuliCA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. JuliCA's or Subordinate CA's right to issue Certificates under the BR expires or is revoked or terminated, unless JuliCA has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the CP and/or this CPS.

4.9.2. Who can request revocation

Certificate Revocation can be requested by:

- The Subscriber or Subject named in the concerned Certificate or its authorized representative;
- Anyone in possession of, or with access to, the Private Key that corresponds to the Public Key in the Certificate;
- Anyone who proves or reasonably suspects that the Private Key which corresponds to the Public Key in the Certificate has been compromised;
- Anyone who proves or reasonably suspects that the certificate has been used fraudulently orin a manner that is otherwise non-compliant with the CP or this CPS;
- Any authorized member of JuliCA's Information Security Team.

4.9.3. Procedure for revocation request

Requests for Certificate revocation and reports concerning suspected certificate misuse, fraud, inappropriate conduct and other certificate related matters can be submitted via email to contact@pki.goog. If the request or report is related to a potential compromise of the private key of a certificate, the requester should also contact security@pki.goog.

JuliCA maintains capabilities to receive Certificate revocation requests 24/7.

Certificate revocation requests that are made by the Subscriber are evaluated using the Identification and Authorization criteria set out in Section 3 of the CP. Requests made by other parties are evaluated on a case by case basis taking into consideration the following criteria:

- The nature of the alleged problem reported by the requestor;
- The evidence provided in support of the request;
- The urgency of the request;

- The quantity of requests received in relation to the concerned Certificate or Subscriber;
- The entity making the request; and
- Applicable legislation.

If JuliCA determines that a revocation is warranted it updates the certificate status information accordingly. Where appropriate JuliCA may also forward the case to law enforcement.

4.9.4. Revocation request grace period

JuliCA may grant revocation grace periods.

4.9.5. Time within which CA must process the revocation request

Within 24 hours after receiving a Certificate Problem Report, JuliCA will investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After having investigated the facts and circumstances, JuliCA will work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the CA will revoke the certificate.

Depending on the revocation reason and as set out in Section 4.9.1., JuliCA will revoke the concerned Certificate no later than 24 hours or 5 days after having received the Certificate Problem Report.
The following criteria will be considered when selecting the revocation date:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint; and
5. Relevant laws and regulations.

4.9.6. Revocation checking requirement for relying parties

Relying Parties are required to confirm the validity of each Certificate in the certificate chain by checking the applicable CRL or OCSP responder before relying on a JuliCA Certificate.

4.9.7. CRL issuance frequency (if applicable)

For the status of Subscriber Certificates: For CAs for which JuliCA publishes a CRL, that CRL is updated and reissued at least once every seven (7) days, and the value of the nextUpdate fieldis not more than ten (10) days beyond the value of the thisUpdate field.

For the status of Subordinate CA Certificates: JuliCA updates and reissues CRLs at least (i) once every twelve (12) months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and

the value of the nextUpdate field is not more than twelve months beyond the value of the thisUpdate field.

See Section 2.2 for CRL locations.

4.9.8. Maximum latency for CRLs (if applicable)

JuliCA maintains sufficient resources to provide a response time for CRL and OCSP responses of ten seconds or less under normal operating conditions.

4.9.9. On-line revocation/status checking availability

JuliCA makes available OCSP status information for all certificates it issues. The OCSP responder locations are included in the respective certificates.

OCSP responses conform to RFC6960 and/or RFC5019. They are either:

1. Signed by the CA that issued the Certificates whose revocation status they indicate, or
2. Signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is indicated. The OCSP Responder's signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10. On-line revocation checking requirements

The OCSP responder supports GET method for receiving OCSP requests. It does not respond with a "good" status on certificates which have not been issued.
For Subscriber Certificates, OCSP data is updated at least every three days. It has a minimum validity of one day and a maximum validity time of seven days.

For Subordinate CA Certificates, OCSP data is updated at least every twelve (12) months and within 24 hours after revoking a Subordinate CA Certificate.

4.9.11. Other forms of revocation advertisements available

Not applicable.

4.9.12. Special requirements related to key compromise

In case of a compromise of the private key used to sign certificates, the Subscriber must immediately notify JuliCA that the Subscriber's certificate has been compromised. JuliCA will revoke the concerned signing key, and publish a CRL to inform relying parties that the certificates issued from it can no longer be trusted.

The subscriber is responsible for investigating the circumstances of any such compromise.

4.9.13. Circumstances for suspension

Suspension of a certificate may occur when the E-CSP determines there is a need for temporary restriction of the certificate's validity pending further investigation. Examples include:

• Suspected (but unconfirmed) compromise of the private key;
• Subscriber request for temporary suspension;
• Investigation of possible fraudulent activity or misuse;
• Any other situation where immediate revocation is not warranted but the certificate should not be used until the matter is resolved.

4.9.14. Who can request suspension

Revocation or suspension may be requested by:

• The Subscriber named in the certificate;

• An authorised representative of the Subscriber;

• The E-CSP itself (for operational or security reasons).

4.9.15. Procedure for suspension request

The E-CSP shall verify the identity of the requestor using the same authentication methods applied during the original registration process or other secure means documented in this CPS (e.g., multi-factor authentication, signed request, or secure portal with OTP).

4.9.16. Processing of revocation or suspension

All revocation and suspension requests shall be processed promptly. Revocation information shall be published to the CRL/OCSP within the timeframes defined in Section 4.9.9.

4.9.17. Reactivation of suspended certificates

A suspended certificate shall be reactivated by the E-CSP only after:

• Completion of a full investigation; and

• Confirmation that no compromise has occurred.

Reactivation shall require dual control, shall be properly logged in the audit trail, and the Subscriber shall be notified.

4.9.18. Revoked Certificates

Once revoked, a certificate shall never be reactivated.

4.9.19. Revocation and suspension information in the CRL

Information about revoked or suspended certificates shall be:

• Updated in the Certificate Revocation List (CRL) immediately upon action;

• Digitally signed by the E-CSP using its private key;

• Clearly distinguished (suspended certificates shall be marked distinctly from revoked certificates).

4.9.20. Protection of CRL information

The E-CSP shall ensure that revocation and suspension information in the CRL is protected from unauthorised modifications through:

• Technical controls (cryptographic signing, access restrictions, audit logging);

• Procedural controls (dual control, change management, and segregation of duties).

4.9.21. Subscriber notification

The Subscriber shall be promptly informed of any suspension or revocation of their certificate via the contact details on record (email and/or SMS).

4.9.22. Revocation checking requirement for relying parties

Relying Parties are required to check the validity status of a certificate using the CRL or OCSP before relying on it.

4.9.23. Limits on suspension period

Not applicable.

4.10. Certificate status services

4.10.1. Operational characteristics

Revocation entries on a CRL or OCSP Response are not removed until after the Expiry Date of the revoked Certificate.

4.10.2. Service availability

Certificate Status Services are available 24x7, unless temporarily unavailable due to maintenance or service failure. Additionally JuliCA maintains a continuous 24x7 ability to respond internally to

high-priority Certificate Problem Reports.

4.10.3. Optional features

Not applicable.

