Welcome to the World of Standards

World Class Standards

ETSI – European CA DAY

TRUST SERVICE PROVIDER (TSP) CONFORMITY ASSESSMENT FRAMEWORK

Presented by Nick Pope, ETSI STF 427 Leader

© ETSI 2012 All rights reserved

Topics

- Background
  - ETSI Activities / Link to Mandate / CAB Forum
- ETSI “Policy Requirements”
- Recommended Framework for European TSP “Conformity Assessment”

© ETSI 2012. All rights reserved

Background: TSP Standards Linked to E-Signature Directive 1999/93

- TS 101 456 “Policy Requirements for Certification Authorities issuing Qualified Certificates”
  - Aimed at requirements in Annex II of Directive
  - First version published in 2000
  - Best practice for CA “trustworthy” operation
- TS 102 042 “Policy Requirements for Certification Authorities issuing Public Key Certificates”
  - Generalised requirements for any kind of public key certificate
  - Derived from TS 101 456
  - First version published in 2002
- Other policies
  - time-stamping authorities
  - Attribute authorities

© ETSI 2012 All rights reserved

Background: Supervisory & Accreditation under Directive 1999/93

- Each Nation has own “Scheme” for supervision of “Certification Service Providers” with “optional” Accreditation
- Many adopted TS 101 456
- Significant variations in approach to audit (Major issue from last workshop)
- ETSI proposed Conformity Assessment Framework

© ETSI 2012 All rights reserved

Background: CAB Forum

- The Certification Authority Browser Forum (CA/Browser Forum) is a voluntary organization of leading certification authorities (CAs) and vendors of Internet browser software and other applications.
- Produced guidance for CAs issuing SSL/TLS (and Code signing) for Browser root programs
  - Extended Validation Certificates
  - Baseline SSL/TLS

© ETSI 2012 All rights reserved

Background: CAB Forum & ETSI

- A number of CA's issuing SSL Certificates also "supervised" against TS 101 456
- Since 2007 ETSI has Worked with CAB Forum to apply ETSI Specifications to CAB Guidance
- TS 102 042 updated to specifically take into account use with CAB Forum Guidelines for:
  - Baseline Guidelines (recent updates – presented later)
  - Extended Validation
- CAB Forum requires audit in accordance with:
  - Webtrust for CA
  - (~~National scheme that audits conformance to ETSI TS 101 456~~)
  - National scheme that audits conformance to ETSI TS 102 042
  - ISO 21188 (PKI for financial services)

© ETSI 2012 All rights reserved

Standardisation Mandate 460

- European Commission Mandate 460 Activities relating to Trust Services:
  - Phase 1 (April 2011 to March 2012)
    - Quick Fixes
      - TS 101 456 & TS 102 042 to European Norm (EN) (excluding web certificates)
      - Certificate Profile to EN
      - Conformity Assessment TS
  - Phase 2 (2013 to 2015) Implement work plan
    - Complete set of TSP policy requirements (Web Certs, Time-stamp, Attribute certs)
    - Conformity Assessment to European Norm (EN)

© ETSI 2012 All rights reserved

Terminology

- Real World Terminology:
  - Certification Authority, Time-stamping Authority, OCSP Service, ….
- Electronic Signatures Directive 1999/93
  - Certification Service Provider (CSP)
- New Draft Regulation Terminology
  - Trust Service Provider (TSP)
  - May include Identity Service Provider ?

