DigiCert

Requirements for Third Party CAs and RAs

DigiCert, Inc.
Version 1.4.2
June 4, 2019

2801 N. Thanksgiving Way
Suite 500
Lehi, UT 84043
USA
Tel: 1-801-877-2100
Fax: 1-801-705-0481
www.digicert.com

1. **Introduction**.

1.1 **Overview**.

These Requirements for Third Party CAs and RAs apply to any third parties conducting either Certification Authority or Registration Authority functions ("Third-Party CA/RA") for Publicly Trusted certificates. Enterprise RAs are not Third-Party CA/RA organizations and are not subject to these requirements. Third-Party CA/RA organizations include, without limitation, organizations operating:

- a Processing Center application;
- an Enterprise Service Center application;
- any organization that controls issuance of Publicly Trusted certificates with the emailProtection EKU where the issuing CA is not Name Constrained;
- a GeoRoot;
- a US Federal PKI Shared Service Provider CA/RA;
- an Omniroot (e.g. a CA under the Baltimore Cybertrust Global Root); and
- any system that can allow the issuance of any Publicly Trusted certificates where DigiCert does not perform pre-issuance validation for the certificates.

Continued operation of a Third Party CA or RA equals agreement with updated terms of this policy document, which is subject to change as industry requirements evolve.

1.2 **Definitions**.

a. "**Applicable Requirements**" means these Requirements for Third-Party CAs and RAs, Final Guidelines adopted by the CA/Browser Forum, WebTrust Requirements, Mozilla Root Store Policy (including the Common CA Database Policy), Microsoft Root Store Policy, the US Federal PKI Policy, the DigiCert Certificate Policy, and other similar industry-wide standards.

b. "**EKU Constrained**" means the SubCA contains an Extended Key Usage ("EKU") and that value is not the anyExtendedKeyUsage EKU.

c. "**Name Constrained**" means the SubCA includes the Name Constraints extension as described in section 7.1.5 of the CA/Browser Forum's Baseline Requirements based on the content of the Extended Key Usage extension.

d. "**Public codeSigning-Enabled**" means the subCA:
   i. Contains no Extended Key Usage value, OR
   ii. Contains the anyExtendedKeyUsage EKU, OR
   iii. Contains the codeSigning EKU AND is not Name Constrained.

e. "**Public serverAuth-Enabled**" means the subCA:
   i. Contains no Extended Key Usage value, OR
   ii. Contains the anyExtendedKeyUsage EKU, OR
   iii. Contains the serverAuth EKU AND is not Name Constrained.

f. "**Publicly Trusted**" means the operations of the Third-Party CA/RA involve the issuance of Certificates that chain to a SubCA that is signed by roots present in the Common CA Database (CCADB) with a status of "not removed" for EITHER Microsoft or Mozilla.

2. **Compliance with Applicable Requirements**.

a. Third-Party CA/RA organizations SHALL comply with all Applicable Requirements. Failure to comply with Applicable Requirements for any Publicly Trusted SubCA MAY result in immediate revocation of any and all of Third-Party CA/RA's SubCAs at DigiCert's sole discretion.

b. These Requirements and DigiCert's audit rights herein survive termination of any agreement with the Third-Party CA/RA (i) as long as ANY Publicly Trusted SubCA is either valid or in an un-revoked state or (ii) for three (3) years following termination of such agreement, whichever period is longer.

c. Effective January 1, 2018 DigiCert requires that ALL new Publicly Trusted SubCAs MUST be EKU Constrained.

d. Effective April 1, 2018 DigiCert requires that ALL existing Publicly Trusted SubCAs that are not EKU Constrained cease certificate issuance. All existing Publicly Trusted SubCAs that are not EKU Constrained MUST be revoked no later than December 31, 2018.

e. On at least an annual basis, ALL Third-Party CAs/RAs MUST (i) review and update their Certification Practice Statements/Registration Practices Statements and (ii) indicate that this has happened by incrementing the version number and adding a dated changelog entry, even if no other changes are made to the document.

f. Third-Party CA/RAs are responsible for ensuring compliance with these Requirements for Third-Party CAs and RAs by their customers who control issuance of certificates with the emailProtection EKU where the SubCA is not Name Constrained. This obligation includes but is not limited to ensuring customer adherence to the Applicable Requirements and all Audit Requirements.

