FORUM OF EUROPEAN SUPERVISORY AUTHORITIES
FOR TRUST SERVICE PROVIDERS

Luxembourg, 4 March 2020

Position Paper
On the review of the eIDAS Regulation
FESA's answer to the European Commission's consultation

The Forum of European Supervisory Authorities (FESA) for trust service providers, is open to national bodies responsible for supervision and/or trusted lists in accordance with the eIDAS Regulation[1].

Supporting the idea of the Digital Agenda for Europe, FESA sees itself as an experienced and competent body that supports the cooperation, information and assistance among its members and facilitates the exchange of views and agreement on good practices corresponding to Arts.17(4)(a), (c) and Art.18(1) of the eIDAS Regulation.

FESA intends to advance the harmonization of supervisory bodies' activities, to develop common points of view for the dialog with political or technical institutions, in particular the European Commission and standardization institutions, and to establish a levelled European playing field for trust service providers in terms of supervision.

Review of the application of the eIDAS Regulation

The eIDAS Regulation entered into force on 17 September 2014. It has been highly beneficial in developing the European Digital Single Market with regards to trust services. Indeed, numerous trust services have since been qualified and an important number of the technical standards on which trust service providers and conformity assessment bodies rely on have been published. Moreover, there is constructive cooperation on this topic between Member States, in particular via FESA and the ENISA/ Article 19 working group.

FESA consulted its members for feedback to the European Commission as review of the application of the eIDAS Regulation is prescribed for 2020[2]. The FESA members submitted 35 suggestions for consideration focussing on the five objectives Convenience, Consumer choice, Protecting data and privacy, Level playing field and Global reach of eIDAS as indicated by the European Commission.

In this Position Paper FESA presents seven suggestions of maximum importance unanimously supported by its members[3]. These suggestions have been discussed extensively within the community over the years[4].
FESA is convinced that a timely implementation of these suggestions will contribute to achieving the afore mentioned objectives of the eIDAS Regulation, and the European Commission.

[1] Regulation 910/2014/EU of the European Parliament and Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market and Repealing Directive 1999/93/EC, OJ L257.
[2] Art. 49 eIDAS Regulation: "Review - The Commission shall review the application of this Regulation and shall report to the European Parliament and to the Council no later than 1 July 2020. The Commission shall evaluate in particular whether it is appropriate to modify the scope of this Regulation or its specific provisions, including Article 6, point (f) of Article 7 and Articles 34, 43, 44 and 45, taking into account the experience gained in the application of this Regulation, as well as technological, market and legal developments."
The report referred to in the first paragraph shall be accompanied, where appropriate, by legislative proposals.
In addition, the Commission shall submit a report to the European Parliament and the Council every four years after the report referred to in the first paragraph on the progress towards achieving the objectives of this Regulation.
[3] The FESA members are requested to submit the other suggestions directly to the European Commission.
[4] A detailed overview of these seven suggestions in relation to the five objectives is presented in Annex I.

Seven FESA Suggestions reviewing the application of the eIDAS Regulation

1. Standards for the accreditation of Conformity Assessment Bodies (eIDAS Arts. 20(4) and 24(2))
   1.1. Observation
   We see a wide variety in certification schemes used by Conformity Assessment Bodies (CABs), both in audit effort and quality, which is reflected in Conformity Assessment Reports (CARs) received by Supervisory Bodies (SBs). Although there is a recommendation of the EA, there is no mandatory accreditation scheme for the CABs, further increasing the risk of a non-harmonized approach of conformity assessments of trust services. This situation leads to a clear risk that (Qualified) Trust Service Providers ((Q)TSPs) will turn to the CABs that are operating a less demanding (and less costly) certification scheme.
   1.2. Motivation
   Harmonization in conformity assessment of Qualified Trust Services (QTSs) is essential for building actual trust in trust services and for mutual recognition of trust services. Harmonization of accreditation and Conformity Assessment Reports (CARs) will allow fair competition between the CABs and will reduce the incentive for QTSPs aiming at the lowest price. Clear and transparent accreditation and certification schemes will foster the uptake and global reach of the eIDAS Regulation. The credibility of conformity assessments and the quality of the CARs will enhance adoption of harmonized accreditation and certification schemes. It will enable TSPs to better make a weighed choice in selecting a CAB without having to make concessions on the quality of the CARs.
   1.3. Proposal
   We propose to promulgate an implementing act as foreseen in article 20(4) referencing ETSI EN 319 403-1 and ETSI EN 319 403-3.