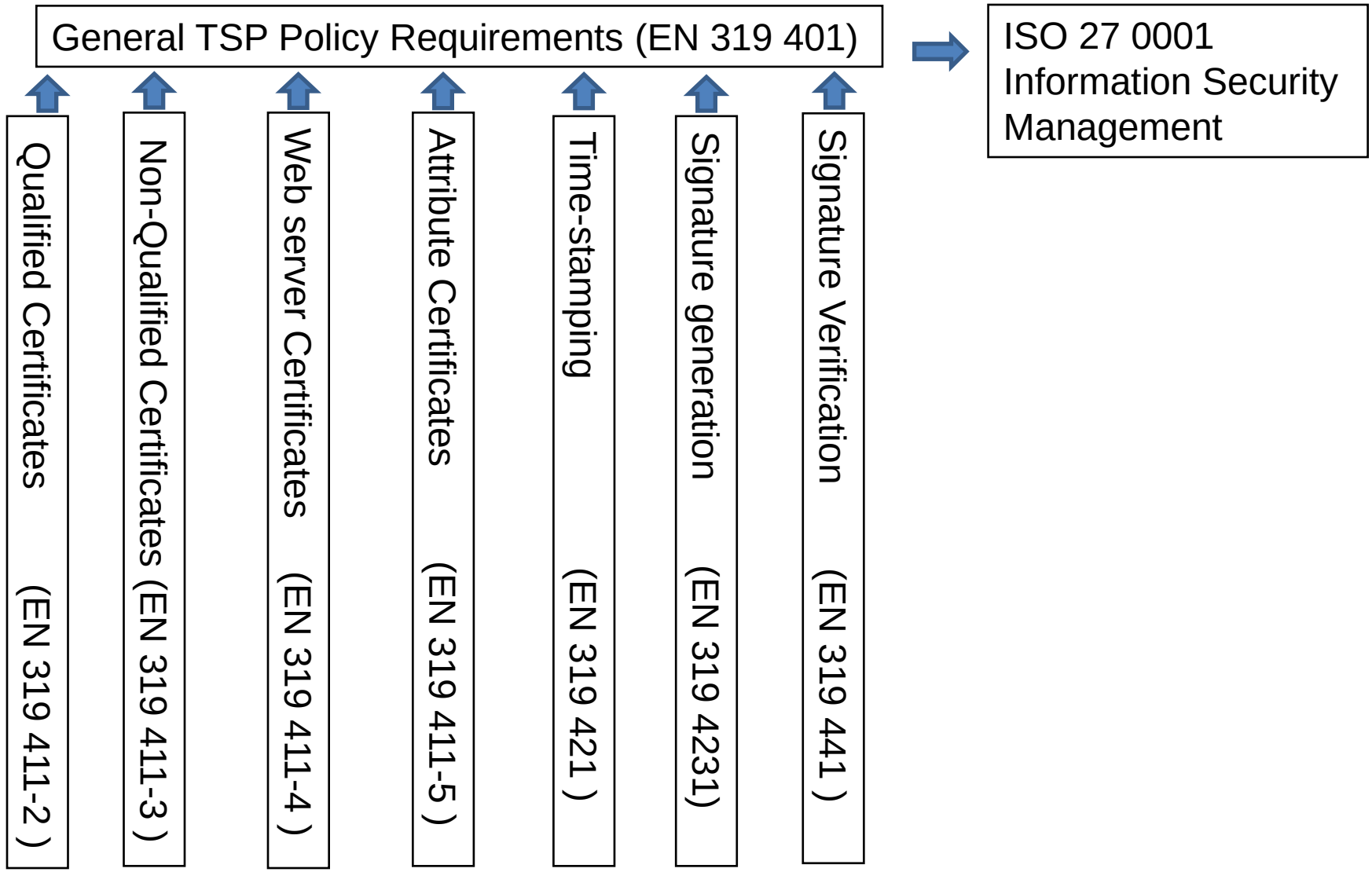
© ETSI 2012. All rights reserved

ETSI "Policy Requirements" Current Specifications

- TS 101 456 – Policy requirements for Certification Authorities issuing Qualified Certificates
- TS 102 042 – Policy Requirements for Certification Authorities issuing Public Key Certificates
  - Non-qualified signing
  - Server certificates (CAB Baseline, Extended Validation)
- TS 102 023 - Policy requirements for time-stamping authorities
- TS102 158 – Policy requirements for CSP issuing attribute certificates usable with Qualified certificates

© ETSI 2012. All rights reserved

TSP Policy Requirements – Updated Structure



© ETSI 2012. All rights reserved

TSP Policy Requirements – Phase 1 Updates

- EN 319 401 – General Policy Requirements for TSPs
- EN 319 411-2 – Policy requirements for certification authorities issuing qualified certificates(was TS 101 456)
- EN 319 411-3 – Policy requirements for Certification Authorities issuing public key certificates (TS 102 042: NCP & LCP)

All:

- published as prEN and completed national standards body review
- Updated to take into resolve comments
- Currently under EN final ballot

