

TOPIC: Requirements for the actors in the CA system in Europe

TITLE: European Approach to oversight of "Trust Service Providers"

ABSTRACT: The presentation describes the approach being established in Europe to improve the trust in the online marketplace through regulatory oversight of "Trust Service Providers" (TSP) issuing SSL server certificates (i.e. Certification Authorities). The European Commission has proposed in a draft regulation "on electronic identification and trusted services for electronic transactions in the internal market" to operate supervisory scheme which has oversees the operation of TSPs.

This allows either

- a) Reactive supervision: TSPs establishes its own procedures based on industry best practice with mandatory requirement to report any security incident potentially with liability implications.
- b) Proactive supervision: TSPs are annually audited for conformance to best practice with "qualified" status recognised by the supervisory body based on the audit report.

ETSI working with the CA/B-Forum, which is the recognised industry body for Certification Authority best practices, has issued as standard for the best practices for issuing public key certificates including SSL certificates published as TS 102042, see:

http://www.etsi.org/deliver/etsi_ts/102000_102099/102042/02.04.01_60/ts_102042v020401p.pdf.

TS 102042 is also based around the recognised international standard for information security management systems (ISO 27001). TS 102042 can be used by "TSPs" for either reactive or proactive (qualified) approach to TSP supervision. A TSP may use TS 102 042 as the basis for its procedures and in so doing demonstrate that it has followed best practice. Alternatively, a TSP can (on implementation of the regulation) opt to having a regulated audit to become recognised as a "qualified" TSP.

A key to the success of this scheme is the ability of the supervision scheme and recognised best practice standards to be kept up to date by reacting to new security threats and reported incidents.

The presentation will provide further information on this European approach and discuss its advantages / disadvantages.

------(296 Words)

Speaker

Arno Fiedler, STF 438 Taskleader, ETSI ESI and MD of Nimbus Technologieberatung GmbH

in cooperation with

Nick Pope, Thales e-Security Ltd, UK

Christoph Sutter, TUVIT, DE

Inigo Barreira, Izenpe, ES

Sylvie Lacroix, Sealed s.p.r.l., BE

If there are further questions please contact me by eMail or meet me at the german booth at RSA-Conference 2013.

<http://www.rsac.german-pavilion.com/content/en/home/home.php>

Best regards

Arno Fiedler