4.11. End of subscription

A subscriber's subscription ends when its Certificate expires or when the Certificate is revoked. A subscription also ends when the applicable subscriber agreement expires and is not renewed.

4.12. Key escrow and recovery

JuliCA does not escrow private keys.

4.12.1. Key escrow and recovery policy and practices

Not applicable.

4.12.2. Session key encapsulation and recovery policy and practices

Not applicable.

5. MANAGEMENT, OPERATIONAL AND PHYSICAL CONTROLS

5.1. Physical controls

The JuliCA infrastructure is located in and operated from secure facilities. Detailed security procedures are in place and followed that prohibit unauthorized access and entry into theareas of the facilities in which CA systems reside.

5.1.1. Site location and construction

JuliCA systems are located in a selected set of locations which have been evaluated for their physical security, as well as local legal considerations that may affect CA operations.

All CA systems are operated from buildings which are solidly constructed to prevent unauthorized entry.

5.1.2. Physical access

JuliCA has in place appropriate physical security controls to restrict access to all hardware and software used for providing CA Services. Access to such hardware and software is limited to those personnel performing in a trusted role as described in Section 5.2.1. Access is controlled through the use of electronic access controls, mechanical combination lock sets, deadbolts, or other security mechanisms. Such access controls are manually or electronically monitored for unauthorized

intrusion at all times. Only authorized personnel will be allowed access, either physical or logical, to the CA systems.

JuliCA enforces two-person access for all access to CA systems.

The JuliCA servers are located inside of a locked cabinet or cage area in a locked server room. Access to the server room is controlled by badge readers. The private keys for the CAs are stored in hardware security modules that are validated to FIPS 140-2 Level 3 or higher and that are physically tamper-evident and tamper-resistant.

5.1.3. Power and air conditioning

JuliCA facilities are connected to a UPS system and emergency power generator. They are equipped with cooling systems to ensure reliable operations.

5.1.4. Water exposures

All JuliCA facilities are equipped with controls which protect CA systems from damage result- ing from water leakage.

5.1.5. Fire prevention and protection

All JuliCA facilities are equipped with fire detection alarms and protection equipment.

5.1.6. Media storage

No stipulation.

5.1.7. Waste disposal

JuliCA takes reasonable steps to ensure that all media used for the storage of information such as keys, Activation Data or its files are sanitized or destroyed before they are released for disposal.

5.1.8. Off-site backup

JuliCA maintains backup facilities for its CA infrastructure which also hold copies of the CA private keys for redundancy. The backup facilities have security controls which are equivalent to those operated at the primary facility.

5.2. Procedural controls

5.2.1. Trusted roles

All personnel who have access to or control over cryptographic operations of a JuliCA that affect the issuance, use, and management of Certificates are considered as serving in a trusted role ("Trusted Role"). Such personnel include, but are not limited to, members of JuliCA's Information Security Team.

5.2.2. Number of persons required per task

The Private Key can only be backed up, stored, and recovered by personnel in trusted roles using, at least, dual control in a physically secured environment.

5.2.3. Identification and authentication for each role

JuliCA maintains controls to provide reasonable assurance that:

- A documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them is followed;
- The responsibilities and tasks assigned to Trusted Roles are documented and "separation of duties" for such Trusted Roles based on the risk assessment of the functions to be performedis implemented;
- Only personnel assigned to Trusted Roles have access to Secure Zones and High Security Zones;
- Individuals in a Trusted Role act only within the scope of such role when required for performing administrative tasks;
- Employees and contractors observe the principle of "least privilege" when accessing, or when configuring access privileges on, Certificate Systems;
- Trusted Roles use a unique credential created by or assigned to a single person for authentication to Certificate Systems;
- Where Trusted Roles use a username and a password to authenticate, access controls are configured such that at a minimum they satisfy the following requirements:
  - Passwords have at least twelve (12) characters for accounts not publicly accessible (accessible only within Secure Zones or High Security Zones);
  - Passwords for accounts that are accessible from outside a Secure Zone or High Security Zone are configured to have at least eight (8) characters, use a combination of at least numeric and alphabetic characters, and may not be one of the user's previous four passwords; and implement account lockout for failed access attempts; OR
  - Implement a documented password management and account lockout policy that the CA has determined provide at least the same level of protection against password guessing as the foregoing controls.
- Trusted Roles log out of or lock workstations when no longer in use;
- Workstations are configured with inactivity time-outs that log the user off or lock the workstation after a set time of inactivity without input from the user;
- Review all system accounts at least every 90 days and deactivate any accounts that are no longer necessary for operations;
- Revoke account access to Certificate Systems after no more than five (5) failed access attempts, provided that this security measure is supported by the Certificate System and does not weaken the security of this authentication control;

- Disable all privileged access of an individual to Certificate Systems within 24 hours upon termination of the individual's employment relationship with the CA;
- Enforce multi-factor authentication for administrator access to Issuing Systems and Certificate Management Systems;
- Restrict remote administration or access to an Issuing System, Certificate Management System, or Security Support System except when:
  - The remote connection originates from a device owned or controlled by the CA and from a pre-approved external IP address,
  - The remote connection is through a temporary, non-persistent encrypted channel that is supported by multi-factor authentication, and
  - The remote connection is made to a designated intermediary device meeting the following:
    * Located within the CA's network,
    * Secured in accordance with these Requirements, and
    * Mediates the remote connection to the Issuing System.

5.2.4. Roles requiring separation of duties

Auditors of the infrastructure and certificate issuance are independent from the operators who approve and issue certificates using a JuliCA.

To review their conformance with applicable policies and procedures, JuliCAs undergo annual audits performed by independent auditors.

5.3. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements

JuliCA has implemented policies for verifying the identity and trustworthiness of its personnel. Furthermore, JuliCA evaluates the performance of its CA staff to ensure that they perform their duties in a satisfactory manner.

All personnel operating the JuliCAs are JuliCA employees. There are no contractors or other third parties involved in the Certificate Management Process.

5.3.2. Background check procedures

JuliCA follows a set of established procedures for selecting and evaluating personnel who operate JuliCAs or act in other information security roles.

5.3.3. Training requirements

All JuliCA personnel who perform information verification duties receive skills-training that covers

basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including this CPS), common threats to the information verification process including phishing and other social engineering tactics.

Validation Specialists receive their skills-training prior to commencing their job role and JuliCA requires them to pass an examination on the applicable information verification requirements.

JuliCA maintains records of such training and ensures that personnel entrusted with Validation Specialist duties maintain an appropriate skill level.

5.3.4. Retraining frequency and requirements

JuliCA requires personnel in Trusted Roles to maintain skill levels consistent with the CA training and performance programs. To this end JuliCA requires such personnel to undergo re-training at least annually.

5.3.5. Job rotation frequency and sequence

No Stipulation.

5.3.6. Sanctions for unauthorized actions

JuliCA will impose sanctions, including suspension and termination if appropriate, on its employees acting in Trusted Roles if they perform unauthorized acts, abuse their authority, or for other appropriate reasons, at the discretion of the CA management.

5.3.7. Independent contractor requirements

Independent contractors must meet the same training requirements as JuliCA employees. Independent contractors will not be used in Trusted Roles.

