Jens Bender

Topic Area: Roles and requirements for the actors in the CA system including network security requirements

Topic: Enhancing Trust by Enhancing the Audit Process

Authors: Kerstin Schönherr, Jens Bender (German Federal Office for Information Security, BSI)

Abstract:

PKIs are about delegating trust. Therefore the entities entitled to delegate trust, i.e. Certification Authorities, must be trustworthy and trusted by the aptly named Relying Parties. The DigiNotar incident has proven that revocation of trust (by the Dutch Government, in this case) can be fatal to the CA itself.

There have been many proposals to enhance the security of TLS (certificate pinning, DANE, ...). The common denominator of these proposals is a general mistrust in CAs, trying to shift security to the end-user (or the browser, as a proxy for the end-user) or other mechanisms like DNS. Unluckily, these proposals do not adress the problem of initial trust (e.g. pinning) or replace one trust-requiring entity by another trust-requiring entity (e.g. DNS registrars/servers), not really solving the problem.

The only way to actually solve the problem is to (re-)establish trust into the CA system. Since the end-user is not able to evaluate the security of CAs himself, he delegates this tasks to the browser vendors, which in turn delegate this task to auditors. The trustworthiness of a CA, established by the security of the CA, is complemented by trust, established via the audit process.

To strengthen the CAs security and the audit process, the German Federal Office for Information Security (BSI) is working on a requirement and audit scheme, which:
-- is process oriented, starting from CA key generation, registration of subjects, certificate issuance, revocation, up to termination of CA operations;
-- borrows some ideas from Common Criteria, e.g. a clear structure starting from Objectives and Threats, leading to Requirements on the CA operation;
-- contains clear guidance on the checks to be performed by the auditor, enhancing transparency and consistency of the audit process;
-- is suitable for general CA operations (not only TLS), enabling trust service providers to cover CAs from different application areas in one audit.

The talk will elaborate on these ideas and the current state of affairs.