© ETSI 2012. All rights reserved

Policy Requirements – Future Plans

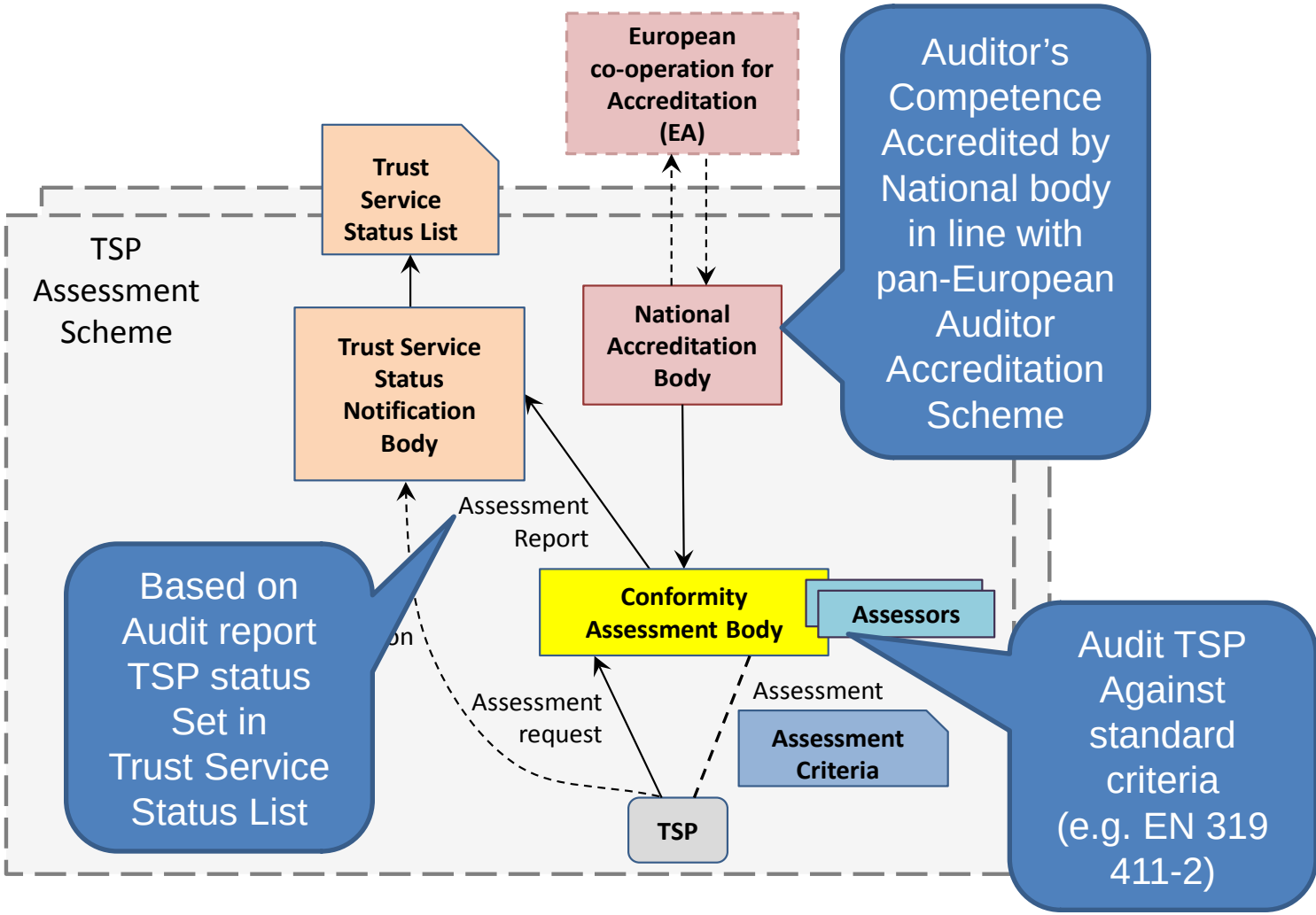
European Norms for policy requirements :

- Web server certificates issuing CAs (TS 102 042 CAB Baseline & EV)
- Attribute authority issuing authorities
- Time-stamping authorities
- Signature generation services
- Signature validation services

All to be developed under Mandate 460 Phase 2 2013-2015

© ETSI 2012. All rights reserved

TSP Conformity Assessment Model



© ETSI 2012. All rights reserved

Basis of Scheme

- ISO 27006 Requirements for Information Security Management System Audit
  - ISO 27000 Risk based controls +
  - Controls to meet Legal requirements

- ISO/IEC 17021 Requirements for Audit of Management System

© ETSI 2012. All rights reserved

TSP Conformity Assessment

- TS Published as TS 319 403
- Available for download from ETSI Download at:
  http://pda.etsi.org/pda/queryform.asp
- Plan to progress to EN in 2013/2014

© ETSI 2012 All rights reserved

Thank you

- For updates on e-Signature Standardisation
  - Subscribe to e-Signature news mailing list:

  http://list.etsi.org/scripts/wa.exe?SUBED1=e-signatures_news&A=1

- ETSI Download :

  http://pda.etsi.org/pda/queryform.asp

© ETSI 2012 All rights reserved