5.3.8. Documentation supplied to personnel

Training and documentation is provided to JuliCA employees as necessary for them to perform competently in their job role.

5.4. Audit logging procedures

5.4.1. Types of events recorded

JuliCA records system and CA application events and creates certificate management logs from the data collected in accordance with internal audit procedures. The following events are recorded:

- CA key lifecycle management events
  - Key generation, backup, storage, recovery, archival and destruction;
  - Cryptographic device lifecycle events.
- Applicant and Subscriber events
  - Request to create a certificate;
  - Request to revoke a certificate.

- CA and Subscriber Certificate lifecycle events
  - Verification activities stipulated in the CP and this CPS;
  - Acceptance and rejection of certificate requests, frequency of processing log;
  - Key generation;
  - Key compromise notification;
  - Creation of a certificate;
  - Delivery of a certificate;
  - Revocation of a certificate;
  - Generation of a Certificate Revocation List;
  - Generation of an OCSP response.
- Actions by Trusted Personnel
  - Login events and use of identification and authentication mechanisms;
  - Changes to CA policies;
  - Changes to CA keys;
  - Configuration changes to the CA.
- Security Events
  - Successful and unsuccessful PKI system access attempts;
  - PKI and security system actions performed;
  - Security profile changes;
  - System crashes, hardware failures, and other anomalies;
  - Firewall and router activities; and
  - Entries to and exits from the CA facility.

Log entries include the following elements:

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

JuliCA collects event information and creates Certificate management logs using automated and procedures. Where this is not possible, manual logging and record keeping methods may be used.

5.4.2. Frequency of processing log

Audit logs are reviewed on an as-needed basis.

5.4.3. Retention period for audit log

JuliCA retains any audit logs generated for at least seven years, or longer if required by law and makes these audit logs available to its Qualified Auditor upon request.

5.4.4. Protection of audit log

Multiple copies of audit logs are stored in different locations and protected by appropriate physical and logical access controls.

5.4.5. Audit log backup procedures

JuliCA maintains formal procedures to ensure that audit logs are backed up and retained to keep them available as necessary for the CA service and as stipulated by applicable standards.

5.4.6. Audit collection system (internal vs. external)

No stipulation.

5.4.7. Notification to event-causing subject

Events that are deemed potential security issues involving the Certificate Authority infrastructure will be escalated to a permanent security monitoring team.

5.4.8. Vulnerability assessments

JuliCA's security program conducts an annual Risk Assessment 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 Processes;
2. Assesses the likelihood and potential damage caused by these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the adequacy of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

JuliCA follows a formal documented vulnerability correction process that includes identification, review, response, and remediation of vulnerabilities.

Additionally, JuliCA performs a Vulnerability Scan on public and private IP addresses belonging to the Certificate Systems on the following occasions:

- Within one week of receiving a request from the CA/Browser Forum;
- After any significant system or network change;
- At least once per quarter.

JuliCA performs a Penetration Test on its Certificate Systems on at least an annual basis and after infrastructure modifications that it determines are significant.

5.5. Records archival

5.5.1. Types of records archived

All certificate suspension and revocation information, certificates, registration documents, and related audit trails are archived for at least 7 years as required by the KICA CAP 411A.

5.5.2. Retention period for archive

JuliCA retains all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that

documentation ceases to be valid, or longer as required by law.

5.5.3. Protection of archive

A backup of archive information is maintained at a distinct, separate location with similar security and availability requirements.

Archives are protected from unauthorised modification through cryptographic signing, access controls, and physical security measures.

5.5.4. Archive backup procedures

Backup and recovery procedures exist and can be utilized so that a complete set of backup copies will be available in the event of the loss or destruction of the primary archives.

5.5.5. Testing of the archival process

The JULICA shall regularly test the archival process to ensure:
• Accuracy – archived records are complete, legible, and identical to the original;
• Security – archives are protected against unauthorised access, modification, or deletion;
• Accessibility – archived records can be retrieved in a timely manner when required.
These tests shall be conducted at least annually and as part of the Business Continuity and Disaster Recovery Plan testing. Results of the tests, including any deficiencies identified and corrective actions taken, shall be documented and retained.

5.5.6. Requirements for time-stamping of records

All archived records will be time-stamped by the CA's normal logging facilities. Such time information need not be cryptography-based.

5.5.7. Archive collection system (internal or external)

No stipulation.

5.5.8. Procedures to obtain and verify archive information

No stipulation.

5.6. Key changeover

The procedure for providing a new CA Certificate to a Subject following a re-key is the same as the procedure for initially providing the CA Certificate.

5.7. Compromise and disaster recovery

5.7.1. Incident and compromise handling procedures

If a disaster causes a JuliCA to become inoperative, JuliCA will re-initiate its operations on

replacement hardware at a comparable, secured facility after ensuring the integrity and security of the CA systems.

JuliCA maintains an Incident Response Plan and a Disaster Recovery Plan, which set out the procedures necessary to ensure business continuity, to notify affected stakeholders, and to reason- ably protect Application Software, Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. JuliCA annually tests, reviews, and updates its business continuity plan and its security plans and makes them available to the its auditors upon request.

The business continuity plan includes:

1. The conditions for activating the plan;
2. Emergency procedures;
3. Fallback procedures;
4. Resumption procedures;
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans;
10. A plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes;
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. A definition of acceptable system outage and recovery times;
13. The frequency at which backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the CA's main site; and
15. Procedures for securing an affected facility following a disaster and prior to restoring a secure environment either at the original or a remote site.

5.7.2. Recovery procedures if computing resources, software, and/or data are corrupted

JuliCA maintains a backup site in a remote location that mirrors its primary facility, so that if any software or data is corrupted it can be restored from the backup site via a secure connection.

Backups of all relevant software and data are taken on a regular basis. They are stored off-site and can be retrieved electronically when necessary.

5.7.3. Recovery procedures after key compromise

In the event that the Private Key of a JuliCA is compromised, JuliCA will:

- Immediately cease using the compromised key material;
- Revoke all Certificates signed with the compromised key;
- Take commercially reasonable steps to notify all Subscribers of the Revocation; and
- Take commercially reasonable steps to cause all Subscribers to cease using, for any purpose, any such Certificates.

Once the compromised key material has been replaced and a secure operation of the CA in question has been established, the CA may re-issue the revoked certificates following the procedure for initially providing the certificates.

5.7.4. Business continuity capabilities after a disaster

JuliCA employs and contracts security personnel who will use all reasonable means to monitor the CA facility after a natural or other type of disaster so as to protect sensitive materials and information against loss, additional damage, and theft.

To confirm that it possesses appropriate disaster recovery capabilities, JuliCA performs periodic tests of its business continuity and disaster recovery plans.

5.8. CA or RA termination

When it is necessary to terminate operation a JuliCA, the impact of the termination is to be minimized as much as possible in light of the prevailing circumstances. This includes:

- Providing practicable and reasonable prior notice to all Subscribers;
- Assisting with the orderly transfer of service, and operational records, to a successor CA, if any;
- Preserving all records for a minimum of one (1) year or as required by this CPS, whicheveris longer; and
- Revoking all Certificates issued by the CA no later than at the time of termination.

If commercially reasonable, prior notice of the termination of a JuliCA will be given at least3 months before the termination date.

