June 28, 2023

Entrust Root Embedding Statements

This document addresses Entrust's values and benefits statement, CA lifecycle management, linting, customer and change management, ACME domain validation and ACME certificate issuance as requested by Apple to support inclusion of new root certificates in Apple products.

Values & Benefits Statement

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

Entrust searches issues through pre-linting, post-linting, review of other CA incidents, and following the ecosystem. We always try to implement changes to ensure that the same error does not occur in the future. We always try to be transparent and consider the interests of the broader ecosystem.

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

Entrust has been a public CA since 1999. This was before there were WebTrust audit criteria for PKI. Nevertheless we had third party audits and were the first CA to have the WebTrust for CA audit and the WebTrust for EV audit. Entrust follows the policy changes from all of our embedding partners to ensure we address their requirements. We implement all CA/Browser Forum ballots in a timely manner to meet effective dates. We also update our CPS on a regular basis to ensure policy and requirements changes are reflected in our practices.

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

Entrust is a founding member of the CA/Browser Forum. Entrust has chaired the Forum for 8 years. Entrust did step back from the Forum for 2-years due to IP concerns, but still stayed active by monitoring all public statements and sending in questions with any concerns. Currently we have one member who is vice-chair of the CA/Browser Forum and another who is vice-chair of the Code Signing working group. Our active members all participate with Server, Code Signing, S/MIME and Network Security working groups.

Entrust helped to develop the certificate management policy defined in the Verified Mark Certificate (VMC) Requirements. Entrust continues to support Apple, Google and the AuthIndicators Working Group for the progression of VMC and the implementation of Marked Certificates (MC).

Entrust has also helped transform the CA Security Council to become the PKI Consortium. This is a group of leading organizations that are committed to improve, create and collaborate on generic, industry or use-case specific policies, procedures, best practices, standards and tools that advance trust in assets and communication for everyone and everything using Public Key Infrastructure (PKI) as well as the security of the internet in general.

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

Entrust has expanded our CA business to include most public trust certificates required by our customers. We have added private trust certificates to address use cases which public trust does not address. We have also added in signing services to generate Subscriber key pairs and securely protect their private keys through their lifecycle.

Entrust is also a manufacturer of the nShield HSM product line which helps to support CAs, time-stamping authority, signing services, and subscriber key generation and protection.

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

Like Apple, as a business and employer, it is necessary for Entrust to collect, store, and process personally identifiable information (PII) about our employees, contingent workers, customers, suppliers and other third parties with whom we engage to provide products or services on our behalf. In order to comply with applicable laws governing data protection, we have a data privacy program and a Global Personal Data Protection Policy. Further information about our program and policies relating to privacy are available at https://www.entrust.com/legal-compliance/data-privacy.

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

Entrust provides trust to protect Apple users by deploying a CA which meets or exceed the industry standards. Entrust makes certificate status available all users through CRL and OCSP responses. In addition, Entrust issues certificates to support Apple eSIM.

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

As noted above, Entrust handles all user information in accordance with applicable laws and our privacy program and policies. We do not share our customer information with any third party vendors except as permitted, for example, with express consent.

CA Lifecycle Management

How many Roots are in active operation?

Entrust has five (5) roots embedded under the Entrust brand and four (4) roots embedded under the AffirmTrust brand in Apple products.

How many Roots are planned for?

Entrust plans to migrate to the following six (6) dedicated roots:

- 4 Entrust TLS roots supporting OV/RSA, EV/RSA, OV/ECC and EV/ECC
- 1 AffirmTrust root supporting DV/RSA
- 1 Entrust S/MIME RSA root

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

The new 4096 and P-384 roots have an expiry of 25 years after issuance. We believe this will address the full period the roots would be trusted by our embedding partners for as long as the crypto remains secure and provide cross-certification for ubiquity to new trusted roots.

How are cross-signatures handled between generations?

The new roots will be cross-signed by 2048-bit RSA roots, as such, the cross-certificates will expire before the end of 2030.

What trust purposes is each Root created to serve?

Dedicated trust services will support TLS (DV/RSA), TLS (OV/RSA), TLS (EV/RSA), TLS (OV/ECC), TLS (EV/ECC), and S/MIME (RSA).

