eIDAS Review

InfoCert Group Contribution to the revision process of the eIDAS Regulation

SUMMARY

AREAS OF ATTENTION

InfoCert Group believes that the eIDAS Regulation and the creation of an interoperable Digital Single Market for trust services is crucial to build a digital society based on trust, security and protection of natural and legal person in Europe.

InfoCert operates in more than 20 Countries in Europe, providing Qualified Trust Services and e-Identity solutions in different vertical markets: we enjoy a privileged point of view on the strengths and weaknesses of the Regulation and we've seen the different implementation approaches across Europe.

In the following paragraphs we will provide some points of attention and some ideas of practical amendments that could help to evolve the current situation toward a better interoperability in order to foster the spread of cross-border trusted transactions.

1.1 IDENTIFICATION METHODS

Article 24 of the Regulation offers a wide range of defined identification methods, plus letter d) that permits to the QTSP to submit for approval to the Conformity Assessment Body an additional identification method, that gives the same level of assurance and security of the concrete presence.

InfoCert believes that **the aim of article 24 shall be strengthen** because it permits to continuously adapt the eIDAS ecosystem including or excluding identification methods enabled or deprecated by technological evolution.

Some standardization bodies are working actively on the definition of standards and guidelines for some of the new identification methods (i.e. ETSI for video-identification): these initiatives are important to improve overall security, but **these standards should not become binding regulations**.

In our opinion, QTSP should be able to quickly dismiss deprecated technologies and, at the same time, have the option to adopt more secure, innovative and technologically advanced identification methods and solutions without having to wait for a new standard or regulation to become effective.

1.2 MANAGEMENT OF PRIVATE KEYS

The actual formulation of the **Annex II** of the Regulation **permits to any Qualified Trust Service provider to generate or manage electronic signature creation data** on behalf of the signatory.

We believe that this possibility doesn't guarantee the highest level of protection to the holder of the qualified certificate, simply because a TSP that has been qualified for a service different from signature and seal might not necessarily possess all the capabilities required to properly manage certificate keys.

We suggest **restricting the possibility to manage private keys just to QTSPs that have been qualified for Qualified Electronic Signature, Qualified Seals** or Qualified Website Authentication Certificates.

1.3 QUALIFICATION OF SIGNATURE CREATION DEVICES AND SIGNATURE SERVICE

The actual **process to certify a signature creation device is cumbersome** and brings to an odd and fragmented situation where:

- there are many certification standards and approaches,
- the perimeter of certification differs between both certification bodies and signature devices,
- the patch management is outside the certified perimeter, so in case of a new vulnerability this cannot be patched without a re-certification of the device, often forcing QTSPs to keep unsafe devices in order to maintain the certification status,
- unlimited certifications are granted to some classes of devices on one extreme while some protection profile might prove to be practically impossible to be fully respected on the opposite extreme.

We need to **simplify the acceptance and management of QSCD without giving up security** and getting to a more homogeneous approach between Member States.
Considering the role of ENISA, the Commission and the Member States could entitle such authority to define a **unique schema for security certification of devices, shaped around the already existing and accepted international security schemas as Common Criteria EAL 4+.**

We notice a lack on eIDAS in **regulating the remote signature service**: even if the trust provider is qualified, the certificate is qualified, the signature creation device is qualified, when the subject uses his/her private keys there is a part of the overall process that is not qualified and doesn’t follow any specific rule.
The definition of a qualification schema or, if not possible, functional recommendations on the remote signature process could improve the overall trust and security and the protection of the subject. In that regards, there are already available some (albeit partial) standards like the ones defined by CSC Consortium.
Therefore, we need to **avoid the risk to overburden the overall system with bureaucratic procedures that don’t add much to security**: the risk is to create unnecessary frictions in the Qualified Signature user experience that will impact on the adoption of QCert in the Single Market to the benefit of less secure and less trustworthy solutions. A clear example of such unnecessary friction is the provision of mandatory detailed instructions on how the document to be signed should be displayed before the signature.

1.4 ROLE OF CABS AND SUPERVISORY BODIES

The creation of a trustworthy, interoperable eIDAS-based Digital Single Market is directly affected by the quality and homogeneity of the approaches of Supervisory Bodies and Conformity Assessment Bodies.

We need more harmonized national qualification procedures between Member States, smoothing the divergence in approaches of the Supervisory Bodies but, at the same time, we also need to **avoid that bureaucratic and too rigid interpretation prevails, destroying the spaces to do business** and opening the market to low-compliant, less-secure, less-trustworthy but, at the same time, highly usable solutions.

We believe that even the role of Conformity Assessment Bodies should change; today each QTSP is audited twice: by the CAB that – with different approaches throughout Europe – performs deep audits on implemented services and processes, and by the Supervisory Body that, not always fully trusting the CAB report, re-executes the same audits and analysis.
There's a need to clarify the liability schema for CABs' activity: if a CAB is liable toward the SB on the audited perimeter, the SB should trust more the conformity report and play the role of ex-post auditing authority over QTSP. Otherwise, the auditing process should be revised **avoiding to QTSPs the unnecessary costs of a double, redundant layer of audit**.

1.5 SUPERVISORY BODIES AND EIDAS ENFORCEMENT

The creation of a Digital Single market passes even through the generalized acceptance and implementation of eIDAS Regulation in the internal processes of each Member State.