3. **Audit Requirements**.

a. For ALL Third-Party CA/RAs performing any CA or RA functions for (i) any Publicly Trusted SubCAs or (ii) any SubCAs cross-signed to the US Federal PKI via the Shared Service Provider program, DigiCert requires one of the following audits:
   i. WebTrust "Principles and Criteria for Certification Authorities - Version 2.0" (for Federal PKI, as supplemented by the Annual Review Requirements, https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/annual-review-requirements.pdf) ; or
   ii. ETSI EN 319 411-1 (LCP, NCP, or NCP+); or
   iii. ETSI EN 319 411-2 (QCP-l, QCP-l-qscd, QCP-n, or QCP-n-qscd).

b. In addition to any other audits required in this section, for any Third-Party CA/RA managing Publicly Trusted SubCAs that are Public serverAuth-Enabled, DigiCert requires one of the following audits:
   i. WebTrust "Principles and Criteria for Certification Authorities – SSL Baseline with Network Security - Version 2.2"; or
   ii. ETSI EN 319 411-1 (LCP and (DVCP or OVCP)) or (NCP and EVCP); or
   iii. ETSI EN 319 411-2 (QCP-w).

c. In addition to any other audits required in this section, for any Third-Party CA/RA managing Publicly Trusted SubCAs that are Public codeSigning-Enabled, DigiCert requires the following audit:
    i. WebTrust for Certification Authorities - Publicly Trusted Code Signing Certificates - Version 1.0; or
    ii. ETSI EN 319 411-1 (LCP, NCP, NCP+, or OVCP); or
    iii. ETSI EN 319 411-2 (any form).

d. In addition to any other audits required in this section, for any Third-Party CA/RA managing Publicly Trusted SubCAs that allow Extended Validation SSL/TLS, DigiCert requires one of the following audits:
    i. WebTrust "Principles and Criteria for Certification Authorities - Extended Validation SSL 1.4.5"; or
    ii. ETSI EN 319 411-1 (NCP and EVCP).

e. In addition to any other audits required in this section, for any Third-Party CA/RA managing Publicly Trusted SubCAs that allow Extended Validation code signing, DigiCert requires the following audit:
    i. WebTrust Principles and Criteria for Certification Authorities – Extended Validation Code Signing – Version 1.4; or
    ii. ETSI EN 319 411-1 (NCP and EVCP).

4. **Audit Scheme Updates**.

For any audit requirements above,

a. All Third-Party CA/RA organizations MUST provide annual audits using the applicable audit scheme as required at aka.ms/auditreqs and https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/ or equivalent published policies such that (i) the latest version of an audit scheme is used if the effective date of that version is on or before the first date of the period of the audit (or of the date of the point in time audit), or (ii) the next earlier version of an audit scheme is used if the effective date of the latest version is after the first date of the period of the audit (or of the date of the point in time audit).

b. Third-Party CA/RA organizations MUST stay current with and comply with these and any other changes to audit requirements associated with Publicly Trusted SubCAs or SubCAs cross-signed to the US Federal PKI via the Shared Service Provider program.

c. All Third-Party CA/RA organizations MUST review with DigiCert the scope of CAs and Operations under audit before scope is finalized with their respective auditors.

5. **Auditor Licensing/Qualification**.

   Third-Party CA/RA organizations MUST engage only auditors appropriately licensed to perform the required audits and approved in advance by DigiCert.

6. **Audit Continuity**.

   All audits specified in Section 3 above are subject to Period-in-Time Audits. The period during which the SubCA issues certificates SHALL be divided into an unbroken sequence of audit periods. Audit reports SHALL be provided as long as the SubCA certificate is valid, even if the SubCA has ceased issuance or has not issued any certificates in the audit period. The audit requirements specified herein apply even if a SubCA has been revoked during the audit period.

7. **Audit Period**.

   Period-in-Time audits MUST NOT be for a period less than three (3) months and must not exceed one (1) year in duration.

8. **Audit Reporting**.

   The SubCA MUST make its audit report publicly available.

   a. Reports must be provided no later than three (3) months after the end of the Audit Period. In the event of a delay beyond this three-month reporting requirement, the SubCA SHALL provide an explanatory letter signed by their qualified auditor. An audit reporting delay in excess of one (1) additional month beyond the above three-month requirement is considered an Audit Failure.

   b. DigiCert may post a copy of the audit report to appropriate public forums as designated by Mozilla and to other relying parties upon request.

9. **Audit Failures**.