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

For TLS we will have 4096-bit RSA roots which will support 2048, 3072 and 4096-bit RSA TLS certificates. We will also have ECC P-384 roots which will support ECC P-256 and P-384 TLS certificates.

For S/MIME we will have 4096-bit RSA root which will support 2048, 3072 and 4096-bit RSA S/MIME certificates.

How quickly are customers transitioned from one Root to another?

There is no formula to answer this question. In the past, roots were deployed to address cryptographic concerns. We started with 1024/SHA1, then 2048/SHA1, then 2048/SHA256. These roots would allow a CA to progress most of the way to the end of 2030. Deployment of the roots would be based on how long it took for the roots to achieve ubiquity with the goal of providing most subscribers with the shortest certificate chain.

With the new Mozilla proposed frequency of expiring roots, this proposed schedule now must be escalated. Entrust will have an issue moving to a new root, if it has not been embedded and the software does not support the legacy root providing cross-certification.

For TLS we would not like to migrate to a new root until it has gotten through the Apple, Google, Microsoft, and Mozilla embedding processes, and the root has been supported by the CT logs.

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

Entrust is currently going through the process to submit the dedicated TLS and S/MIME roots in 2023.

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

Roots can be deprecated once their replacement has been embedded in Apple software. The assumption being that the deprecated root will remain in Apples old software and that the new root will be cross-certified by the old root.

Linting

Do you perform pre-issuance linting?

Entrust performs pre-issuance linting for all TLS certificates using zlint.

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

If a pre-issuance linter detects an issue, then the certificate will not be issued. If the issue corresponds to a pre-certificate, then the pre-certificate will be revoked.

Do you regularly run linters post-issuance?

Post-issuance linting is performed on all Subscriber certificates including TLS, S/MIME, Code Signing, Document Signing and VMC. Third party linting software is used if it is designed to support a specific certificate type. In addition, post-issuance linter has a certificate profile for every CA including static content which is expected in each field. For variable content, post-linting will check against the source to ensure the correct content is in the certificate. Other checks are added to post linting such as weak key and CT logging.

What linters do you run?

Certlint, Cabint and zlint, plus our own linter designed to lint for specific requirements for each issuing CA.

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

Third party linting software is updated within 3 months from release. Entrust post-linting software is updated with each certificate management software major release, so approximately 3-4 time per year.

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

Pre-issuance linters run to check for errors and will not issuance a certificate with an error. No errors are disabled. Warnings are ignored.

What is your process for reviewing or contributing new lints?

TLS pre-issuance linting appears to be mature, but Entrust has contributed to help detect known issues where Entrust has reported an incident. For instance we proposed an update to zlint for Close Primes weak key.

Entrust may get more involved with contributing to S/MIME linting.

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

Post-linting is run on all valid certificates within 30 minutes of issuance. Post-linting may also be run all unexpired certificates, when the post-issuance linter has been updated and we check to see if any old certificates have been miss-issued.

Entrust has found that post-issuance linting detects most new issues for miss-issued certificates. Since the error is found within 30 minutes of issuance, it is much easier to have the certificate revoked before it is in use by the Subscriber. Also, the more post-linting you perform, the detected incidents you will have in the future.

Customer and Change Management

Do you provide public resources about upcoming changes?

No, with the exception of notification of ecosystem changes through a blog.

Entrust issues primarily to Enterprise customers. These customers have an account, 2-factor login, dashboard and memos. Upcoming changes of significance are provided to the customers through the memo feature. Non-enterprise customers would find out about any change with impact at renewal time or through the blog.

How do you communicate to existing subscribers about upcoming changes?

Customer account memo feature.

How do you ensure that you have current and correct contact information for Subscribers?

Subscribers are our customers. We need to be able to reach out to them on a continuous basis for verification and re-verification. For all customer contacts we have email and phone numbers. In addition we have their corporate number.

How is feedback gathered regarding potential changes under discussion in the industry?

Feedback is generally gathered by a customer survey.

ACME Domain Validation

Do you support domain validation compliant with the ACME protocol?

No.

ACME Certificate Issuance

Do you support certification issuance through the ACME protocol?

Yes.