



ENISA – Trust Services Forum

A brief summary on issues that create problems on the Qualification of TSP

Riccardo Bianconi

**Ispettore, ACCREDIA
(on behalf of EA)**

Our European Market is based on some principles that are also the politic, economic and juridical **foundation** holding the concept of **common market**.

One of the original and foudamental principle is the **free circulation of citizens (and professionalism), goods, capitals and services** among nations that are linked by treaty of Rome, Maastricht and Lisbon and signatories of European Constitution.

In this framework of principles, in 2014 was adopted the Eu Reg. 910.

- 1 - The aim of the Regulation is *"building trust in the online environment is key to economic and social development"*.
- 2 - *This Regulation seeks to enhance trust in electronic transactions in the **internal market** by providing a **common foundation for secure electronic interaction between citizens, businesses and public authorities**, thereby increasing the effectiveness of public and private online services, electronic business and electronic commerce in the Union.*

04 - *The Commission communication of 26 August 2010 entitled ‘A Digital Agenda for Europe’ identified the **fragmentation of the digital market, the lack of interoperability and the rise in cybercrime as major obstacles to the virtuous cycle of the digital economy.** In its EU Citizenship Report 2010, entitled ‘Dismantling the obstacles to EU citizens’ rights’, the Commission further highlighted the need to solve the main problems that prevent Union citizens from enjoying the benefits of a digital single market and cross-border digital services.*

72 - When adopting delegated or implementing acts, the Commission should take due account of the standards and technical specifications drawn up by European and international standardisation organisations and bodies, in particular the European Committee for Standardisation (CEN), the European Telecommunications Standards Institute (ETSI), the International Organisation for Standardisation (ISO) and the International Telecommunication Union (ITU), with a view to ensuring a high level of security and interoperability of electronic identification and trust services.



In this moment EA is making a survey over all the EU Accreditation Bodies, in order to understand exactly what approach they have had in performing the Accreditation process.

What is more than a feeling, is that the EA recommendation to adopt ETSI Standard to perform Accreditation was not adhered to, in different level of scattering.

This is only a feeling.

If confirmed, that some EU partner didn't follow EA addresses, **a real concern will rise.**

No certainty about the level of security required by the Commission and by the Parliament could be guaranteed.



Using Standards is the better approach in order to perform a repeatable measure of TSP organisation, processes and services provided, against issues of security and trust, with a high level of dependability, among different countries in Europe.



This chance to measure performances and to assess organization rules and processes **is fundamental** in order to guarantee National Authorities about the "cybersecurity" resilience, the services level, that are the basis to confirm the level of liability stated by different TSP.

The above assessment results, when conforming ETSI Standards, are the ones needed to be Qualified by National Authorities and give a predictable guarantee to the market, **to create the needed confidence in Qualified**

Trusted Services by:

- **Fighting against fragmentation of approaches to electronic services;**
- **Fighting cybercrime that could be able to compromise services;**
- **Creating interoperability of services [that needs a standardisation approach!!]**

Article 20

Qualified trust service providers shall be audited at their own expense at least every 24 months by a conformity assessment body. The purpose of the audit shall be to confirm that the qualified trust service providers and the qualified trust services provided by them fulfil the requirements laid down in this Regulation.

The qualified trust service providers shall submit the resulting conformity assessment report to the supervisory body within the period of three working days after receiving it.

The question is:

HOW TO CONFIRM... IF THERE ARE NO STANDARD FOR AUDITING, OR IF ANY PLAYER ADOPT DIFFERENT RULES.

Without standards as references, the assessment processes are neither solid nor sound, because too many uncontrolled issues are affecting the same process.

One over the other: in different TSP, with different CAB, the audit approach could be probably different, giving a dramatic different level of dependability.



