Trust Service Provider Technical Best Practices

Considering the EU eIDAS Regulation (910/2014)

This document has been developed by representatives of
Apple, Google, Microsoft, and Mozilla.

Document History

Version	Date	Notes
1.2	2018-05-22	Initial external version.

Background

EU Regulation (910/2014) on electronic identification and trust services for electronic transactions in the internal market, the "eIDAS Regulation", sets the broad framework under which Trust Service Providers (TSP) must operate and how they are supervised. Recital 34 in the Regulation (http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG) indicates that EU Member States should exchange information on those providers' "best practices in the field" without setting specific standards. Recognizing that "best practices in the field" change over time, Recital 67 in the Regulation considers industry-led initiatives to define appropriate best practices. Through complementary Implementing Acts, Section 3 of the Regulation sets out the European Commission's right to specify security standards for qualified trust service providers, especially under Article 24. The purpose of this document is to describe the principles and concepts behind current security best practices for Trust Service Providers that are not covered by any Implementing Acts on electronic trust services.

Incident Handling

An incident is any event, situation, or circumstance that has, could have, or might cause the TSP to operate outside the requirements laid down by the Certification Authorities/Browsers (CA/B) Forum Baseline Requirements or Extended Validation (EV) Guidelines, Root Store Policies, Audit Requirements, or other security relevant obligation.

An incident should be reported to Root Store Operators as soon as practicable after discovery - and in no cases later than 72 hours after initial discovery, and followed up with a detailed postmortem. Individual Root Store Policies may have requirements for the information to be included in reports and/or postmortems as well as timeframes and delivery methods for this additional reporting.

Reporting an incident to a National Accreditation Body, Supervisory Body, Auditor, or other party is not a substitute for the TSP's responsibility to Root Store Operators, which may take action independent from these bodies according to their policies and procedures.

Secure Development and Deployment Practices

TSP's software and systems are security critical and must be developed, deployed, and updated accordingly.

Software developed directly by or for the TSP must follow industry best practices for design, design review, coding, code review, and change control. Static analysis, fuzzing, and code audit should be conducted during all stages of development.

Software developed by a third party, including open source software, must be used in accordance with a documented procedure to ensure security updates are applied quickly, and no undesired or unexpected behaviour is introduced by upstream changes. TSPs are responsible for the secure and correct operation software they use, whether developed by themselves or not.

All software deployed by a TSP must be subject to third party penetration testing, with a documented procedure to ensure any identified security issues are rapidly and properly fixed.

TSPs are subject to compliance with a constantly evolving set of requirements and standards. In addition to adhering to these secure development practices, TSP software must be developed and updated with a frequency that keeps pace with these requirements. Inability to update software due to insufficient engineering resources, contractual barriers, reprioritization, or other delay is not a valid reason for non-compliance.

System Security

TSPs must operate digital infrastructure in accordance with all industry best practices, including:

- Trusted roles and separation of duties
- Access controls
- Monitoring
- Audit logging
- Patching
- Network security
- Backup and recovery
- Protection of private keys

Intermediate CAs

Root Store Policies may impose requirements on Intermediate CAs that must be followed. Such requirements may include, but are not limited to:

- The types of end entity certificates that can be issued by an intermediate CA, including by technical means such as requiring the inclusion of Extended Key Usage (EKU) values restricting an intermediate CA certificate to a single purpose.
- Limitations on the storage and use of intermediate CA keys, e.g. requirements for keys to be stored 'offline'.
- Disclosure of all intermediate CA Certificates chaining up to a CA Certificate included in a Root Store.
- Auditing of all intermediate CA Certificates chaining up to a CA Certificate included in a Root Store.
- Restrictions or conditions on the transfer of an intermediate CA to a different organization.

CA Certificate Lifecycle

Once a CA Certificate is included in a Root Store, Root Store Policies may impose ongoing requirements on the CA Certificate, even if the TSP requests that the CA Certificate be removed from the Root Store. For example, a Root Store may require that a TSP continues to follow audit and other Root Store Policy requirements with respect to the CA Certificate until the TSP has ceased all use of the CA Certificate and provides audited proof that the private key has been destroyed.

