TeleTrusT-EBCA "PKI-Workshop" 2025

Berlin, 18.09.2025

"Vertrauen in Bewegung: Wie sich QWAC's und Certificate Transparency aufeinander zubewegen"

Enrico Entschew, D-Trust

Worum geht es?

- Vertrauen ist kein statisches Konzept – es entwickelt sich weiter.
- Zwei Welten bewegen sich:
- QWACs (eIDAS, ETSI, Implementing Act) und
- WebPKI mit CT (Baseline Requirments/ EV-Guidelines, CA/Browser-Forum, Browser Policies)

Wie kommen beide Ansätze zusammen?

QWACs im Überblick

- Rechtsgrundlage: eIDAS, Art. 45
- Zweck: Sicherer Identitätsnachweis im Web
- Implementing Act (Draft 2025): legt technische Details fest
- Standard:
  - Für QWACs ohne Einsatz in der WebPKI: ETSI EN 319 411-2 V2.6.1 (2025-06) – QNCP-w-gen certificate policy, QEVCP-w certificate policy oder QNCP-w certificate policy
  - Für QWACs mit Einsatz in der WebPKI: ETSI TS 119 411-5 (02/2025)

Ziel: Einheitliche, interoperable QWACs in Europa

WebPKI: Zwei QWAC-Varianten

- Definiert in ETSI TS 119 411-5 (02/2025)
- 1-QWAC: QWAC = TLS-Zertifikat, nahe EV, browserfreundlich, einfach
- 2-QWAC: getrenntes QWAC + Standard-TLS, erweiterte Identitätsattribute, regulatorisch verankert

2-QWAC Binding

- Mechanismus: TLS-Zertifikat + QWAC über Binding-Datei (JSON, signiert) gekoppelt
- Bereitstellung via HTTP-Header Link: rel="tls-certificate-binding"
- Browser-Validierung: prüft TLS-Zertifikat, lädt Binding-Datei, verifiziert Signatur
- Vorteile: volle TLS-Kompatibilität + zusätzliche regulatorische Sicherheit

Herausforderungen bei QWACs

- Browser zögern mit nativer Unterstützung
- Spannungsfeld: regulatorische Anforderungen vs. technische Realität

Wie schafft man Transparenz und Akzeptanz in einem globalen Ökosystem?

WebPKI: Certificate Transparency – Ausgangspunkt

- Trotz strenger Browser-Vorgaben Risiko: fehlerhafte oder missbräuchliche Zertifikate
- Klassische Rootstore-Audits → ex post, nicht in Echtzeit

Lösung: Transparenz in der Ausstellung

Funktionsweise von CT

- Jedes Zertifikat wird in öffentliche, unveränderliche Logs eingetragen
- Logs kryptografisch gesichert (Merkle Trees, SCTs)
- Verschiedene Rollen: CA, CT-Log-Betreiber, Monitor, Auditor, Client
- Jeder kann überwachen: Browser, CAs, Forscher, Unternehmen
- Standards: RFC 6962, RFC 9162 und Static Certificate Transparency API

Vorteile von CT

- Früherkennung von Missbrauch
- Accountability der CAs
- Ökosystem-Monitoring durch jedermann
- Vertrauensbildung durch Transparenz

QWAC & CT – eine Annäherung

- Gemeinsame Basis: Vertrauen, Sichtbarkeit, Überprüfbarkeit
- Diskussionspunkte: QWACs könnten in CT-Logs sichtbar werden
- Static CT APIs für regulierte Szenarien
- Fragen zu Datenschutz und Governance (EU vs. Browser)

ETSI Technical Report zu CT

- ETSI arbeitet an einem Technical Report (TR) zu CT
- Analyse: Status Quo CT (Browser-getrieben, nur TLS-Server)
- Herausforderungen: keine QWAC-Abdeckung, Datenschutz
- Diskussionsansätze: Logging von QWACs, Static CT APIs, europäisches CT-Ökosystem
- Ausblick: TR als Basis für einen möglichen ETSI-Standard

Chancen & Synergien

- CT stärkt Transparenz der QWAC-Ausstellung
- QWACs bringen regulatorische Legitimität ins Web
- Brücke zwischen Regulierung und Technik
- Europäisches CT-Ökosystem im Einklang mit eIDAS

Fazit

- QWACs und CT bewegen sich aufeinander zu
- Gemeinsames Ziel - Vertrauen im digitalen Raum
- Dialog zwischen EU, ETSI, CAs, Browsern nötig