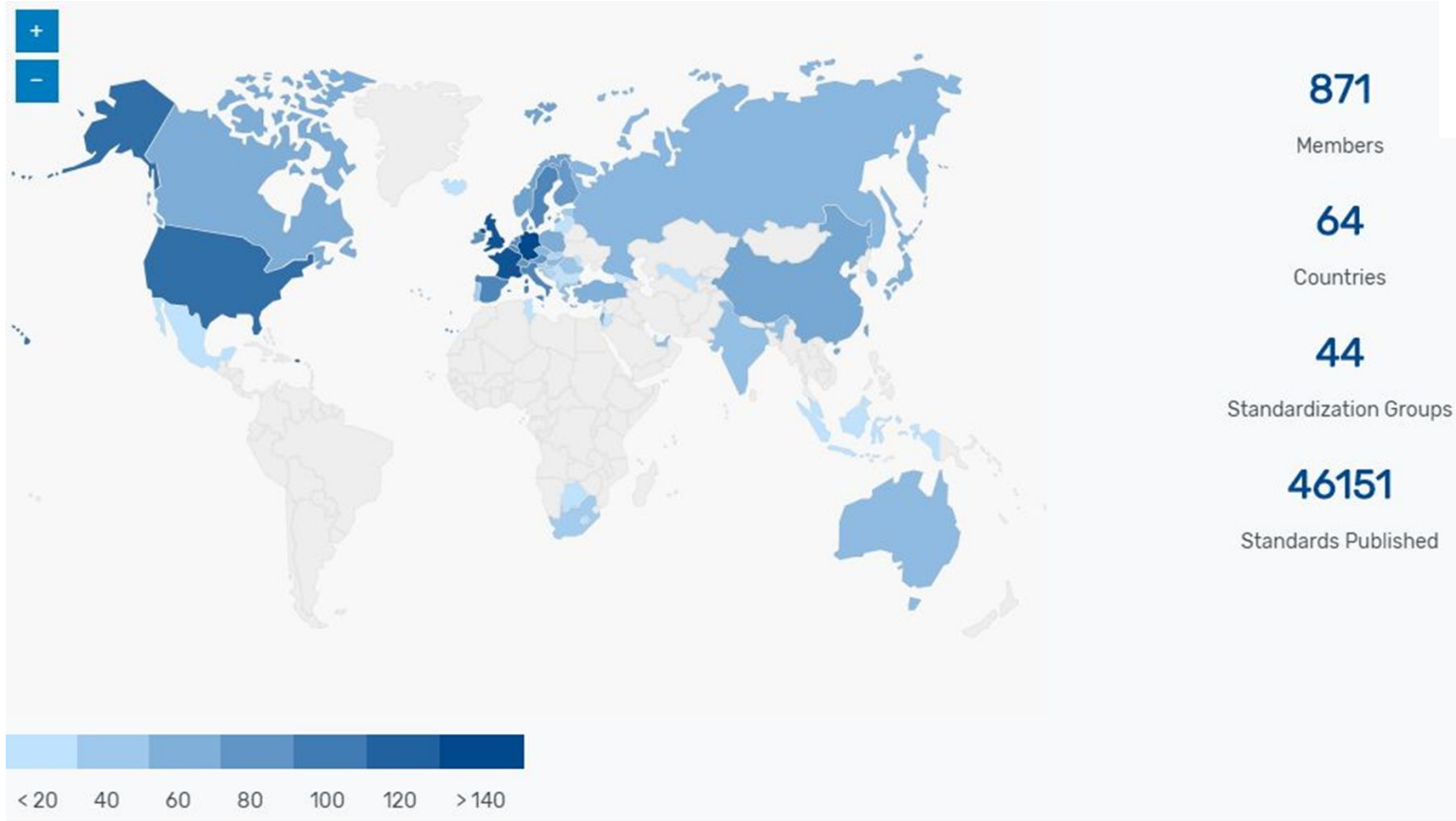
Conformity Assessment processes was created exactly to have the chance to measure processes and organizations against a Benchmark.

The Benchmark is the use of Accepted Standards.

Standards are a must also to drive the Auditor competence, behaviour and approach. There's difference between a 17065 and 17021 approach.



ETSI EN Standards are the accepted output of the best competences in Europe.



If any National Authority, or other player, believe to have a better mean, ETSI is the right place where to analyse this hypothesis and transform the same, if possible, in common value.

Value of knowledge is real, when it is for everybody.

At the moment, what we can say is that Regulation 910 allows the Commission (72) to ***adopt delegated or implementing acts.***

Next one should be the formal adoption of **ETSI EN 319 403** as Accreditation Standard to address AB processes.

From this approach the adoption of other ETSI EN Standard should be a real valuable consequence.



Thanks for your attention



www.accredia.it



info@accredia.it