CA/BROWSER FORUM

Clarify the scope of TLS Baseline Requirements

F2F#64 26-March-2025 | Tokyo, Japan

Presenter: Dimitris Zacharopoulos (HARICA)

Existing scope

- Section 1.1
  - *"This document describes an integrated set of technologies, protocols, identity-proofing, lifecycle management, and auditing requirements that are necessary (but not sufficient) for the issuance and management of Publicly-Trusted TLS Server Certificates;* ***Certificates that are trusted by virtue of the fact that their corresponding Root Certificate is distributed in widely-available application software****. The requirements are not mandatory for Certification Authorities unless and until they become adopted and enforced by* ***relying-party Application Software Suppliers****."*
  - *"These Requirements only address Certificates intended to be used for authenticating* ***servers accessible through the Internet****. Similar requirements for code signing, S/MIME, time-stamping, VoIP, IM, Web services, etc. may be covered in future versions."*
- Section 1.6.1
  - ***Application Software Supplier****: A supplier of* ***Internet browser software*** *or* ***other relying-party application software*** *that displays or uses Certificates and incorporates Root Certificates.*

Other excerpts

- "*The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates describe a subset of the requirements that a certification authority must meet in order to issue digital certificates for SSL/TLS servers* ***to be publicly trusted by browsers.***" [About the Baseline Requirements]
- Scoping statements from the SCWG Charter, including:
  - *"1. Scope: The authorized scope of the SCWG shall be as follows:*
  - *(a) To specify Baseline Requirements, Extended Validation Guidelines, and other acceptable practices for the issuance and management of TLS server certificates used for* ***authenticating servers accessible through the Internet****;"*
  - *"****Out of Scope****: The SCWG will not address certificates intended to be used primarily for code signing, S/MIME, time-stamping,* ***VoIP, IM, or Web services.****"*
  - *"3. Membership:*
  - *(b) Certificate Consumer: The Certificate Consumer voting class shall consist of eligible organizations meeting the following criteria:*
  - *(1)* ***it produces a software product intended for use by the general public for browsing the Web securely;****"*

Problem statement

- **Subscribers of certificates containing one of the CA/Browser Forum Reserved Policy OIDs described in the TLS Baseline Requirements are sometimes not using them as described in the scope of the TLS BRs**
- Public TLS Certs used on servers not accessible **by the entire** Internet
  - Usually protected by a firewall, accessible from authorized network segments, or through VPN
- Consumed by Application Software Suppliers that are **not Browsers** (e.g. popular call centers, cloud/hosting providers, ERP software vendors)

Open discussion

- Why should the SCWG further clarify the scope of the TLS BRs:
  - CAs will better satisfy subscriber needs, while also better preventing private/local PKI use cases from encumbering the agility and innovation in the modern Browser use cases
  - Subscribers will understand where and how these certificates are supposed to be used
  - Backwards compatibility will not prevent new RFCs from being introduced (e.g. 9549, 9618)
- Should the SCWG update section 1.1 to state that:
  - *TLS BRs are designed only for Browser use cases?*
  - *Certificates conforming to the TLS BRs are to be be installed on servers accessible from the public Internet without restrictions on TCP ports 80/443?*
- ETSI allows different rules for “non-Browser” server TLS use cases. Should the SCWG flag browser-only requirements?
  - Restrictions can be enforced/signaled via EKU or policy OIDs