Minutes: Trust Services Workshop

WORKSHOP CONTEXT

On June 30th ENISA conducted, in collaboration with the European Commission eIDAS Task Force, a workshop on the European Trust Services. The objective of the workshop was to provide a forum to the three stakeholder communities in the qualified trust service market, namely: trust service providers, conformity assessment bodies and supervisory authorities, to exchange ideas on priorities, best practices, etc.

The workshop was the first of a series of activities launching the Forum for the Trust Services Market. This forum is meant to become a place for open discussions related to the entry into force of the Regulation 910/2014 on electronic identification and trust services for electronic transactions in the internal market.

The main objectives of the workshop were:

- To share good practices and experience as well as views on various aspects of the implementation of eIDAS by the concerned stakeholders and their compliance to EU legislation
- To understand the priorities and needs of trust service providers in the development of the eIDAS Regulation.
- To exchange ideas on the positions of the different stakeholders in aspects like standards, certification, qualification, etc.
- To discuss strategies to promote the use of qualified trust services in Europe.

CONTENT OF DISCUSSIONS

The workshop consisted in a series of presentations, panels and open discussion sessions. Before the thematic sessions started, two introductory presentations took place. The first presentation “eIDAS Regulation – State of Play” described the ongoing developments of the eIDAS Regulation, the current status of implementing acts and secondary legislation, as well as the ongoing activities to facilitate the involvement of key stakeholders.

The second presentation “CEF TELECOM - Building block DSIs” introduced the instruments and initiatives in place within the CEF program where trust services are building blocks (eIdentification and eSignature, eProcurement, eInvoicing, etc.) and pointed to participants where to access all the relevant information and calls.

The presentations were followed by five thematic blocs which consisted in a series of presentations and panels where key topics regarding the development of the framework around eIDAS where discussed:

- Supervision under eIDAS: full supervision versus light ex post monitoring
- Certification of QSCDs
- Standardisation and conformity assessment of qualified TSPs
- Increasing market adoption of qualified trust services
- Risk management, security measures and security breach notifications

THEMATIC SESSIONS

"Supervision under eIDAS: full supervision versus light ex post monitoring"

The session started by a presentation to describe the two models of supervision under eIDAS, for qualified and non-qualified providers, and a description of the common and specific requirements. The presentation was followed by a panel where participants discussed about the current supervision of trust services providers and how it can evolve with the entry into force of the Regulation 910/2014. The main points discussed were:

- Currently many TSPs are subject to supervision, not only from national supervisory bodies, but also from commercial entities in order for TSPs to be included in the root stores of these commercial organizations. The requirements of these other entities are not lighter than the ones set for qualification. TSPs face an increasing compliance cost burden.
- There are important differences between supervisory bodies, not all of them have the same resources and supervision capabilities, which can lead to TSPs from different Member States being subject to different levels of supervision.
- Another issue are public sector TSPs that are supervised by the national supervisory body, which in some cases are subject to a lighter type of supervision.

"Certification of QSCDs"

This session consisted on two presentations. The first presentation "IT security certification of QSCDs under Regulation 910/2014", clarified the existing framework for certification of QSCD and presented the possible options ahead to define such framework under the new Regulation, which still needs to be defined through secondary acts.

The second presentation: "Giving confidence in Server Signing for eIDAS using Common Criteria evaluation", presented the technical architecture of remote server signing, the associated risks and how they could be mitigated, and the possibilities for remote server signing QSCD within this model via the existing certification framework of Common Criteria.

"Standardisation and conformity assessment of qualified TSPs"

The session started by two presentations. The first, "standardization development status" offered an update on the current situation in the drafting and publication of European standards for trust services. The second, "assessment of standards for TSPs" introduced the 2015 ENISA study aimed to map the published and draft European and international standards for trust services to the requirements set in the Regulation.

The presentations were followed by a panel where participants discussed about the current standardization status and how to implement a harmonized framework for conformity assessment. The main points discussed were:

- Common points of reference for the audits exist already – ETSI, CEN and ISO standards fill basically all areas.
- Standards developed under mandate m460 will give more precise rules for CABs and will provide coverage for new technologies and aspects. They will also contribute to help stakeholders to assess presumption of compliance of TSPs

- Current framework provides already a good auditing regime. More guidelines are expected in relation to eIDAS
- A challenge for the cooperation between CABs and TSPs is how to reach the common understanding on minimal requirements.
- Regular exchange of views from TSPs and CABs has been judged needed, especially in the first period after eIDAS requirements related to audits become mandatory

"Increasing market adoption of qualified trust services"

The session started by a presentation to introduce ENISA's 2015 study on the introduction in the trust services market of qualified website authentication certificates. The presentation was followed by a panel where participants discussed about possible business cases for the new trust services and how their market adoption can be promoted. The main points discussed were:

- The increase of online transactions, both involving public administration but also private sector, opens a large market for trust services.
- Qualification can be perceived as a quality and transparency mark for customers. In order for this to be effective, it is important for authorities to increase awareness of what qualification means.
- Some sectors, which require high assurance level in transactions, like the government and banking sector sectors, can benefit from the clarified legal framework qualification provides (liability, burden of proof, etc.).
- It is important to keep in mind global interoperability, as the online services market is becoming more and more globalized; providers should be able to operate globally, not only in Europe.

"Risk management, security measures and security breach notifications"

The session started by a presentation which introduced ENISA's 2015 study on incident reporting for TSPs. It was followed by a panel where participants discussed topics related to the obligations set in Article 19 of the eIDAS Regulation regarding risk assessment, security measures for TSPs and reporting of security and trust breaches. The main points discussed were:

- Whether authorities should intervene in the risk assessment process, or this should be undertaken solely by the TSP taking into account its specific risk environment.
- Available recommended security measures for Art 13a of the Telecom Package could be used as a candidate for minimum security measures.
- There is a good coverage for standards on security measures for TSPs, there is no urgent need to develop new standards on this area.
- Harmonization of security measures is a difficult task, but it should be addressed as different security requirement are in contrast with digital single market. Use cases should be taken into account, but no such cases exist at the moment.

FURTHER ACTIONS

The discussions that took place showed that there is interest from participants, both from industry and the public sector, in continuing this initiative. In this respect a number of possibilities of the follow up were discussed:

- To create national events with the same format as the workshop, facilitating the discussion among industry and supervisors on the ongoing issues related to the entry into force of the application of the rules applicable to trust services set in the Regulation, at national level.
- To conduct periodical workshops with a similar format to this first one, to cover the most relevant topics that will arise with the sequential development of secondary legislation to the Regulation.
- To open electronic forms of communication, by means of, for example, an online platform or a mailing list, to facilitate the exchange of information among stakeholders.

EVALUATION OF RESULTS

Overall the workshop was successful. The main results/conclusions can be summarised as follows:

- The number of participants exceeded expectations, approximately 110 participants, comprised of a balanced representation of Member States competent authorities and stakeholder communities.
- Participants actively contributed to the discussions in the panels as well as to the open session that concluded the workshop.
- The agenda was organized around different thematic sessions that were relevant to the ongoing discussions, which facilitated the interaction with the public. Speakers were also balanced in terms of MS and stakeholder communities.