   Any Audit Failure MAY result, at DigiCert's sole discretion, in DigiCert's immediate revocation of the SubCA. An "Audit Failure" will result from any audit:

   a. receiving a qualified opinion; OR

   b. conducted with an earlier version of an audit scheme than required; OR

   c. conducted by an auditor failing to meet the Auditor Licensing/Qualification requirements or not approved in advance by DigiCert; OR

   d. failing to meet the Audit Continuity requirements; OR

   e. conducted for a period shorter or longer than the allowed Audit Period requirements; OR

   f. not provided by the Third-Party CA/RA within the required Audit Reporting timeframe.

10. **Audit Failure Remedy**.

    At DigiCert's sole discretion, a Third-Party CA/RA with an Audit Failure MAY be offered the opportunity to correct such failure in lieu of immediate revocation of the SubCA. If offered, the remedy process is as follows:

    a. Within 15 days of notice of an Audit Failure, the Third-Party CA/RA must schedule a meeting with DigiCert to discuss the failure and the detailed plan and schedule for remediation.

    b. Within no greater than 45 days of notice of an Audit Failure, the Third-Party CA/RA must produce a signed engagement letter for a "Point-in-Time" audit with a scope that explicitly covers each element of the remediation plan and is conducted in accordance with Section 3.

    c. The Point-in-Time audit MUST be started no greater than 30 days from the scheduled remediation completion date. All audit requirements in Sections 3 through 8 apply to the Point-in-Time Audit.

11. **Certificate Checking**.

    a. Third-Party CA/RAs SHALL implement systematic certificate compliance checking such as CertLint (https://github.com/awslabs/certlint) for all Public serverAuth-Enabled or all Public codeSigning-Enabled certificates to confirm issued certificates comply with the Applicable Requirements.

    b. Third-Party CA/RAs are responsible for compliance with the Applicable Requirements for ALL certificates. This includes but is not limited to:

        i. monitoring certificate compliance;
        ii. revoking non-compliant certificates, if necessary and within designated timeframes, in accordance with the Applicable Requirements;
        iii. implementing timely corrective action to address compliance failures; and
        iv. reporting non-compliant certificates and corrective action to DigiCert and in accordance with the Mozilla reporting requirements (https://wiki.mozilla.org/CA/Responding_To_An_Incident#Incident_Report).

12. **DigiCert Audits**.

    In addition to the required audits detailed in Section 3, effective April 1, 2018 DigiCert requires that Third-Party CA/RA organizations provide, at no less than monthly intervals, copies of ALL issued certificates from (i) any Public serverAuth-Enabled or Public codeSigning-Enabled SubCAs OR (ii) any SubCAs cross-signed to the US Federal PKI via the Shared Service Provider program. The completeness and accuracy of the provided certificates must be confirmed by the Third-Party CA/RA organization's independent auditor as part of the audit specified in Section 3.a.

13. **System Updates**.

    DigiCert periodically releases mandatory compliance patches for its products, including without limitation, its Processing Center platforms. Third-Party CA/RA organizations must install mandatory patches within the specified timeframe communicated with delivery of the patch. Failure to install mandatory patches within the specified timeframe may result, at DigiCert's sole discretion, in DigiCert's immediate revocation of all relevant SubCAs.

14. **Annual Training**.

All Third-Party CA/RA personnel with authentication or issuance duties, or with CA/RA system access, must complete DigiCert-provided compliance training and successfully pass a mandatory exam at least annually.

15. **Additional US Federal PKI Requirements**.

In addition to the requirements in this Section, all US Federal Shared Service Provider (SSP) Customers MUST:

a. Execute and maintain RA Agreements with DigiCert and corresponding Registration Practice Statements based on https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-registration-auth-agree-template.docx.

b. Annually submit to DigiCert all materials required to comply with sections 5.1, 5.2, 5.5 and 5.6 at https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/annual-review-requirements.pdf.

16. **SubCA Path Length**.

As of June 1, 2018, no SubCA operated by a Third-Party CA/RA MAY contain a pathLenConstraint > 0, with the following exceptions:

a. The Third-Party CA/RA presents, and DigiCert accepts, an exception request due to a widely deployed application that requires a certificate chain with a specific path length due to CA pinning, or

b. The Third-Party CA/RA presents, and DigiCert accepts, an exception request due to published national regulations, such as data privacy, for an application that is required to operate within a geographic boundary not served locally by DigiCert and, due to population-level issuance volumes, issuing CAs are generated in bulk.

c. A Third-Party CA/RA currently operating under the GeoRoot or Omniroot Programs.

Any Third-Party CA with a CA certificate that has pathLenConstraint > 0 MUST obtain DigiCert's written pre-authorization before creating any new SubCA certificate and MUST provide DigiCert with a copy of the new sub CA certificate within 24 hours of its creation.