2. Practices regarding remote identification (eIDAS Arts. 24(1)(b) and (d))
   2.1. Observation
   Currently acceptance of remote identification methods (equivalent to physical face-to-face) is left to the discretion of each Member State SB, without any clear requirements. This creates a heavily unlevelled playing field for QTSPs at European level. The lack of requirements will presumably lead to a race to the bottom. We need clarification on the requirements applying to the physical presence mentioned in Art. 24(1)(b).
   2.2. Motivation
   Ensure a high level of assurance promoting the global reach of eIDAS. We aim at a level playing field for QTSPs delivering qualified certificates on a remote basis. SBs see a growing demand from the market for remote identification according to Article 24(1). Harmonizing the requirements on practices regarding remote identification will further foster trust in the services from the eIDAS Regulation. An implementing act is needed referring to standards with respect to which remote identification tools and procedures can be evaluated.
   2.3. Proposals
   We propose to amend the eIDAS Regulation in order to give the European Commission the mandate for an implementing act specifying the requirements for remote identification according to Article 24(1). Eliminating the text “recognized at a national level” in matters concerning remote identification in Art. 24(1)(d) should also be considered.

3. Server signing/sealing certification process (eIDAS Art. 29(2) and Annex II Arts. 3 and 4)
   3.1. Observation
   Stakeholders have different views on remote signing/sealing. With the increasing use of remote identification this issue will get more problematic and eventually put the trustworthiness of the eIDAS framework at stake.
   3.2. Motivation
   Providing greater clarity on the requirements for remote signing systems will lead to a higher level of assurance and confidence that such systems are meeting the requirements of the eIDAS Regulation. Similar to other harmonisation initiatives, this will provide enhanced confidence and easier decision making for consumers whilst also reducing potential variances in the security of such systems. This in turn will lead to greater confidence in the overall eIDAS

scheme by non-EU parties and thus support global adoption. There is a need to make certification more comparable and give legal certainty to models like on the fly certification and subscribers managed Qualified electronic Signature Creation Devices (QSCDs).

3.3. Proposal

We propose to amend CID (UE) 2016/650 with the inclusion of EN 419 221-5 and EN 419 241-2 allowing a harmonized certification process in all Member States. Clarify the requirements regarding server signing services, also known as remote signing and signing on behalf. Specifying the type of QTSP that can manage signature or seal creation data on behalf of the signatory shall be considered. In particular Annex II of the eIDAS Regulation must be clarified.

4. Requirements of Qualified Trusted Services (eIDAS several articles).

4.1. Observation

ETSI has performed outstanding work producing almost all the standards called for by the Implementing Acts of the eIDAS Regulation regarding qualified trust services. These standards set a clear framework for (Qualified) Trusted Services ((Q)TSs) and help the eIDAS community to branch out on a global scale. Despite this work, the standards are yet not officially recognized and therefore there are still inconsistencies between (each of) the QTSs.

4.2. Motivation

Granting TSPs clarity on the requirements to comply with the eIDAS Regulation, thus harmonizing the products of European QTSPs. It would help data protection and privacy since these requirements would be a mandatory level of security guaranteeing a security framework. Ensuring harmonization of the different requirements and practices among the Member States, thus create a level playing field. Current ETSI standards set a clear framework for QTSs. This clear framework would help adoption outside of the EU and help the global reach of the eIDAS Regulation.

4.3. Proposal

We propose a mandatory adoption of the Implementing Acts already foreseen by the eIDAS Regulation, adopting the currently published standards concerning the requirements of QTSs (eIDAS Arts. 24(5), 28(6), 32(3), 33(2), 34(2), 38(6), 40, 42, 44(2) and 45).

