Microsoft

Microsoft Root Program Overview

Panel: Conformity Assessment under eIDAS
September 25, 2019

Agenda

- Overview & References
- Operating Principles
- General Approach to Adding CAs/TSPs
- Contract Highlights

Root Program Overview & References

- Approximately 140 Certificate Authorities representing approximately 400 Root Certificates
  - Compete list at: https://docs.microsoft.com/en-us/security/trusted-root/participants-list
- Program requirements at: https://aka.ms/RootCert
- Audit requirements at: https://aka.ms/auditreqs
- Application requires a contractual agreement with Microsoft

Root Program Operating Principles

- Our Program reflects Microsoft's values. We should be able to stand by the statement *"Microsoft runs on trust and Microsoft trusts <Company name> Certificate Authority and the certificates they issue to ensure the security and privacy of our customers"*
- We run a reliable, secure root store for the benefit for our users. Security of our users is paramount
- Our root store provides a consistent user experience across our products and services
- All CAs are treated equally, independent of their geographic area of operations or market size. Same rules for everyone, rigorously enforced
- Trust, but verify through audits (WebTrust and ETSI) and available open source and proprietary PKI monitoring
- Service and encourage the widest possible use of PKI activities
- CAs are our partners. We partner with them in the certificate lifecycle, audits, ecosystem monitoring and security response
- Microsoft independently conducts regular risk assessments to inform our "trust" decisions

General Approach to Adding New CAs/Roots

- Application completed
- Certificate Policy/Certificate Practice Statement (CP/CPS) review
- Review of audit reports
  - Auditor certified by either WebTrust or EU governance bodies?
  - Any qualifications from the audit?
  - Test websites active?
- Telemetry
- Vetting of the CA and related businesses
  - Management
  - Operations
  - Beneficial Ownership Screening
  - State-Owned Entity review
  - Other due diligence as appropriate
- Threat and intelligence review
- Legal review and contractual agreement
- Microsoft leadership approval
- Annual review of all the above while in our Root Program

Contract Highlights

- CA must agree to comply with our requirements, including compliance with applicable standards, requirements, or audit criteria
- Our relationship with a CA is purely a private contractual agreement between two parties
- Microsoft may audit and verify CA's compliance with our agreement during and up to five years after termination or expiration of our agreement
- If our audit reveals a material breach of security obligations or the performance of operations, then the CA will reimburse Microsoft for the cost of the audit
- At Microsoft's request, an officer of the CA will conduct a self-audit and certify in writing that the CA is in compliance with our Agreement