Certificate Transparency

By issuing a Publicly Trusted Certificate, all data within that certificate is considered to be publicly published, whether or not such certificates are used on a publicly accessible network service. TSPs may be required to disclose the entire contents of certificates they have issued, including, but not limited to, investigations into misissuance or as part of disclosure requirements using technology such as Certificate Transparency (CT). TSPs should thus limit their Certificate Profiles to only include data which is publicly relevant and appropriate.

Certificate Format and Issuance

Trust Service Providers should have automated procedures in place to ensure technical and policy compliance of each certificates' tbsCertificate sequence before signing: routine rejection or revocation of non-complying certificates after issuance is not a substitute for pre-issuance checks, and such certificates will be considered mis-issued even if immediately revoked. Certificates must conform to RFC 5280, and Trust Services Providers should use automated tooling such as "certlint" (https://github.com/awslabs/certlint) to ensure conformance. Issuance of a certificate which fails to conform to RFC 5280 will be treated as a mis-issuance event even if the information it contains is otherwise correct.

Certificate Agility

The web is a rapidly moving ecosystem with evolving standards. As security threats evolve, Root Store Operators may stop accepting certificates that are still within their validity period even if they were adhering to current requirements at time of issuance. To minimise ecosystem disruption in such cases, Trust Services Providers should:

- Issue website authentication certificates with as short a validity period as possible (and in no case longer than the maximum imposed by bodies such as the CA/B Forum and Root Store Policies).
- Ensure their customers are aware of changes in standards or requirements as soon as possible and help them obtain new certificates well in advance of any cutoff date.

Issuance of a certificate which uses a forbidden technical or procedural method (e.g. a key size, hash algorithm, validity length, or domain verification method) after the cutoff date for that method will be considered mis-issuance even if there is a pressing customer requirement for such issuance.

As the TSP ecosystem is dynamic, and may suddenly change in response to security incidents or market unpredictability, TSPs can take steps to greatly minimize the risk and disruption to users by supporting standardized methods of issuance and enrollment, particularly by automatic means. By supporting standard enrollment protocols for website certificates, TSPs can help ensure minimal disruption through facilitating an open market capable of rapid response to the changing security landscape.

Test and Failover Environments

TSPs should maintain a test environment that mirrors their production environment but does not have access to production systems or CA key material. The test environment provides a safe place to test issuance processes, controls and software changes without risking the integrity of the production PKI and should be used to validate technical and procedural changes before implementing in production.

Failover and disaster preparedness environments must have the same security controls, patching regime etc as the TSP's primary production environment.

Audit Requirements

Audit Periods must be no greater than one year. There must not be gaps in audit periods, and ETSI audits, if used, must be a Full Conformance Assessment; Surveillance Audits are not sufficient.

Root Store Policies may impose requirements about how Root Store Operators are notified about the completion of audits. Failure to properly inform a Root Store Operator

about an audit may be grounds for removal from the Root Store, even if the audit was otherwise conducted correctly.

If an Auditor finds non-compliance with Audit Criteria, the Auditor should provide a qualified report that indicates the controls that failed. If there are any changes in the certification status of a CA, the TSP should notify Root Store Operators immediately. The Auditor should provide qualified reports for all time periods until the problems have been fixed. After which, the Auditor may provide a Point-in-time Audit statement to confirm that the problems have been resolved. However as a Point-in-time Audit statement only validates a TSP practices on that date so Period-of-time Audit statements are still required over that timeframe.

CP/CPS Detail

The CA's Certificate Policy (CP) and Certificate Practice Statement (CPS) must provide enough detail to allow third parties to assess how TSPs enforce imposed requirements. A CP/CPS section that simply notes its compliance with the Baseline Requirements is insufficient.