5. Qualified electronic Signature Creation Devices (QSCDs) conformity certificate (eIDAS Arts. 24(2)(d), (e) and 30(1))

5.1. Observation

Assurance of conformity, for Qualified electronic Signature Creation Devices (QSCDs), is given once and is valid for an undefined period of time, regardless of discovered vulnerabilities and new requirements.

5.2. Motivation

The rise of remote QSCDs increases the need of periodic vulnerability assessment and set limitations to validity period of QSCDs. This might also impact the eID infrastructure of Member States, since some QSCDs are used as electronic identity cards.

5.3. Proposal

We propose to limit the validity of a QSCDs' conformity certificate and demand a periodic vulnerability assessment. This could be reached by promulgating Implementing Acts, containing details on the validity period of QSCDs, including SSCDs, on the withdrawal of the QSCD conformity certificate (e.g., in case of a vulnerability that has been discovered), and on the frequency of vulnerability assessments.

6. Sharing information on vulnerabilities and almost incidents (eIDAS Art. 19(2))

6.1. Observation

In order to contribute to trust in the European Digital Single Market it is essential that the SBs receive the necessary information on vulnerabilities and almost incidents as soon as possible. Sharing information on vulnerabilities, almost incidents and threats is a pre-requisite for building trust. The ROCA vulnerability showed that all Member States and stakeholders had very different modus operandi.

6.2. Motivation

Sharing information in general and about technical vulnerabilities without providing specific details of national QTSPs will offer all involved parties convenience. Recent events show that early warnings are essential (e.g. ROCA, Grenfell Towers, Ponte Morandi Genua). Acting upon early warnings will help to mitigate possible negative impact on the trust ecosystem as a whole and help to retain the essential trustworthiness consumers expect from eIDAS governed Trust Services.

6.3. Proposal

We propose to provide clarity on sharing information on vulnerabilities and almost incidents. Notification to interested parties should be harmonized. We propose to provide guidelines based on recital 39 and to promulgate an Implementing Act as foreseen in Art.19(4).

7. Termination of Qualified Trust Services (eIDAS Art. 24(2)(i))

7.1. Observation

At the moment the eIDAS regulation does not have any requirements on the termination of QTSs except a general requirement for the termination plan, causing different practices and understandings of this process. Currently there is no common understanding on what should be arranged beforehand for example financially, on different scenario's, on the continuity of active services, logs or specific services for the signatory.

7.2. Motivation

QTSPs, like any other company, may find themselves in a situation where they have to voluntarily or forcefully terminate their services. To ensure sustainability and durability of qualified trust services and to boost user confidence in the continuity of qualified trust services it is essential that QTSPS have provisions in place to ensure a smooth transition. Harmonization of requirements and practices related to termination of qualified trust services among all Member States will ensure a common understanding and foster a levelled playing field.

7.3. Proposal

We propose to harmonize the requirements related to termination of qualified trust services. We propose to promulgate an Implementing Act as foreseen in Art. 24(5).

