Welcome to the World of Standards

ETSI

World Class Standards

RESULTS ON STF 412 AND 438

Arno Fiedler, STF 438

Berlin, 2. CA-Day Meeting

Some History (motivation?)

- In 2006 the “green bar concept” with “extended Validation Certificates” for websites with SSL-Certs was established as simple Trustmark by Browsers and CA´s.
- Policies, Procedures and Audit framework are needed to secure a common level of trust.
- CA/B-Forum as “voluntary gathering” was founded, they accepted the WebTrust quality seal for CA´s first.
- Many non US-CA´s are not happy with WebTrust-Audits made by chartered accountants.
- Since 2007 ETSI collaborate with CA/B-Forum on base of the existing policies (mostly TS 102 042) as alternative to Webtrust compliance.

Scope of STF 412 and 438 in 2010-2012

- Guide to a framework for CSPs which want to issue “Extended Validation Certificates”
- Harmonised EU framework for assessing conformance of CAs in line with EVC Guidelines as issued by CA/B Forum
- Extends TS 102 042 “Policy requirements for certification authorities issuing public key certificates” to incorporate support for CA Browser Forum Guidelines Baseline and EVC-Requirements
- Define Audit requirements for TS 102 042

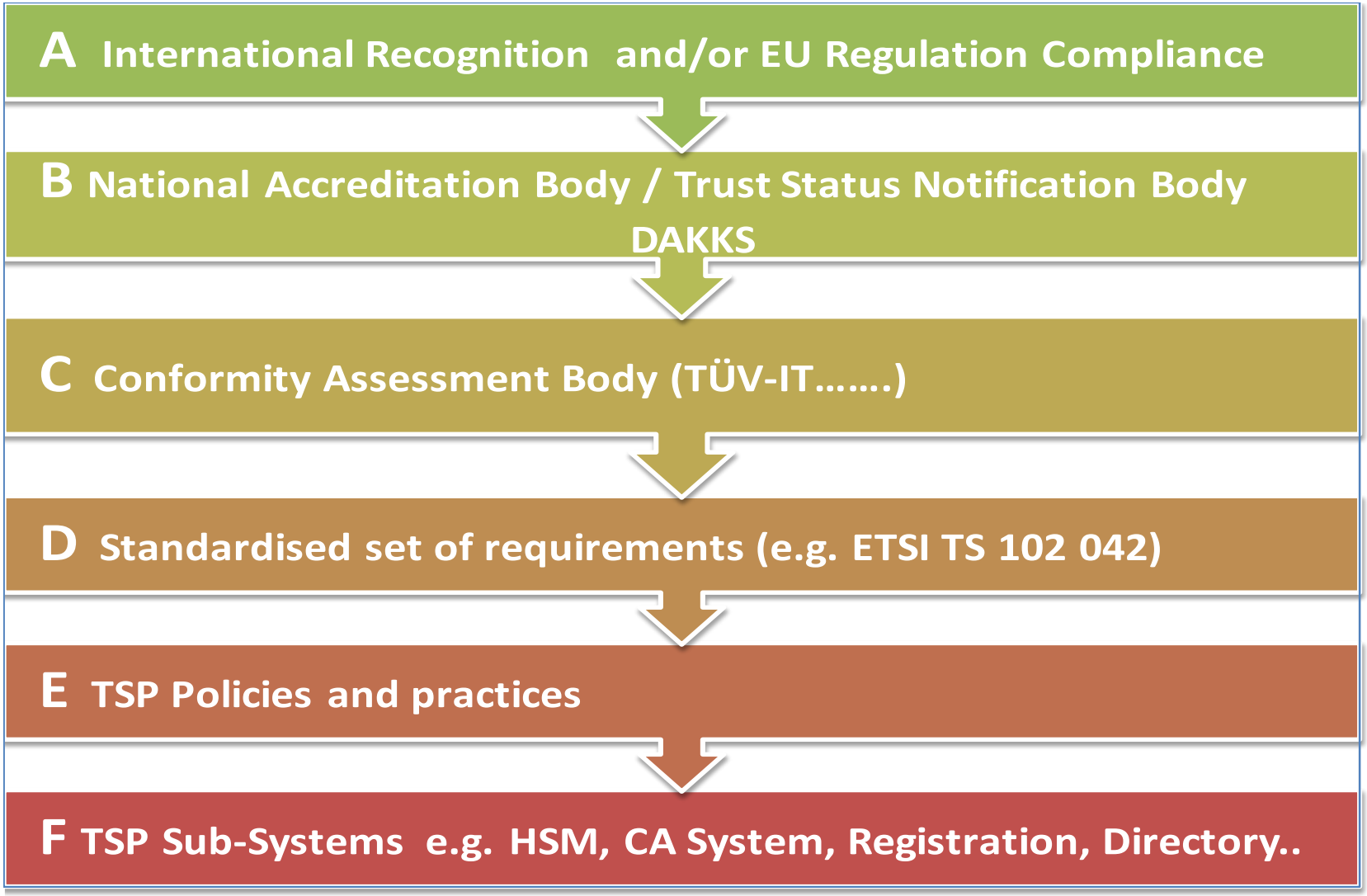
Results of STF 412 in 2010-2011

Reference	Current Status
DTR/ESI-000107 (TR 101 564) **Guidance on ETSI TS 102 042 for Issuing Extended Validation Certificates for Auditors and CSPs**	Publication (2011-09-19)
DSR/ESI-000109 (SR 003 091) **Recommendations on Governance and Audit Regime for CAB Forum Extended Validation and Baseline Certificates**	Publication (2012-04-11)
DTS/ESI-000108 (TS 103 090) **Conformity Assessment for Trust Service Providers issuing Extended Validation Certificates**	Publication (2012-04-20)

Results of STF 438 in 2011-2013

Reference	Version	Current Status
DTR/ESI-000118 (TR 103 123) **Guidance for Auditors and CSPs on ETSI TS 102 042 for Issuing Publicly-Trusted TLS/SSL Certificates** Microsoft Word 97-2003-Dokumen	1.1.1	Publication (2012-11-16)
