The Auditor’s view

ETSI - European CA-Day - November 29th, 2012 - Bundesdruckerei, Berlin

Christoph SUTTER

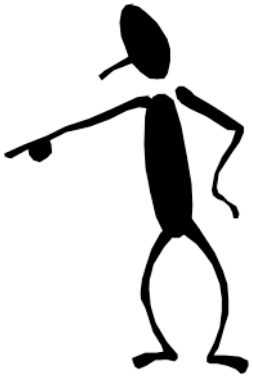
TÜVIT®

Outline

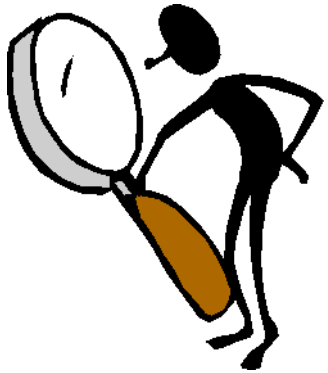
1. Introduction
2. ETSI Framework for TSP Conformity Assessment
   - Assessment-Criteria
   - Audit-Criteria
   - Conformity Assessment Guidance
3. EU Regulation on Electronic Identification and Trust Services for Electronic Transactions
   - Proposal COM(2012) 238/2
4. Summary

© TÜV Informationstechnik GmbH – Member of TÜV NORD Group

Introduction – Investigation of Damages



garage:
repair costs
1,500 €



insurance: need independent assessor

assessor:
need to repair more
2,500 €

What was the basis for the assessments?

© TÜV Informationstechnik GmbH – Member of TÜV NORD Group

Introduction – Conformity Assessment Basics

1. Object of Conformity Assessment
   - product (incl. services), process, installation, system, person, body
2. Specified Requirements
   - normative documents such as regulations, standards and technical specifications
3. Conformity Assessment System / Scheme
   - rules, procedures and management for carrying out conformity assessment
   - operated at international, regional, national or sub-national level
4. Conformity Assessment (Activities)
   - selection and determination (sampling, testing, inspection, audit)
   - review and attestation (certification)
   - surveillance including suspension and withdrawal
5. Major Players
   - client, conformity assessment body, accreditation body

© TÜV Informationstechnik GmbH – Member of TÜV NORD Group

Introduction – Conformity Assessment of TSP

1. Object of Conformity Assessment
   - certification service of TSP
2. Specified Requirements
   - e. g. ETSI TS 102 042, 101 456 & 102 023
3. Conformity Assessment System / Scheme
   - based on ISO/IEC 17021 & 17065
   - defined by nationally accredited conformity assessment bodies
4. Conformity Assessment (Activities)
   - selection and determination (sampling, testing, inspection, audit)
   - review and attestation (certification)
   - surveillance including suspension and withdrawal
5. Major Players
   - TSP, Certification Body, National Accreditation Body

© TÜV Informationstechnik GmbH – Member of TÜV NORD Group

Introduction – ISO/IEC 17007: Drafting Principles

5 Principles for Drafting Normative Documents:

1. separation of specified requirements for
   - object of conformity assessment and
   - conformity assessment activities
2. neutrality towards parties performing conformity assessment activities
   - possibility of first, second or third party assessment
3. functional approach
   - selection and determination / review and attestation / surveillance
4. comparability of conformity assessment results
5. good practice in conformity assessment
   - use of international standard, best practices etc.

© TÜV Informationstechnik GmbH – Member of TÜV NORD Group

ETSI Framework for TSP Conformity Assessment

1. Specified Requirements for Object of Conformity Assessment (TSP)
   - General Policy Requirements for TSP supporting Electronic Signatures
   - Policy and Security Requirements for TSP issuing certificates
     - part 2: Policy Requirements for CAs issuing Qualified Certificates
     - part 3: Policy Requirements for CAs issuing Public Key Certificates
2. Specified Requirements for Conformity Assessment Activities
   - Guidance on ETSI TS 101 456 – Qualified Certificates
   - Guidance on ETSI TS 102 042 – EV Certificates
   - Guidance on ETSI TS 102 042 – Publicly-Trusted TLS/SSL Certificates
3. Criteria for Conformity Assessment Scheme
   - TSP Conformity Assessment – General Requirements and Guidance

© TÜV Informationstechnik GmbH – Member of TÜV NORD Group

ETSI Framework - Summary

- ✓ Specified Requirements for Object of Conformity Assessment (TSP)
- ✓ Specified Requirements for Conformity Assessment Activities
- ✓ CA/Browser Forum Requirements Incorporated:
  - ✓ EV-Guidelines
  - ✓ Baseline Requirements
  - ✓ Network and Certificate System Security Requirements
- ✓ Criteria for Conformity Assessment Scheme
  - but: ETSI is a European Standardization Organization (ESO) and no assessment scheme operator

© TÜV Informationstechnik GmbH – Member of TÜV NORD Group

EU Regulation on Electronic Identification and Trust Services for Electronic Transactions (1/2)

- requires an annual security audit on qualified TSPs by a recognised independent body (supervision)
  - … to confirm that they and the qualified trust services provided by them fulfil the requirements set out in this Regulation
- 2+1 paragraphs for security requirements for TSPs
  1. manage risks posed to the security of the service and take appropriate measures
  2. notify breach of security or loss of integrity
  3. Commission shall be empowered to adopt delegated acts for further specifications of measures
- plus further requirements for qualified TSPs (Art. 19)
  - e. g. on identification, certificate status provision, revocation (within 10 min!), staff qualification, trustworthy systems, etc.

© TÜV Informationstechnik GmbH – Member of TÜV NORD Group

EU Regulation on eID and Trust Services (2/2)

From the TSP auditor‘s point of view:

- requirements of the regulation need „translation“ and extension into testable / auditable requirements
- TSP risk management approach (Art. 15.1) needs to be amended by mandatory minimum security measures, especially for network security (Art. 15.5)
- minimum requirements on audit methods, e. g. penetration testing, need to be defined (Art. 16.5)
- certified products are needed as secure anchors:
  - qualified electronic signature creation device
  - trustworthy systems for TSP operation

© TÜV Informationstechnik GmbH – Member of TÜV NORD Group

The auditor‘s propositions (for delegated acts)

1. Use recognised ETSI and CEN standards to define requirements for TSP services
2. Add additional requirements where needed, e. g.
   - detailed network security requirements
   - requirements for secure products
3. Define requirements for conformity assessment activities:
   - for sampling of sites, testing, inspection and audit
   - example: mandatory penetration testing
4. Rely on existing TSP conformity assessment schemes
   - ISO/IEC 17021 for security management systems
   - ISO/IEC 17065 for products, processes and services

© TÜV Informationstechnik GmbH – Member of TÜV NORD Group

Summary

- existing national conformity assessment schemes (ISO/IEC 17021/17065) are a suitable and powerful framework for assessing the security of TSPs
- ETSI criteria provide valuable requirements for the different types of conformity assessment activities
- additional mandatory network security requirements and certified products will enhance the overall security level of TSPs significantly
- additional requirements for conformity assessment activities will enhance the assurance that stated requirements are fulfilled

© TÜV Informationstechnik GmbH – Member of TÜV NORD Group

Thank you very much for your attention!

TÜV Informationstechnik GmbH
Member of TÜV NORD Group

Dr. Christoph SUTTER
Division Manager IT Infrastructure

Langemarckstr. 20
45141 Essen, Germany

Phone: +49 201 8999 – 582
Fax: +49 201 8999 – 555
E-Mail: C.Sutter@tuvit.de
URL: www.tuvit.net