6. TECHNICAL SECURITY CONTROLS

6.1. Key pair generation and installation

6.1.1. Key pair generation

Key Pairs for JuliCAs are generated pursuant to formal key generation procedures and inside of a FIPS 140-2 Level 3 certified Hardware Security Module from where the private key cannot be extracted in plaintext.

Key pairs for intermediate CAs are generated in accordance with the requirements set forth by the corresponding root CA including any contractual obligations that might exist between JuliCA and the root CA.

Requests for Subscriber Certificates are rejected if the Public Key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 or if it has a known weak Private Key.

6.1.2. Private key delivery to subscriber

JuliCA does not archive Subscriber Private Keys.

6.1.3. Public key delivery to certificate issuer

Subscribers provide their public key to JuliCA for certification through a PKCS#10 Certificate Signing Request. The preferred transfer method for sending this information is HTTP over Secure Sockets Layer (SSL).

6.1.4. CA public key delivery to relying parties

The public keys of JuliCAs are made available from the online repository at http://pki.goog/. Additionally the public keys of JuliCA root CAs are delivered through their inclusion into the root programs of software and equipment manufacturers.

6.1.5. Key sizes

To prevent cryptanalytic attacks, all JuliCAs use key sizes and cryptographic protocols which adhere to NIST recommendations and to the applicable provisions of the CP.

6.1.6. Public key parameters generation and quality checking

For RSA keys, JuliCA confirms that the value of the public exponent is an odd number equal to 3 or more.

6.1.7 Key usage purposes (as per X.509 v3. key usage field)

Root CA Private Keys are not 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 infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates, and OCSP Response verification Certificates); and
4. Certificates issued solely for the purpose of testing products with Certificates issued by a Root CA.

6.2. Private Key Protection and Cryptographic Module EngineeringControls

6.2.1. Cryptographic module standards and controls

All CA private keys used to sign certificates, CRLs, or any related information leverage hardware security modules meeting FIPS 140-2 Level 3 or higher and Common Criteria EAL4+ security specifications. Cryptography leveraged to protect this information is selected to withstand cryptanalytic attacks for the lifetime of the encrypted key.

CA Private Keys are kept in a physically secure location, and are never stored unencrypted outside of Hardware Security Modules.

6.2.2. Private key (n out of m) multi-person control

All Certificate Authority Key Pairs are generated in pre-planned key generation ceremonies. Upon finalization of the ceremony, all individuals involved sign off on the successful completion of the script, and thoroughly describe any exceptions that may have been applied in the process.

Records are maintained at least for the lifetime of the key pair.

6.2.3. Private key escrow

The Private Keys of JuliCAs are not escrowed.

6.2.4. Private key backup

Backups of CA Private Keys are stored in a secure manner in accordance with applicable JuliCA policy.

6.2.5. Private key archival

Private Keys belonging to JuliCAs are not archived by parties other than JuliCA.

6.2.6. Private key transfer into or from a cryptographic module

Private Keys generated on behalf of a Subordinate CA are encrypted for transport to the Subordinate CA.

All transfers of Private Keys into or from a cryptographic module are performed in accordance with the procedures specified by the vendor of the relevant cryptographic module.

6.2.7. Private key storage on cryptographic module

Private keys are stored in accordance with applicable instructions specified by the cryptographic module manufacturer.

6.2.8. Method of activating private key

Private keys are activated in accordance with applicable instructions specified by the cryptographic module manufacturer

6.2.9. Method of deactivating private key

Private keys are deactivated in accordance with applicable instructions specified by the cryptographic module manufacturer.

6.2.10. Method of destroying private key

Private Keys are destroyed in accordance with applicable instructions specified by the cryptographic module manufacturer. In addition JuliCA policy on destruction of highly confidential information is followed.

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

No stipulation.

6.3.2. Certificate operational periods and key pair usage periods

Certificates are valid starting at the moment of signing, unless otherwise specified in the certificate validity structure, until the end noted in the certificate expiration time.

Subscriber certificates are issued for a period of one year or less.

6.4. Activation data

6.4.1. Activation data generation and installation

No stipulation.

6.4.2. Activation data protection

Hardware Security Module keys are stored in the Hardware Security Module, and can only be used by authorized CA administrators upon authentication. Passphrases required to unlock the keys are stored in an encrypted form. Physical activation data such as smart cards, when applicable, are stored in a protected and secured environment.

6.4.3. Other aspects of activation data

No stipulation.

6.5. Computer security controls

6.5.1. Specific computer security technical requirements

JuliCA system information is protected from unauthorized access through a combination of operating system controls, physical controls and network controls. Network security controls are specified in Section 6.7.

CA systems enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2. Computer security rating

No stipulation.

6.6. Life cycle technical controls

6.6.1. System development controls

JuliCA uses software that has been formally tested for suitability and fitness for purpose. Hardwareis procured through a managed process leveraging industry-standard vendors.

6.6.2. Security management controls

JuliCA has established an Information Security Organization which implements and operates a framework of internal controls and comprises technical, organizational, and procedural measures.

6.6.3. Life cycle security controls

System security management is controlled through the privileges assigned to the operating system accounts of the CA infrastructure and by the Trusted Roles described in this CPS.

6.7. Network security controls

The secure equipment for JuliCAs is located behind hardware firewall devices that restrict access to only the internal JuliCA network, and only to ports used for managing the CA and issuing Certificates.

6.8. Time-stamping

All logs contain synchronized time stamps.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. Certificate profile

JuliCA Certificates conform to RFC 3647, Internet X.509 Public Key Infrastructure Certificate and CRL Profile. Certificate extensions and their criticality, as well as cryptographic algorithm object identifiers, are populated according to the IETF RFC 3647 standards.

In cases where stipulations of RFC 3647 and the applicable CA/Browser Forum Baseline Requirements differ, the Baseline Requirements notion will be adhered to.

7.1.1. Version number(s)

X.509 Subscriber Certificates issued by JuliCAs conform to X.509 version 3.

7.1.2. Certificate extensions

See JuliCA Certificate Profiles appendix.

7.1.3. Algorithm object identifiers

See JuliCA Certificate Profiles appendix.

7.1.4. Name forms

By issuing a Certificate, JuliCA represents that it followed the procedure set forth in this CPS to verify that, as of the issuance date, all of the Subject Information was accurate. JuliCA does not include a Domain Name in a Subject attribute except as specified in Section 3.2.5.1

Wildcard names may be used for wildcard certificates.

JuliCA's processes relating to I&A and Certificate issuance prevent an OU attribute from includ- ing a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless this information has been verified in accordance with Sec- tion 3.2 and the Certificate also contains subject:organizationName, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 3.2.2.1.

All attributes, when present within the subject field, contain information that has been verified.

SSL certificates may not contain metadata such as '.', '-', and '' (i.e. space) characters, and/or any other indication that a value is absent, incomplete, or a field is not applicable. dNSName entries may not contain underscore characters ("_").

7.1.5. Name constraints

No stipulation.

7.1.6. Certificate policy object identifier

End-entity Certificates include the following Object Identifiers depending on the method of validation used.

