CABF Questions&answers

ETSI questions

The following answers provide best understanding of individual experts from ETSI but do not represent any definitive position of ETSI.

Q1: When is ETSI ESI publishing the new ENs regarding policies?

A plan for the publication and migration to the ETSI standards for the EU Regulation are given in draft document "ETSI / EA Recommendations regarding Preparation for Audit under EU Regulation (EU) No 910/2014 Article 20.1."

Draft versions of the ETSI policy requirements documents will be available for review and comment at the beginning of 2015.

Q2: When the schema of the auditing process is going to be ready in all countries? What about the new conformity assessment? How to change from a TS to a new EN? How the browsers should treat all these options? Where to get a list of the accredited auditors? How´s the maintenance of that list?

It is aimed to have a conformity assessment scheme in place by Jul 2016 as outline in the migration document mentioned above. Until that date TS 102 042 may be used to assess conformance to the CAB Forum requirements under the rules proposed in the recent motion:

> "The resulting section 17.6, bullet 4, would read as follows:
> 4. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with what stated in Annex E of the ETSI TS 102 042 to provide proof of accreditation from, an accreditation body that is a members of EA or IAF, against the requirements of ISO/IEC 17021 or EN 45011 or ISO 17065 (ISO equivalent to EN 45011) or ISO 27006 / 27001."

Guidance information is available on accredited auditors is available at:
http://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx

Q3: Up to now, and being 2 ENs currently published, should the browsers admit them? In which conditions?

The 2 ENs published now, EN 319 411-2 and EN 319 411-3, are for CAs issuing qualified certificates and public key certificates, but none of those, mainly the second one, adopt the CABF documents, so are not of interest of the CABF at the moment.

Q4: What about the network security requirements? Are the CAs to be audited against the 319 401 plus the others?

The requirements of EN 319 401 (which also include the CABF network security requirements) are incorporated by reference into EN 319 411-x. So CABF audits should be against EN 319 411-x, other requirements from CABF & 319 401 are incorporated in 319 411 audit.

The network security requirements are also incorporated in ETSI TS 102 042 v 2.4.1 by reference.

Q5: About the ISO 27002 controls, does it mean that you don´t have to do an ISO audit? Can this be considered as a substitution?

ISO 27002 controls are used only for guidance on nhow to meet the ETSI requirements for security management. There is no requirement to carry out any separate audits under the ETSI based audit scheme.

Q6: Regarding the TLs, if you´re a TSP which don´t have your CAs or your services in the TL in the country you operate for whatever reason, does it mean that you´re not qualified? If being in the TL means that you´re qualified? Which are the requirements to be included in a TL? It depends on the country you operate? Can you "change" the country if does not offer what you expect? How? Can you be in more than one TL? How to check the list of list?

I would say that from a pan_EU (and global) viewpoint on qualified TSP are in the TL. Any others are against specific national requirements which are not aimed at use outside the country. The TL includes information about the type service provided, so those providing say "qualified web site certificates" should be easily identifiable.

For specific requirements under eIDAS regulation regarding qualified trust services and approval and use of TL, CABF members should read the regulation and the specific requirements of a particular country of their interest.

EU Regulation questions

It is recommended that if the CAB Forum has any specific questions regarding the regulation then this is addressed to the EU Commission. Some informal suggestions are provide below but no guarantees are provided regarding whether these are correct. Legal advice should be sought to obtain a more definitive answer.

Q1: Why Webtrust is not included? Where and how to find an ETSI auditor?

Attention is drawn to Article 20.1 and Article 3(18) regarding the legal requirements for audit.

See above regarding requirements and information on ETSI audits.

Q2: What about insurances in the EU for CAs?

Attention is drawn to Article 13 regarding liability, and Article 24.2 c).

Q3: How to apply according to article 14 on international aspects?

It is recommended that the CAB Forum raise this question to the EU commission for guidance.

Q4: Why the change from 3 years to 2 in the audit processes?

For qualified TSPs it is required that the TSP be audited under the Article 20 requirements by July 2017, thereafter the 2 year requirement applies.

Q5: Requirements for QTSPs if none of the certificates the CABF is dealing with are not considered qualified, does this article 24 apply to them?

No, but some of the requirements expressed in the regulation does affect to all kind of CAs.

Q6: What´s the difference between a qualified web site certificate of those managed by the CABF? Do you need to be a QTSP to issue these certificates? Are they going to be the EVs?

The requirements for qualified web sites are specific to the regulation. However, ETSI standards (including those for qualified certificates for web sites) are based around the CAB Forum Baseline and EV requirements, thus making it easier for a TSP to meet the requirements of both the CAB Forum and the EU Regulation.

Q7: when do browsers have to “apply” the regulation?

The regulation makes no direct regulatory requirements on web browsers. Most of the requirements of the regulation apply from July 2016. All TSPs, other than those “used exclusively within closed systems resulting from national law or from agreements between a defined set of participants” (Article 2.2) will be required to comply with the general requirements of the regulation It is up to the TSP whether it decides to offer qualified trust services.

Q8: when the new ENs entry in force and when the “old” TS have to be removed to be applied in the browsers root programs?

Currently the EU Regulation makes no regulatory requirements on use of specific standards. See separate document on planned migration on how ETSI standards may be used to meet the requirements of the regulation.

Q9: from the browsers perspective and the CABF as an organization as well, how to know if an auditor and an audit are accredited?

The national accreditation body should be contacted to identify “conformity assessment bodies” that have been accredited by that national body.

Some further guidance is provided at:

http://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx

Q10: If an auditing body ceases its activity or is no longer accredited, are there audits still valid?

Contact your national accreditation body for guidance.

Q11: How to distinguish and treat the so called qualified certificates for web site authentication?

No answer. Will see how the implementing act indicates.

Q12: Will they follow the CABF Baseline requirements?

ETSI standards in this area are based around the CAB Forum baseline. Conformance to specific CAB Forum requirements (OV, DV, EV) will depend on the particular “certificate policy” options selected.

Q13: What is going to happen with the code signing certificates?

I would see TSPs issuing code signing certificates may well come under the provisions of the regulation.

Q14: Will these follow the same rules the CABF specifies?

It is aimed by ETSI to maintain alignment with the CAB Forum requirements, but compliance to future CAB Forum requirements, e.g. for code signing, will depend the impact of these new requirements on the objectives of ETSI members which includes alignment with EU regulations.