Annex 1. FESA – evaluation of the eIDAS regulation

			Does it contribute to:							
Nr.	**Suggestion for improvement**	**Links to**	**Convenience?**	**Consumer choice?**	**Data protection and privacy?**	**A Level Playing Field?**	**The global reach of eIDAS?**	**Needs Implementing Act(s)?**	**Additional Notes**
1	Adopt standards for the accreditation of CABs and the conformity assessment (report) of QTSPs. Implement an accreditation scheme based on a mandatory adoption of ISO 17065 and standard ETSI TS 119 403-3 as the basic minimum for the drafting of CARs and an accreditation scheme based on ETSI EN 319 403-1.	Art. 20.4(a,b)	This will allow greater competition between the CABs and would reduce the perverse incentive of discriminating by price that harms the CABs that perform with higher quality. Harmonisation of accreditation practises will enhance the quality and uniformity of CARs. It will help TSP‘s to better make a weighed choice in selecting a CAB without having to make consession on the quality of the CARs. For SB‘s it will enhance the supervision tasks.		Implementing the (adopted) standards will eventually lead to an increased level of trust in the security of the offered services.	CABs’ accreditation are not harmonized between Member States. Adopting and implementing standards will enhance a level playing field. Clarification in accreditation scheme would also reduce administrative burden for all the stakeholders and ease and encourage to acquire accreditations.	A framework of standards for conformity assessment bodies will enhance trust in eIDAS services and improve global reach.	Yes, in line with art. 20 par. (4) of the eIDAS Regulation, to adopt standards and set a minimum to enhance harmonization of conformity assessment (reports). There is a widely supported need to implement a certification scheme on basis of the standards ISO/IEC 17065 and ETSI EN 319 403 (for the accreditation of conformity assessment bodies) and ETSI TS 119 403-3 (for conformity assessment reports). MS‘s do oppose the suggestion to formalize accreditation frameworks for the eIDAS QTS standards adopting certification schemes under the Cybersecurity Act.	There is a wide variety in certification schemes in use by CABs, both in scope and quality, which is reflected in CARs received by SBs. SB's don't have a legal basis to reject CAR's.

Annex 1. FESA – evaluation of the eIDAS regulation

Nr.	Suggestion for improvement	Links to	Convenience?	Consumer choice?	Data protection and privacy?	A Level Playing Field?	The global reach of eIDAS?	Needs Implementing Act(s)?	Additional Notes
2	Harmonize the requirements on practices regarding remote identification.	Art. 24.1(b,d)	Stakeholders have different views on remote identification. This situation is not beneficial to the purpose of the regulation.		QTSPs could create establishments in other countries with a less strict rule set.	Currently remote identification (equivalent to physical face-to-face) is left to the discretion of each Member State SB, without any guidelines in the regulation (or standards). This can create unfairness in competition for QTSPs at European level because they depend on the SB where they are established.	Clear guidance on remote identification will help the Global reach of eIDAS.	Yes, the implementing act should refer to standards with respect to which remote identification tools can be evaluated.	Strict and specific requirements in the regulation (and in standards) is needed. It could be considered to eliminate the text " recognized at a national level" in art. 24.1.d. Remote ID should be made one more possibility at EU level, with the same requisites for all MSs set in an act of execution. The same should be done with Digital Onboarding. Otherwise we would be encouraging current "legal environment shopping" with a race to the bottom.

Annex 1. FESA – evaluation of the eIDAS regulation

Nr.	Suggestion for improvement	Links to	Convenience?	Consumer choice?	Data protection and privacy?	A Level Playing Field?	The global reach of eIDAS?	Needs Implementing Act(s)?	Additional Notes
3	Amend CID (UE) 2016/650 with the inclusion of EN 419 221-5 and EN 419 241-2 allowing a harmonized certification process in all MSs. Clarify the requirements regarding server signing services, aka as remote signing and signing on behalf. Specify the type of QTSP that can manage signature or seal creation data on behalf of the signatory.	Art. 29.2, Annex II 3,4	There is a rapid growing demand for remote signing implementations. It would open a market for one more QTS.	There is a rapid growing demand for remote signing implementations. More clarity will give the consumer the ability to make an informed decision.	There is a strong need for harmonization in order to ensure an adequate and homogeneous level of security of all implementations across the European Union.	Stakeholders have different views on remote signing. With the increasing use of remote identification this issue will get more problematic and eventually put the trustworthiness of the eIDAS framework at stake. This situation is contrary to the purpose of the regulation. Amending CID (UE) 2016/650 with the inclusion of EN 419 221-5 and EN 419 241-2 and clarifying the requirements will allow a certification process which creates a fair and equal playing field.	Clarity on this will raise the applicability of eIDAS trust services on a global scale.	IA needed to amend CID (UE) 2016/650 in order to allow for a harmonized certification process.	There is a strong need for harmonization in order to ensure an adequate and homogeneous level of security for all QSCDs solutions across the European Union as well as guarantee a fair playing field between vendors. The certification of remote QSCDs is performed according to national alternative certification processes in some countries. The main vendors of HSMs and providers of signature solutions have contributed significantly to Protection Profiles. The type of QTSP that is required for managing signature creation data is not specified. We would welcome a requirement stating that this is limited to TSPs issuing qualified certificates for ESig or ESeal. Based on Art 39 1. , Annex II applies “mutatis mutandis” to qualified seal creation devices. NOTE: Only the SAM PP (CEN EN 419 241-2) may be included in the IA since the HSM certified against the CEN EN 419 221-5 is required to support the operation of the SAM.
4	Harmonize the requirements of all qualified services. Build upon the already performed standardization work.	eIDAS	It offers companies clarity on the requirements to comply with eIDAS and allows harmonizing the products of European QTSPs.		It will ensure a minimum level of security and will help to guarantee a security framework.	It will ensure harmonization of requirements and practices among all Member states and thus create a level playing field.	ETSI has performed outstanding work producing almost all the standards called for by the implementing acts of the regulation. These standards set a clear framework for (qualified) Trusted Services and help the eIDAS community to branch out on a global scale.	Yes, the adoption of results of standardization of requirements of qualified services as implementing acts.	