- CA/Browser Forum Baseline Requirements: 1.3.6.1.4.1.11129.2.5.1
- Domain Validated (DV) Certificates 2.23.140.1.2.1
- Organization Validated (OV) Certificates 2.23.140.1.2.2
- Extended Validation (EV) 2.23.140.1.1
- Individual Validated (IV) 2.23.140.1.2.3
- EV Code Signing 2.23.140.1.3
- Non-EV Code Signing 2.23.140.1.4

7.1.7. Usage of Policy Constraints extension

The PolicyConstraints extension shall be empty.

7.1.8. Policy qualifiers syntax and semantics

No stipulation.

7.1.9. Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2. CRL profile

CRLs issued by JuliCAs conform to RFC 3647 standards.

7.2.1. Version number(s)

No stipulation.

7.2.2. CRL and CRL entry extensions

No stipulation.

7.3. OCSP profile

All JuliCAs support OCSP, and their responders conform to the RFC 6960 standard.

7.3.1. Version number(s)

No stipulation.

7.3.2. OCSP extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. Frequency or circumstances of assessment

Compliance Audits are conducted at least annually.

8.2. Identity/qualifications of assessor

Compliance audits of JuliCAs are performed by a public accounting firm that possesses the following qualifications and skills:

1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in the WebTrust standard;
3. 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;
4. Is licensed by WebTrust;
5. Bound by law, government regulation, or a professional code of ethics; and
6. 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 in coverage.

8.3. Assessor's relationship to assessed entity

Compliance audits of JuliCAs are performed by a public accounting firm that is independent of the subject of the audit.

8.4. Topics covered by assessment

Annual Compliance Audits of JuliCAs cover a validation of controls relevant for the proper operation of the CAs. In particular they cover an assessment of the auditee's compliance with the WebTrust Principles and Criteria for Certification Authorities formulated by CPA Canada and the American Institute of Certified Public Accountants (AICPA) as well as the CA/Browser Forum's Baseline Requirements.

8.5. Actions taken as a result of deficiency

Significant deficiencies identified during a Compliance Audit will result in a determination of actions to be taken by the CA management. These decisions are made with input from theauditor, and implemented within a commercially reasonable period of time.

8.6. Communication of results

The Audit Report is made publicly available no later than three months after the end of the audit period. JuliCA is not required to make publicly available any general audit findings that do not impact the overall audit opinion. In the event of a delay greater than three months, and if so requested by an Application Software Supplier, JuliCA will provide an explanatory letter signed by the Qualified Auditor.
The Audit Report shall state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates by the JuliCAs.

8.7. Self-Audits

JuliCA monitors its adherence to the CP and this CPS by performing self audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

JuliCA requires all Subordinate CAs that it cross signs as well as all Delegated Third Parties to undergo an annual audit which meets the criteria specified in Section 8.1.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. Fees

9.1.1. Certificate issuance or renewal fees

JuliCA may charge Subscribers for the issuance, management and renewal of Certificates. JuliCA

will never charge for the revocation of certificates it has issued.

9.1.2. Certificate access fees

JuliCA may charge a reasonable fee for access to its Certificate databases.

9.1.3. Revocation or status information access fees

JuliCA does not charge a fee as a condition of making the CRLs required by this CPS available in a Repository or otherwise available to Relying Parties. JuliCA may however charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. JuliCA does not permit access to revocation information, Certificate status information, or time stamping in its Repository by third parties that provide products or services that utilize such Certificate status information without JuliCA's prior express written consent.

9.1.4. Fees for other services

JuliCA does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with JuliCA.

9.1.5. Refund policy

No stipulation.

9.2. Financial responsibility

9.2.1. Insurance coverage

JuliCA maintains general liability insurance coverage.

9.2.2. Other assets

No stipulation.

9.2.3. Insurance or warranty coverage for end-entities

No stipulation.

9.3. Confidentiality of business information

9.3.1. Scope of confidential information

The following Applicant and Subscriber related information is considered confidential information.

1. Certificate applications;
2. Records submitted by the Applicant in support of Certificate applications;
3. Private keys;

4. Log files and other audit records;
5. Transaction records.

9.3.2. Information not within the scope of confidential information

Certificates and revocation data are not considered confidential information. Furthermore information is not considered confidential if its disclosure is mandated pursuant to the CP or this CPS.

9.3.3. Responsibility to protect confidential information

JuliCA, its contractors and agents use a reasonable degree of care when processing and protecting confidential information.

9.4. Privacy of personal information

9.4.1. Privacy plan

JuliCA follows its Privacy Policy which is available at: https://www.JuliCA.com/policies/privacy/

9.4.2. Information treated as private

See Section 9.4.1.

9.4.3. Information not deemed private

See Section 9.4.1.

9.4.4. Responsibility to protect private information

See Section 9.4.1.

9.4.5. Notice and consent to use private information

See Section 9.4.1.

9.4.6. Disclosure pursuant to judicial or administrative process

See Section 9.4.1.

9.4.7. Other information disclosure circumstances

See Section 9.4.1.

9.5. Intellectual property rights

JuliCA, or its licensors, own the intellectual property rights in the JuliCA services, including the Certificates, trademarks used in providing Certificate services and this CPS.

Certificate and revocation information are the exclusive property of JuliCA. JuliCA grants permission to reproduce and distribute certificates on a non-exclusive and royalty-free basis, provided that they are reproduced and distributed in full. JuliCA does not allow derivative works of its Certificates or products without prior written permission.

Private and Public Keys remain the property of the Subscribers who rightfully hold them. All secret shares (distributed elements) of the JuliCA Private Keys are the property of JuliCA.

9.6. Representations and warranties

9.6.1. CA representations and warranties

9.6.1.1. Limited warranty

JuliCA provides the following limited warranty to the Certificate Beneficiaries at the time of Certificate issuance: (a) it issued the Certificate substantially in compliance with this CPS; b) the information contained within the Certificate accurately reflects the information provided to JuliCA by the Applicant in all material respects; and (c) it has taken reasonable steps to verify that the information within the Certificate is accurate. The steps JuliCA takes to verify the information contained in a Certificate are set forth in this CPS.

9.6.1.2. CABF Warranties and Obligations

Domain-validated and organization-validated SSL Certificates conform to the CA/Browser Forum ("CABF") Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates. By issuing such a Certificate, JuliCA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, JuliCA has complied with this Section and its CPS in issuing and managing the Certificate.

The Certificate warranties to Certificate Beneficiaries are as follows:

1. Right to Use Domain Name or IP Address: That, at the time of issuance, JuliCA (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 this CPS;
2. Authorization for Certificate: That, at the time of issuance, JuliCA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant 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 this CPS;
3. Accuracy of Information: That, at the time of issuance, JuliCA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;
4. No Misleading Information: That, at the time of issuance, JuliCA (i) implemented a pro-

cedure 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 this CPS;

5. Identity of Applicant: That, if the Certificate contains Subject identity information, JuliCA (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.1.1.1 and 3.2.2.1; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in this CPS;
6. Subscriber Agreement: That, if Subscriber is not a JuliCA Affiliate, the Subscriber and JuliCA are parties to a legally valid and enforceable Subscriber Agreement that satisfies the requirements of this Section, or, if Subscriber is a JuliCA Affiliate, the Applicant acknowledged and accepted JuliCA's Certificate terms of use, notice of which is provided by JuliCA to Applicant during the Certificate issuance process;
7. Status: JuliCA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
8. Revocation: JuliCA will revoke the Certificate for any of the reasons specified in this CPS.