Relevant to Customers and Benefit to the Ecosystem

Root Store Operators reserve the right to determine which CA Certificates are included in their software products, based on the benefits and risks of such inclusion to typical users of those products. At a minimum, the TSP must:

- Provide some service relevant to users of the Root Store Operator's software products.
- Publicly disclose information about their policies and business practices (e.g., in a Certificate Policy and Certification Practice Statement).
- Operate in accordance with published criteria.
- Provide public attestation of their conformance to the stated verification requirements and other operational criteria by a competent independent party or parties with access to details of the TSP's internal operations.

Root Store Operators reserve the right to not include a particular CA Certificate for any or no reason. When assessing suitability for inclusion, Root Store Operators take into consideration criteria that include (but are not limited to):

- If there is reason to believe that including a CA Certificate would cause undue risks to users' security. For example, has the TSP knowingly issued certificates without the knowledge of the entities whose information is referenced in the certificates; or knowingly issue certificates that appear to be intended for fraudulent use?
- If there is reason to believe that including a CA Certificate might cause technical problems with the operation of the Root Store Operator's software.

- The industry reputation and public perception of the TSP. For example, does the TSP or the TSP's controlling entity or associated entities engage in practices which are against the security interests of Root Store Operators' users, or against Root Store Operators' mission, ethos or ethical norms.

TSPs must carefully consider whether their root certificates need to be directly included in a Root Store or if it would be better for their root certificate to be cross-signed by a certificate of an already publicly trusted TSP. It is the TSP's responsibility to demonstrate why their root certificate needs to be included in a Root Store.

Unless explicitly agreed upon in writing in a legally valid contract, Root Stores include CA Certificates without condition, and without being bound by any restrictions or requirements which may be included in a TSP's CP, CPS, or other publications.

Definitions

Audit Period

The time between the start and end dates of a Period-of-time Audit.

Audit Requirements

Obligations set out in an audit standard, such as WebTrust Program for CAs or ETSI EN 319 411.

Auditor

A legal entity authorised to carry out an audit required the Baseline Requirements, EV Guidelines, Root Store Policy, or other audit obligation a TSP may have.

Baseline Requirements

The document "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" published by the CA/B Forum and available at https://cabforum.org/baseline-requirements-documents/

CA Certificate

A certificate whose corresponding private key is used to sign other certificates.

CA/B Forum

An industry group made up of Certificate Authorities / Trust Service Providers and Browsers that establish and manage documents outlining requirements for publicly trusted website authentication certificates.

Certification Authority (CA)

See Trust Service Provider.

EV Guidelines

The document "Guidelines For The Issuance And Management Of Extended Validation Certificates" published by the CA/Browser Forum and available at https://cabforum.org/extended-validation/

Full Conformance Assessment

An audit that covers all Audit Requirements, irrespective of when they were last audited or if they have changed.

Intermediate CA

A CA Certificate that isn't included in a Root Store, but is nevertheless trusted because it chains up to a CA Certificate which is.

Period-of-time Audit

An audit that covers the design and and implementation of policies, procedures and controls and their effective operation over a period of time.

Point-in-time Audit

An audit that covers design and implementation of policies, procedures and controls at a specific point in time, with no assurance on period before or after that date and assurance on effective operation of control.

Publicly Trusted Certificate

Certificates that chain up to a CA Certificate included in a Root Store.

Qualified Report

A report produced by an Auditor which lists one or more Audit Requirements that a TSP failed to meet.

Root Store

A list of CA Certificates that a Root Store Operator has decided to trust, along with associated metadata.

Root Store Operator

A legal entity that maintains a Root Store and/or incorporates a Root Store in software, products, or services that it produces.

Root Store Policy

A published set of requirements that a Trust Service Provider must comply with if they wish their CA Certificate to be included in the Root Store Operator's Root Store.

Surveillance Audit

An audits which does not cover all Audit Requirements, e.g. an audit which covers only changed processes or performs spot checks performed.

Trust Service Provider (TSP)

A legal entity that is responsible for the creation, issuance, revocation, and management of Certificates. Also known as a Certification Authority.