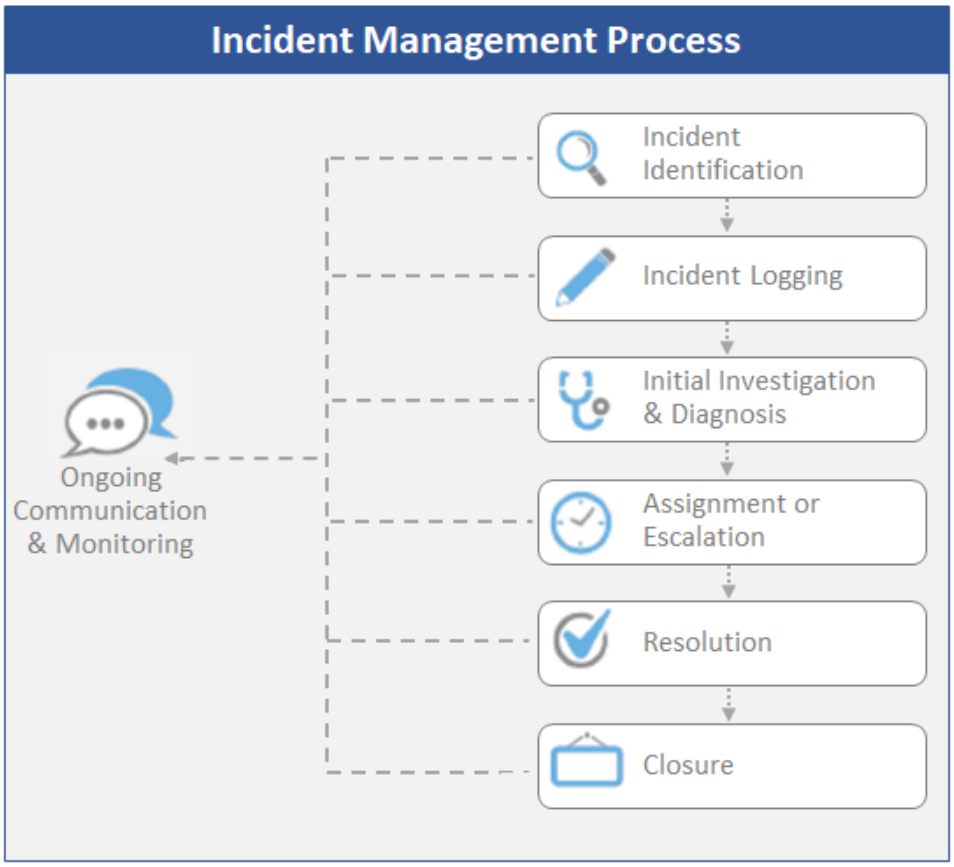
Values & Benefits Statement

What broad value and benefits does your CA provide Apple? Please provide as much detail covering as many areas as possible.

- How do your processes ensure timely and transparent reporting of compliance incidents?

Upon detection or reporting of an incident, DigiCert creates a slack channel dedicated to investigating and resolving the issue. Participants include the CTO, CPO, CISO, EVP of Support, VP of compliance, VP of engineering, and other key stakeholders. Concurrent to assembling the incident response team, DigiCert initiates the process shown in the diagram below.



The goal is to determine the root cause and remediate within 24 hours of an event.

Each incident has set roles that operate to ensure efficiency in the investigation and report. The incident commander controls the incident and makes decisions on priorities and severity. This is usually the CISO or VP of Compliance. The Incident Manager tracks progress and ensures we hit key timelines for filing and updating bugs. The Communication Manager manages any customer comms required and ensures that we maximize notice to impacted third parties. Finally, the cross-functional subject matter experts remediate and test the fix to ensure no additional issues were introduced and the root cause was investigated and resolved.

DigiCert has set timelines for managing the incident. The violation assessment and impact analysis occur within 24 hours of the report. Critical stop gaps are immediately enabled to prevent further mis-issuance. For less critical issues, the team attempts to implement the stop-gap within 24 hours but no more than 48 hours. Long-term fixes are implemented within two weeks.

- How does your organization's internal processes reflect PKI industry standards for annual audits and policy maintenance?

DigiCert has an external annual Webtrust and SOC2 audit and performs continuous internal audits on systems and operations. DigiCert has a policy authority that oversees all policy changes and ensures updates to policies are made at least annually.

- How involved is your organization in the CA/B Forum, and how do you contribute to the CA community?

DigiCert is very involved in the CA/B Forum. DigiCert chairs the Code Signing WG, the S/MIME WG, and the Validation sub-committee. DigiCert has two full-time representatives that participate on both the mailing list and in-person meetings.

- Does your organization's future goals, as a CA, align with the goals of the CA community?

Yes. DigiCert is dedicated to the security of the Internet and betterment of PKI. As part of this dedication, DigiCert maintains the only non-Google source code for CT logs.

- How does your organization align with Apple's policy on privacy?

Yes. DigiCert values the privacy of our customers and users. Personal information obtained from an applicant during the application or identity verification process is considered private information if the information is not included in a Certificate. DigiCert will only use private information after obtaining the subject's consent or as required by applicable law or regulation. All Subscribers must consent to the global transfer and publication of any personal data contained in a Certificate.

- Does your organization provide a current security policy to protect Apple users?

Yes. Our information security policy protects sensitive information from both accidental and intentional disclosure.

- Does your organization keep user information private from third party vendors?