9.6.2. RA representations and warranties

No stipulation.

9.6.3. Subscriber representations and warranties

JuliCA requires, as part of the Subscriber Agreement or Terms of Use Agreement, that the Applicant make the commitments and warranties in this Section for the benefit of the CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, JuliCA obtains, for its express benefit and that of the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the CA, or
2. The Applicant's agreement to the Terms of Use agreement.

JuliCA implements a process to ensure that each Subscriber or Terms of Use Agreement is legally enforceable against the Applicant. In either case, the Agreement must apply to the Certificate to be issued pursuant to the certificate request. JuliCA may use an electronic or "click-through" Agreement provided that it has determined that such agreements are legally enforceable. A separate Agreement may be used for each certificate request, or a single Agreement may be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certifi- cate that the CA issues to the Applicant is clearly covered by that Subscriber or Terms of Use Agreement.

The Subscriber or Terms of Use Agreement contains provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to JuliCA, both in the certificate request and as otherwise requested by JuliCA in connection with the issuance of the Certificate(s) to be supplied;
2. Protection of Private Key: An obligation and warranty by the Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
3. Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. Use of Certificate: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber or Terms of Use Agreement;
5. Reporting and Revocation: An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request JuliCA to revoke the Certificate, in the event that: (a) any information in the Certificate is, or becomes, incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate;
6. Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
7. Responsiveness: An obligation to respond to JuliCA's instructions concerning Key Compromise or Certificate misuse within a specified time period.
8. Acknowledgment and Acceptance: An acknowledgment and acceptance that JuliCA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Agreement or if JuliCA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

Subscriber Agreements may include additional representations and warranties.

9.6.4. Relying party representations and warranties

Relying Parties represent and warrant that: (a) they have read, understand and agree to this CPS; (b) they have verified both the relevant JuliCA's Certificate and any other certificates in the certificate chain using the relevant CRL or OCSP; (c) they will not use a Certificate if the Certificate has expired or been revoked; (d) they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate; (e) they have studied the applicable limitations on the usage of Certificates and agree to JuliCA's limitations on liability related to the use of Certificates; (f) they are solely responsible for deciding whether or not to rely on information in a Certificate; and (g) they are solely responsible for the legal and other consequences of their failure to perform the Relying Party obligations in this CPS.

Relying Parties also represent and warrant that they will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a Certificate after considering:

1. Applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;

2. The intended use of the Certificate as listed in the Certificate or this CPS;
3. The data listed in the Certificate;
4. The economic value of the transaction or communication;

5. The potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication;
6. The Relying Party's previous course of dealing with the Subscriber;
7. The Relying Party's understanding of trade, including experience with computer-based methods of trade; and
8. Any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

9.6.5. Representations and warranties of other participants

No stipulation.

9.7. Disclaimers of warranties

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1 OF THIS CPS, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE." TO THE MAXIMUM EXTENT PERMITTED BY LAW, JULICA DISCLAIMS ALL OTHER WARRANTIES, BOTH EXPRESS AND IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OF MERCHANTABILITY, ANY WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OF ACCURACY OF INFORMATION PROVIDED WITH RESPECT TO CERTIFICATES ISSUED BY JULICA, THE CRL, AND ANY PARTICIPANT'S OR THIRD PARTY'S PARTICIPATION IN THE JULICA PKI, INCLUDING USE OF KEY PAIRS, CERTIFICATES, THE CRL OR ANYOTHER GOODS OR SERVICES PROVIDED BY JULICA TO THE PARTICIPANT.

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1 OF THIS CPS, JULICA DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE.

JuliCA does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time. A fiduciary duty is not created simply because an individual or entity uses JuliCA's services.

9.8. Limitations of liability

TO THE EXTENT PERMITTED BY APPLICABLE LAW, JULICA SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL,

EX- EMPLARY OR PUNITIVE DAMAGES, INCLUDING BUT NOT LIMITED TO DAMAGES FOR LOST DATA, LOST PROFITS, LOST REVENUE OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY, INCLUDING BUT NOT LIMITED TO CONTRACT OR TORT (INCLUDING PRODUCTS LIABILITY, STRICT LIABILITY

AND NEGLIGENCE), AND WHETHER OR NOT IT WAS, OR SHOULD HAVE BEEN, AWARE OR ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY STATED HEREIN. JULICA'S AGGREGATE LIABILITY UNDER THIS CPS IS LIMITED TO $500.

9.9. Indemnities

9.9.1. Indemnification by CAs

No stipulation.

9.9.2. Indemnification by subscribers

No stipulation.

9.9.3. By relying parties

To the extent permitted by applicable law, Relying Parties shall indemnify JuliCA for their: (a) violation of any applicable law (b) breach of representations and obligations as stated in this CPS; (c) reliance on a Certificate that is not reasonable under the circumstances; or (d) failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

9.10. Term and termination

9.10.1. Term

The CPS becomes effective upon publication in the Repository. Amendments to this CPS become effective upon publication in the Repository.

9.10.2. Termination

This CPS and any amendments remain in effect until replaced by a newer version.

9.10.3. Effect of termination and survival

Upon termination of this CPS, Participants are nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates.

9.11. Individual notices and communications with participants

Unless otherwise specified by agreement between the parties, Participants shall use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12. Amendments

9.12.1. Procedure for amendment

JuliCA may change this CPS at any time in its sole discretion and without prior notice to Subscribers or Relying Parties. The CPS and any amendments thereto are available in the Repository. Amendments to this CPS will be evidenced by a new version number and date, except where the amendments are purely clerical.

9.12.2. Notification mechanism and period

JuliCA may provide additional notice (such as in the Repository or on a separate website) in the event that it makes any material changes to its CPS. JuliCA is responsible for determining what constitutes a material change of the CPS. JuliCA does not guarantee or set a notice-and-comment period.

9.12.3. Circumstances under which OID must be changed

No stipulation.

9.13. Dispute resolution provisions

No stipulation

9.14. Governing law

This CPS is governed by the laws of the Republic of Kenya,

9.15. Compliance with applicable law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information. JuliCA licenses its CAs in each jurisdiction that it operates where licensing is required by the law of such jurisdiction for the issuance of Certificates.

9.16. Miscellaneous provisions

9.16.1. Entire agreement

No stipulation.

9.16.2. Assignment

Relying Parties and Subscribers may not assign their rights or obligations under this CPS, by operation of law or otherwise, without JuliCA's prior written approval. Any such attempted assignment shall be void. Subject to the foregoing, this CPS shall be binding upon and inure to the benefit of the parties hereto, their successors and permitted assigns.