Annex 1. FESA – evaluation of the eIDAS regulation

Nr.	Suggestion for improvement	Links to	Convenience?	Consumer choice?	Data protection and privacy?	A Level Playing Field?	The global reach of eIDAS?	Needs Implementing Act(s)?	Additional Notes
5	Limit the validity of a QSCDs' conformity certificate and demand a periodic vulnerability assessment.	Art. 24.2(e); Art. 30.1	Patch mechanisms in scope of the certification and enforced vulnerability assessment would help to mitigate for known vulnerabilities.	Consumers depend upon the QTSP using specific QSCD's. Limiting validity might lead to a broader market and that might enhance the freedom of choice for consumers.	Limitation of the validity of QSCDs' certificate helps to manage the security of the QSCD over its lifetime, and to detect any vulnerability as soon as possible (and hopefully before it goes public). It would prevent the QTSPs to stick to older and possibly vulnerable technology too long.	It will give QSCD manufacturers the chance to present new technology and products. It might create an opportunity for new QSCD manufacturers.	A more secure and reliable QTSP framework will help to enhance the global trust.	Yes, the implementing act should contain details on the validity period of QSCDs, on the withdrawal of the conformity certificate from a QSCD (e.g., in case of a security vulnerability that has been discovered), and on the frequency of vulnerability assessments.	The rise of remote QSCDs may increase the need of periodic vulnerability assessment and set limitations to validity period of QSCD.
6	Clarity is needed on sharing info on vulnerabilities and almost incidents.	art. 19.2	As long as shared information is general and about technical vulnerabilities without providing specific details of national QTSPs it will offer all involved parties convenience.		Recent incidents show that early warnings are essential (e.g. ROCA, Grenfell Towers, Ponte Morandi Genua). Acting upon early warnings will help to mitigate possible negative impact on the trust ecosystem as a whole.	Notification to interested parties should be harmonized. In ROCA, different MSs had very different modus operandi.	To contribute to trust in the European Single Market it is essential that the supervisory authorities receive the necessary information on vulnerabilities and almost incidents as soon as possible.		Sharing information on vulnerabilities and almost incidents and threats is a pre-requisite for building trust. Some modification may be needed of the legal text, in order to enforce this requirement
G	Harmonize the requirements related to termination of qualified trust services	Art 24.2 i)	It will give the market more trust that termination of QTSs follow a standardized path.		It will strengthen the data protection and privacy even after a QTSP has been terminated.	It will ensure harmonization of requirements and practices among all Member states and thus create a level playing field.		Yes. More details on termination of QTS could be placed within an IA	As at the moment eIDAS regulation does not have any requirement on termination of QTS (except general requirement for the termination plan) therefore there are different practices and understandings about this process (on what condition QC issued before termination of QTS could be used further, shall SB take over QTS in case no one form the market agrees to do that, how it should be reflected within TSL, etc.)