We have seen situations of MS introducing specific requirements **creating unnecessary national barriers**. For example, some countries demand specific technical requirements and specific data in the certificates in order to use it for accessing public services or in public tender and procurement processes. This approach undermine interoperability and forces multi-national companies to use different certificates to operate in different Member States. We suggest a stricter control from the Commission on similar situations.

In addition, we believe that one of the greatest strengths of eIDAS is its universality, i.e. its ability to build an infrastructure of trust accessible to business in all industries and sectors. Many of these sectors are regulated by national authorities in charge of issuing Circulars, Orders and second-level regulation. Even if the eIDAS Commission has been able to influence different Directives and Regulations (ex. AML V Directive, PSD2 Implementation, etc), **many National sectoral authorities are still ruling without considering the existence of a super-national qualified trust services Regulation**. The result is a fragmented situation where a foreigner QTSP is often not in the conditions to compete on equal terms with local players.
We suggest to **evolve Supervisory Bodies toward the role of eIDAS enforcing authorities**, with the responsibility to influence and even sanction national authorities that are blocking or slowing the proper and smooth application of the eIDAS Regulation.

1.6 QWAC, VALIDATION SERVICES, DELIVERY SERVICES

The main priorities for implementing the Regulation have been so far the development of the national eID schemas and the security of QCERT for signatures and seals. We believe there are three additional priority areas that the Commission should focus on: enforcing the acceptance of QWACs, make available a single validation service and develop a European-wide interoperable system of qualified delivery.

Qualified Webserver Authentication Certificates are a powerful tool to enhance the security of server-to-server transactions and now are bringing trust and interoperability into PSD2 transactions between PSPs. Unfortunately, the **CA-Browser forum is creating resistance and**

tensions in accepting it, substantially ignoring the trust and auditing framework behind the QWAC. We suggest a norm to **force the browser providers operating in Europe to accept the eIDAS compliant QWAC in the same way TSL certificates are accepted**.

The validation of the signature is crucial for the owner of the signed document, that should be in the position to verify with a secure, free and independent service the validity of the signature. Today this seems to be a market failure, because the private sector doesn't have the incentive to create the validation service, being no revenues attached to it.
European Commission DSS is a partial response: lacking a clear commitment over the value of the service, the liability schema, the service level guaranteed, it is under-used while instead it could play an important role in the implementation of eIDAS enabled processes. We believe that this experience should become stable and regulated, with a **Qualified Signature/Seal Validation service provided and managed by the EU**. A second option, if a more decentralized architecture is preferred, would be that each Supervisory Body operates a local validation service based on a common European framework developed by the Commission, to avoid differences of approaches and strengthen the interoperability.

Finally, we believe that **an interoperable, EU based Qualified Electronic Delivery Service could enhance security and trust in the Digital Single Market**, permitting the exchange of documents, information, electronic invoices, contents between natural and legal persons in cross-border communication.
Nowadays there are two big delivery services in Europe: PEPPOL system and the Italia PEC – Posta Elettronica Certificata (registered email) that, with more than 10 million of active accounts, is probably the largest e-delivery service with legal value in the world. Considering that **the PEC system is now evolving toward a full compliance with the QERDS requirements** and the REM technical standard, there are all the preconditions to **extend the reach of such system in other Member States**. eIDAS revision process could help specifying that the requirement of identification of sender and receiver stated in article 44 can be practically met with the identification at the creation of the delivery account and the authentication each time a message is sent and read. The actual formulation stress just the "identification", and seems depicting a situation where each time a message is sent or received there is an identification process in compliance with article 24, requirement that would inevitably create an uncoherent process, with a poor user experience mining its wide adoption.

2 THE EUROPEAN DIGITAL CHAMPION OF TRUST

2.1 INFOCERT SPA

InfoCert is the largest QTSP in Europe active in more than twenty countries. We enable companies to digitalize their business processes leveraging on our compliance expertise and our portfolio of trust-based solutions like eId, eDelivery, eSignature, eSeal and the award-winning TOP (Trusted Onboarding Platform) solution to assists companies to digitally onboard their clients.
InfoCert manages millions of legally binding transactions per day across a variety of industries and business processes. We are trusted by thousands enterprise clients across Europe.
InfoCert holds a significant number of patents in the "digital trust" space while the ISO 9001, 27001 and 20000 certifications testify our commitment to the highest level of quality in the provision of our services and in the management of IT security.
InfoCert is a Qualified Trust Service Provider fully compliant with the requirements of the eIDAS Regulation and ETSI-EN-319-401 standards and an accredited provider of the digital identity for Italian citizens.
In Europe, InfoCert holds a 51% stake in Camerfirma, a leading certification authority in Spain, and 50% in LuxTrust, the leading company in Digital Trust in Luxembourg. In Italy, InfoCert owns 80% of Sixtema a provider of technological solutions and consulting services for SMEs and trade associations.

2.2 AC CAMERFIRMA

Camerfirma, incorporated in 2000 by the Chamber of Commerce of Spain, is an eIDAS qualified Certification Authority, with the participation of 72 Spanish Chambers of Commerce. Camerfirma's mission is to offer its customers the possibility of using digital certification as a working instrument for the interaction with other companies and public administration bodies.

2.3 LUXTRUST S.A.

Founded in 2005, LuxTrust is a Qualified Trust Service Provider and Certification Authority. LuxTrust issues and manages electronic identities, provides services such as strong authentication, qualified electronic signatures, seals and timestamping solutions. The company is compliant with latest European regulations and certified for the highest standards: eIDAS, PSD2, EBA/RTS, ETSI and listed as Qualified Trust Service Provider under the supervision of ILNAS.