9.16.3. Severability

If any provision of this CPS shall be held to be invalid, illegal, or unenforceable, the validity, legality, or enforceability of the remainder of this CPS shall not in any way be affected or impaired hereby.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

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

9.16.5. Force Majeure

JuliCA shall not be liable for any default or delay in the performance of its obligations hereunder to the extent and while such default or delay is caused, directly or indirectly, by fire, flood, earthquake, elements of nature or acts of God, acts of war, terrorism, riots, civil disorders, rebellions or revolutions in the United States, strikes, lockouts, or labor difficulties or any other similar cause beyond the reasonable control of JuliCA.

9.17. Other provisions

No stipulation.

Appendix A: Definitions, Acronyms and References

Definitions

Automatic Certificate Management Environment (ACME): A communications protocol for automating interactions between Certificate Authorities and their Subscribers.

Activation Data: Data, other than keys, that is required to access or operate cryptographic modules (e.g., a passphrase or a Personal Identification Number or "PIN").

API: An interface that allows users to programmatically access the features of a system, application, or service.

Applicant: The natural person or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issuedto 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 Information is correct written by an accoun- tant, lawyer, government official, or other reliable third party customarily relied upon for such information.

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the audit opinion.

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of the BR.

Baseline Requirements (BR): CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates, available at https://cabforum.org/baseline-requirements-documents/

CAA: From RFC 3467 (http:tools.ietf.org/html/rfc3467): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis- issue."

CA Services: Services relating to the creation, issuance, or management of Certificates provided by JuliCA under this CPS.

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

Certification Authority (CA): 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. The term CA can depending on the context also refer to the infrastructure used by that organization to provide CA Services.

Client Authentication Certificate: A Certificate intended to be issued to individuals (as well as devices not acting in the capacity of a server), solely for the purpose of identifying that the holder of the Private Key is in fact the individual or device named in the Certificate's subject field.

Certificates: The Certificates that a JuliCA is authorized to issue pursuant to this CPS. See JuliCA Certificate.

Certificate Beneficiaries: any of the following parties:

(i) The Subscriber that is a party to the Subscriber or Terms of Use Agreement for the Certificate;

(ii) all Application Software Suppliers with whom the Root CA has entered into a contract for

inclusion of its Root Certificate in software distributed by such Application Software Supplier; and

(iii) 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.

Certification Practice Statement (CPS): This document.

Certificate Policy (CP): JuliCA's Certificate Policy.

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

Certificate Revocation List (CRL): A regularly updated time-stamped list of revoked Certifi- cates that is created and digitally signed by the CA that issued the Certificates.

CN: Common Name

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

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

CSPRNG: A random number generator intended for use in cryptographic system.

DBA: Doing Business As

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

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 rightto 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).

Domain Validated (DV) Certificate: A Certificate which verifies that the Subscriber controlsthe domain names and IP addresses included in the Certificate.

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

Fully-Qualified Domain Name (FQDN): A Domain Name that includes the labels of allsuperior nodes in the Internet Domain Name System.

FIPS: (US Government) Federal Information Processing Standard

JuliCA: JuliCA Trust Services LLC (a Delaware corporation).

JuliCA Affiliate: An entity that is controlled with or by or is under common control with JuliCA.

JuliCA: A CA operated by JuliCA in accordance with this CPS and listed in Section 1.3.1of this CPS.

JuliCA Certificate: A certificate issued by a JuliCA under this CPS.

JuliCA PKI: The JuliCA Public Key Infrastructure established, operated and maintained by JuliCA for publicly trusted certificates.

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.).

High Risk Certificate Request: A Request that the CA flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which may include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, names listed on the Miller Smiles phishing list or the JuliCA Safe Browsinglist, or names that the CA identifies using its own risk-mitigation criteria.

Identification and Authentication (I&A): The process for ascertaining and confirming through appropriate inquiry and investigation the identity and authority of a person or entity. See Section 3.2

Incorporating Agency: The government agency in the jurisdiction in which an entity is incorpo- rated under whose authority the legal existence of the entity was established (e.g., the government agency that issued the Certificate of Incorporation).

Information Security Team: JuliCA employees who belong to the Privacy & Security organi- zation.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

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.
Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it.

Key Pair: Two mathematically related numbers, referred to as a Public Key and its corresponding Private Key, possessing properties such that: (i) the Public Key may be used to verify a Digital Signature generated by the corresponding Private Key; and/or (ii) the Public Key may be used to encrypt an electronic record that can be decrypted only by using the corresponding Private Key.

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

NIST: (US Government) National Institute of Standards and Technology

OCSP: Online Certificate Status Protocol

OID: Object Identifier

Object Identifier: 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.

Operational Period: The intended term of validity of a JuliCA Certificate, including beginning and ending dates. The Operational Period is indicated in the Certificate's "Validity" field. See also Expire.

Organization Validated (OV) Certificate: A Certificate which includes the Subscriber's organization name.

Participants: The persons authorized to participate in the JuliCA PKI, as identified in Section 1.3. This term includes the JuliCAs, and each Subscriber and Relying Party operating under the authority of the JuliCA PKI.

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.

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 Cryptography: A type of cryptography, also known as asymmetric cryptography, that uses a unique Key Pair in a manner such that the Private Key of that Key Pair can decryptan electronic record encrypted with the Public Key, or can generate a digital signature, and the corresponding Public Key, to encrypt that electronic record or verify that Digital Signature.

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.

Qualified Auditor: A natural person or Legal Entity that meets the requirements of Section 8.2.

RA: See Registration Authority.

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.

Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governmentsas reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

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.

Registration Process: The process, administered by the CA or an RA, that a Subscriber uses to apply for and obtain a JuliCA Certificate.

Reissuance: The process of acquiring a new JuliCA Certificate and associated Key Pair to replacean existing JuliCA Certificate and associated Key Pair, prior to the Expiration of the existing JuliCA Certificate and associated Key Pair's Operational Period.

Relying Party: A recipient of a Certificate who acts in reliance on the Certificate and/or digital signatures verified using the Certificate.

Repository: An online accessible database in the JuliCA PKI containing this CPS, the CRL for revoked JuliCA Certificates, and any other information specified by JuliCA.

Request Token: A value derived in a method specified by the CA and used to demonstrate domain control.

Revocation: The process of requesting and implementing a change in the status of a Certificate from valid to Revoked.

Revoked: A Certificate status designation that means the Certificate has been rendered permanently Invalid.

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.

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 Subject commonName field.

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

Subscriber: The individual or organization that is named as the Subject of a Certificate and that has agreed to the terms of a Subscriber Agreement with JuliCA.

Subscriber Agreement: The contract between JuliCA and a Subscriber whereby the Subscriber agrees to the terms required by this CPS with respect to each Certificate issued to the Subscriber and naming the Subscriber as the Subject.

Subsidiary Company: A company that is controlled by or under common control of a Parent Company.

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 scopewithin which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

TLS: Transport Layer Security

Token: A hardware device (such as a smart card) used to store a Key Pair and associated Certificate and to perform cryptographic functions.

Validation Specialists: Someone who performs the information verification duties specified by these Requirements.

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

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

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

Wildcard Domain Name: A Domain Name consisting of a single asterisk character followed bya single full stop character (“*.“) followed by a Fully-Qualified Domain Name.