RTS/ESI-0002042version231 (TS 102 042) **Policy requirements for certification authorities issuing public key certificates** Microsoft Word 97-2003-Dokumen	2.3.1	Publication (2012-11-16)

Requirements for defining a appropriate Security Level for Certification Service Provider through Conformity Assessment



Deliverables of the STF 438. Status of TS 102 042 V 2.3.1

In addition, the TS 102 042 specifies six alternative variants of NCP, The alternatives are referred to as:

- **the Lightweight Certificate Policy (LCP)** for use where a risk assessment does not justify the additional costs of meeting the more onerous requirements of the NCP (e.g. physical presence);
- **the extended Normalized Certificate Policy (NCP+)** for use where a secure user device (signing or decrypting) is considered necessary;
- **the Extended Validation Certificates Policy (EVCP)** for use with code signing or TLS/SSL where provisions, additional to those indicated in NCP, are required to issue EVCs, consistently with what is specified in the EV Certificates Guidelines [16] issued by the CAB Forum;
- **the enhanced Extended Validation Certificates Policy (EVCP+)** for use with code signing or TLS/SSL where, in addition to the requirements to issue EVCs, a secure user device (signing or decrypting) is considered necessary.
- **The Domain Validation Certificates Policy (DVCP)** for use with TLS/SSL where provisions, additional to those indicated in NCP, are required to issue DVCs, consistently with what is specified in BRG [20] issued by the CAB Forum
- **The Organizational Validation Certificates Policy (OVCP)** for use with TLS/SSL where provisions, additional to those indicated in NCP, are required to issue OVCs, consistently with what is specified in BRG [20] issued by the CAB Forum

© ETSI 2011. All rights reserved

QUESTIONS?

THANK YOU ON BEHALF OF STF438

© ETSI 2012. All rights reserved