DigiCert employees and contractors are expected to handle personal information in strict confidence and meet the requirements of US and European law concerning the protection of personal data. All sensitive information is securely stored and protected against accidental disclosure

CA Lifecycle Management

Apple is looking to have CAs more regularly replace root certificates and key material, which helps ensure that keys are generated, protected, and used according to the most effective security practices currently known. As this may involve CAs replacing roots and keys created under older security standards and practices with new key material, Apple would like to understand CAs' current and planned approaches to CA lifecycle management. Please describe your CA Lifecycle Management plan. Please provide a link to an externally hosted document.

A detailed plan should be able to answer questions such as:

- How many Roots are in active operation?

Seventeen:

CommonName	Certificate Serial Number	Valid From (GMT)	Valid To (GMT)
Baltimore CyberTrust Root	020000B9	5/12/2000	5/12/2025
DigiCert Assured ID Root CA	0CE7E0E517D846FE8FE560FC1BF03039	11/10/2006	11/10/2031
DigiCert Global Root CA	083BE056904246B1A1756AC95991C74A	11/10/2006	11/10/2031
DigiCert High Assurance EV Root CA	02AC5C266A0B409B8F0B79F2AE462577	11/10/2006	11/10/2031
DigiCert Assured ID Root G2	0B931C3AD63967EA6723BFC3AF9AF44B	8/1/2013	1/15/2038
DigiCert Assured ID Root G3	0BA15AFA1DDFA0B54944AFCD24A06CEC	8/1/2013	1/15/2038
DigiCert Global Root G2	033AF1E6A711A9A0BB2864B11D09FAE5	8/1/2013	1/15/2038
DigiCert Global Root G3	055556BCF25EA43535C3A40FD5AB4572	8/1/2013	1/15/2038
DigiCert Trusted Root G4	059B1B579E8E2132E23907BDA777755C	8/1/2013	1/15/2038
DigiCert SMIME ECC P384 Root G5	053F6EA00601727DED3FC3A3B6A3D6EF	1/15/2021	1/14/2046
DigiCert TLS RSA4096 Root G5	08F9B478A8FA7EDA6A333789DE7CCF8A	1/15/2021	1/14/2046
DigiCert TLS ECC P384 Root G5	09E09365ACF7D9C8B93E1C0B042A2EF3	1/15/2021	1/14/2046
DigiCert SMIME RSA4096 Root G5	05F6BA04238346CB7D5CE6B95BBA1C55	1/15/2021	1/14/2046
DigiCert RSA4096 Root G5	08BFA26F9A3F3365A2ACF0A638C40170	1/15/2021	1/14/2046
DigiCert ECC P384 Root G5	0DF3D93765A379C59566EA92E2244F34	1/15/2021	1/14/2046
DigiCert Client ECC P384 Root G5	064FA6A62829141F0E9D8362E1175E3A	1/15/2021	1/14/2046
DigiCert Client RSA4096 Root G5	04C8FC03A854EB98A09B02883C66A3C0	1/15/2021	1/14/2046

- How many Roots are planned for?

Seventeen.

- How far in advance of a Root expiring is its replacement signed?

As of now, ~15 years. Future plans will be highly dependent on trust store policies, but currently the pattern is roots with 25 year validity with a new set being created approximately ev **DigiCert TLS ECC P384 Root G5** ery 10 years.

- How are cross-signatures handled between generations?

We will cross-sign with previous generation roots as necessary for ubiquity.

- What trust purposes is each Root created to serve?

As of DigiCert G5 root certificates, we use separate roots for TLS, Client, and SMIME. There is also a set of G5 general purpose roots.

- How comprehensive is the PKI with regards to algorithmic and key size usage?

See section 6.1.5 and 7.1.3 of the DigiCert CPS.

- How quickly are customers transitioned from one Root to another?

Due to the time it takes to gain ubiquity among trust store operators, the current minimum time required to roll out a new root is approximately 3 years, with 5 years being more realistic to attain high enough saturation levels among end user clients.

- When are new Roots submitted to the Apple Root Program for inclusion?

We submit new roots to trust store operators as soon as we have generated a new batch of roots, issuing subCAs and example end entity certificates signed by the new hierarchy.

- When can deprecated Roots be removed from the Apple Root Program?

When all end entity certificates under that root hierarchy are no longer active.

Linting

If linting is performed by your CA, please provide a detailed description of your linting configuration and playbooks. If linting is not performed by your CA, please confirm that and outline any plans you have for introducing linting into your processes. Please provide a link to an externally hosted document.
A detailed description should be able to answer questions such as:

- Do you perform pre-issuance linting?

Yes

- If a pre-issuance linter detects an issue, what steps are performed?

The certificate is blocked from reaching the CA and rejected.

- Do you regularly run linters post-issuance?

Yes

- What linters do you run?

DigiCert uses digi-lint (an internal linter) and zlint.

- How often do you update linters and/or linter configurations?

Linters are updated continuously as new updates are made. Our internal linters are updated as needed to support new requirements changes.

- Do you disable any lints from any linters? If so, what lints? How do you decide what lints to disable?

Only lints unrelated to the certificate profile we are issuing are disabled from the linters at any given time. No lints are permanently disabled from any linter.

- What is your process for reviewing or contributing new lints?

New lints are contributed when it is determined they will have wide industry applicability and fit the charter of public lint libraries. When new lints are added externally, we run all lint updates through a set of previously issued certificates to confirm compatibility with our existing processes.

- What is your process for executing lints on all of your valid certificates?

We run pre-issuance and post-issuance lints on all issued certificates.