Acronyms

AICPA, American Institute of Certified Public

AccountantsCA, Certificate Authority

CAA, Certificate Authority

AuthorizationccTLD, Country Code Top-

Level Domain

CICA, Canadian Institute of Chartered

AccountantsCP, Certificate Policy

CPS, Certification Practice Statement

CRL, Certificate Revocation List

DBA, Doing Business As

DNS, Domain Name System

FIPS, (US Government) Federal Information Processing Standard

FQDN, Fully Qualified Domain Name

IM, Instant Messaging

IANA, Internet Assigned Numbers Authority

ICANN, Internet Corporation for Assigned Names and Numbers

ISO, International Organization for Standardization

NIST, (US Government) National Institute of Standards and Technology

OCSP, Online Certificate Status Protocol

OID, Object Identifier

PKI, Public Key Infrastructure

RA, Registration Authority

S/MIME, Secure MIME (Multipurpose Internet Mail Extensions) SSL Secure Sockets Layer

TLD, Top-Level Domain

TLS, Transport Layer Security

VOIP, Voice Over Internet

Protocol

Appendix B: Permissible Cryptographic Algorithms andKey Sizes

The following algorithms and key lengths are permissible for subscriber certificates:

Type	Permissible values
Digest Algorithm	SHA-256, SHA-384 or SHA-512RSA
	2048 or longer
ECC	NIST P-256, P-384

For RSA keys the public exponent must be an odd number equal to 3 or more.

Appendix C: JuliCA Certificate Profiles

This appendix sets out the Profiles of Certificates issued from JuliCAs. Fields and extensions not mentioned herein shall be set in accordance with RFC 3647.

JuliCA does not issue Certificates that contain a keyUsage flag, extendedKeyUsage value, Certificate extension, or other data not specified in the corresponding certificate profile unless it is awareof a reason for including the data in the respective Certificate.

Moreover JuliCA does not issue Certificates with:

1. Extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network), unless:
    1. such value falls within an OID arc for which the Applicant demonstrates ownership, or
    2. the Applicant can otherwise demonstrate the right to assert the data in a public context; or
2. semantics that, if included, will mislead a Relying Party about the certificate information verified by the JuliCA Internet Authority (such as including extendedKeyUsage value for a smart card, where the JuliCA Internet Authority is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

The following EKUs may be enabled:

- Server Authentication =1.3.6.1.5.5.7.3.1
- Client Authentication =1.3.6.1.5.5.7.3.2
- Secure E-mail EKU=1.3.6.1.5.5.7.3.4
- Code Signing EKU=1.3.6.1.5.5.7.3.3
- Time stamping EKU=1.3.6.1.5.5.7.3.8

Certificates, do not combine server authentication with code signing uses unless the uses are separated by application of Extended Key Uses ("EKU"s) at the intermediate CA certificate level that are reflected in the whole certificate chain.

Algorithm object identifiers

Effective 1 January 2016, JuliCA does not issue any new Subscriber certificates or Subordinate CA certificates using the SHA-1 hash algorithm.

Application of RFC 3647

For purposes of clarification, a Precertificate, as described in RFC 6962 – Certificate Transparency,is not considered to be a "certificate" subject to the requirements of RFC 3647 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Root CA Certificate

Field	Content
issuer	Matches subject
validity:not after	At least 8 but less or equal to 25 years after the certificate was issued or the validity:notBefore date – whichever is later.
subject	Contains countryName, organizationName and commonName. commonName attribute identifies the publisher, is unique, readable and in a language appropriate for the market of the respective CA.
extension:subjectKeyIdentifier	160-bit SHA-1 hash of subjectPublicKey [RFC 3647]
extension:basicConstraints	marked critical, cA is TRUE
extension:keyUsage	digitalSignature, keyCertsign and cRLSign are set, other bits are not set

Subordinate CA Certificate

Field	Content
validity:not after	Not later than notAfter date of signing certificate
subject	Contains countryName, organizationName and commonName
extension:subjectKeyIdentifier	160-bit SHA-1 hash of subjectPublicKey [RFC 3647]
extension:authorityKeyIdentifier	not marked critical, matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber not present
extension:certificatePolicies	not marked critical, contains at least one policyIdentifier
extension:basicConstraints	marked critical, cA is TRUE
extension:cRLDistributionPoints	not marked critical, contains HTTP URL of CRL service
extension:keyUsage	marked critical, digitalSignature, keyCertsign, and cRLSign bits are set, all other bits are not set
extension:authorityInfoAccess	not marked critical, contains at least one DistributionPoint containing a fullName of type uniformResourceIdentifier

Organization Validation TLS Certificates

Field	Content
validity:not after	Not more than 365 days after the later of validity:notBefore or the date the certificate was issued

Field	Content
subject	Contains countryName, locality, organizationName. May contain commonName, may contain organizationUnit. If the subject contains a commonName attribute, the value must be one of the values in the subjectAlternativeName extension.
extension:subjectKeyIdentifier	not marked critical, 160-bit SHA-1 hash of subjectPublicKey [RFC 3647]
extension:authorityKeyIdentifier	not marked critical, matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber not present
extension:certificatePolicies	not marked critical, contains at least one policyIdentifier
extension:basicConstraints	is either absent or cA is FALSE
extension:authorityInfoAccess	not marked critical, contains at least one DistributionPoint containing a fullName of type uniformResourceIdentifier of the issuing CA's OCSP responder
policyQualifiers:policyQualifierId	optional. if present, not marked critical and id-qt 1 [RFC 3647]
extension:cRLDistributionPoints	not marked critical, contains HTTP URL of CRL service
extension:subjectAltName	not marked critical, must contain at least one name and all names must be of type dNSName or iPAddress
extension:keyUsage	optional. if present, marked critical, digitalSignature bit must be set, keyExchange may be set, other bits should not be set
extension:extkeyUsage	not marked critical, must include either serverAuth or clientAuth, or both [RFC 3647]

Domain Validation TLS Certificates

Field	Content
validity:not after	Not more than 365 days after the later of validity:notBefore or the date the certificate was issued
subject	May be an empty sequence. May contain

	commonName. If the subject contains a commonName attribute, the value must be one of the values in the subjectAlternativeName extension.
extension:subjectKeyIdentifier	not marked critical, 160-bit SHA-1 hash of subjectPublicKey [RFC 3647]

Field	Content
extension:authorityKeyIdentifier	not marked critical, matches subjectKeyIdentifier of signing certificate; authorityCertIssuer and authorityCertSerialNumber not present
extension:certificatePolicies	not marked critical, contains at least one policyIdentifier
extension:basicConstraints	is either absent or cA is FALSE
extension:authorityInfoAccess	not marked critical, contains at least one DistributionPoint containing a fullName of type uniformResourceIdentifier of the issuing CA's OCSP responder
policyQualifiers:policyQualifierId	optional. if present, not marked critical and id-qt 1 [RFC 3647]
extension:cRLDistributionPoints	not marked critical, contains HTTP URL of CRL service
extension:subjectAltName	must contain at least one name and all names must be of type dNSName. Must be marked critical if Subject is empty, not marked critical otherwise.
extension:keyUsage	optional. if present, marked critical, digitalSignature bit must be set, keyExchange may be set, other bits should not be set
extension:extkeyUsage	not marked critical, must include either serverAuth or clientAuth, or both [RFC 3647]