European
Signature Dialog

Feedback on the eIDAS inception impact assessment

ESD's response to the EU Commission

We, the undersigned organizations, represent the leading European trust service providers: European Signature Dialog enables secure digital interactions all across Europe - between public entities, businesses and individuals. We all experience every day the crucial challenge of trustworthiness, security and cross-border interoperability of digital services and hence acceptance by business and consumers alike. The large number of active users shows that we are constantly getting closer to achieving our goal of helping Europe into the new digital age.

A view at the current crises around the COVID-19 outbreak proofs that digital technologies like e-Trust infrastructures are essential to keep businesses operative and to mitigate the far-reaching negative effects on the wider economy. It is therefore crucial that certain articles of the eIDAS regulation will be strengthened and further specified with appropriate transitional arrangements and sufficient transition time for existing certificates and systems on the market. The members of ESD explicitly welcome this process and will participate with market insights and industry know-how.

In this respect ESD wants to contribute and support the European Commission in the goal to establish trust in electronic transactions in the internal market, secure interoperability and also cybersecurity and thus enhance transparency and consumer protection.

Accordingly, with reference to the three "policy options" set out in the EU Commission's inception impact assessment, ESD members strongly encourage to further specify the regulation through **THREE CRITICAL IMPROVEMENT PROGRAMS**:

1. **<u>OPERATIVE PROGRAM</u>: Increase safety, efficiency and trustworthiness of cross-border interactions**

   This entails the following measures:

- Standardize the certification process and requirements for QSCD / HSM through an implementing decision referring to the newer ETSI standards
- Publish baselines rules for the assessment of trustworthy systems and the reliability of processes supporting them
- Extend EU Trusted List with new qualified service type (“pure player” signature service)
- Harmonize evaluation of alternative methods and certification processes, especially for innovation such as remote face to face and new authentication solutions

2. **<u>HARMONISATION PROGRAM</u>: Enforce harmonisation and standardisation across member states**

   This entails the following measures:

- Add references to implementing acts to specific articles of the eIDAS regulation in the areas of trustworthiness of systems and products, functionality and security of qualified signature services, equality of national qualification procedures and requirements as well as interoperability and cross-border deployment of trust services
- Standardize security requirements for remote qualified signature process and officially reference existing CEN and ETSI standards
- Standardize accreditation process for Conformity assessment Bodies (CAB), using, for instance, ETSI EN 319 403 standards
- Create a set of baselines of auditing rules and a baselines audit plan for each trust service

3. **<u>SUPPORT PROGRAM</u>: Establish an advisory/administrative body to support the industry by implementing eIDAS**

   This entails the following measures:

- Produce and publish implementing acts to create real interoperability with appropriate transitional arrangements and sufficient transition time for existing certificates and systems on the market
- Create a way to simply validate every qualified trust service according the eIDAS regulations without relying on private software. Furthermore, strengthening Europe's digital sovereignty by requiring the availability of eIDAS trust services in standard software products. This should be promoted through reference implementations and open source software.
- An institution should be created in which supervisory bodies can coordinate their activities in order to ensure a common interpretation of the eIDAS regulation in all member states and thus promote the increased use of eIDAS services.

Implementing these 11 measures into the eIDAS review would lead to the following benefits for the European marketplace:

a) Foundation for a true Digital Single Market

Trust is crucial for building a digital society. With its purpose of building trust in the online environment, eIDAS structures e-trust all around Europe in a homogenous way. E-transactions build the foundation for the Digital Single Market in Europe. A powerful eIDAS consequently is the crucial foundation for digitalisation.

b) Highest level of security and transparency for companies and people

Sharpening the regulation will enhance security standards and ensure legal certainty. It will strengthen trustworthiness in electronic commerce. As a result, Europe’s digitalization will experience a strong boost.

c) Fair level playing field for market participants

A strong eIDAS will achieve real harmonisation and homogenisation of the European Digital Single Market and thus enable fair competition amongst member states. Providing the basis for functional competition is crucial to be able to hold a strong position compared to the US-American and Asian market and keeping the lead of careful handling of trust in an online environment.

As the CEOs of the leading trust service providers we share the ambition of strengthening trust and security in Europe. Beside these strategic recommendations ESD has identified **detailed "action recommendations"** for strengthening the eIDAS regulation, which we attach to this paper. The following pages will provide inputs in terms of practical amendments that could help **to foster the spread of cross-border trusted transactions, enhance trust in the online environment and strengthen the European Digital Single Market.**

We are happy to **share market insights and recommendations any time**, to support Europe on a way forward to a strong Digital Single Market.

Signed by:

Michael Butz
Chairman ESD
CEO A-Trust, Austria
CEO FLZ, Liechtenstein

Mikko Pitkänen
CEO Digital and Population
Data Services Agency, Finland

Danilo Cattaneo
CEO Infocert, Italy

Etienne Combet
CEO Sealweb/ ClubPSCo, France

Pascal Rogiest
CEO LuxTrust, Luxembourg

Kim Nguyen
CEO D-Trust, Germany

Hélder Neves
Chairman of Board of Directors
Multicert, Portugal

Gergely Vanczak
CEO Microsec, Hungary

Alfonso Carcasona
CEO Camerfirma, Spain

Adrian Floarea
CEO certSIGN, Romania

European
Signature Dialog

Action Recommendations

based

on the eIDAS conference in Paris at the 18th of October in 2019

organized by

ClubPSCo
Le club des Prestataires de Services de Confiance

Contents

1 SECURITY LEVEL OF CRITICAL ASSETS: TRUSTWORTHY SYSTEMS AND PRODUCTS, QSCD (ART. 24, 20, 30)

1.1 Observation & issues

1.1.1 Use of trustworthy systems and procedures

Article 24 requires qualified trust service providers to "*use trustworthy systems and products*" and "*ensure the technical security and reliability of the processes supported by them*", but these notions are not defined nor detailed in the eIDAS Regulation (for instance, as it is the case for QSCD in an annex to the Regulation). In practice, the Conformity Assessment Bodies (CAB) have to interpret them, and their "mileage may vary" from one to another.

1.1.2 Private key management

Several QTSP issuing qualified certificates allow (usually for *QCP-l* and *QCP-l-qscd* certificates) the signatory to generate, store and use his/her/its private key on premise, with low or no assurance that the signatory actually uses a QSCD or applies any security measures on the protection of his/her/its private key. For instance, the user may contractually agree to use a QSCD and actually use one, but he probably will not (or may not have the necessary expertise to) monitor the qualification status of his device. While QTSP issuing *QCP-*-qscd* certificates have an obligation to *"verify that the device is certified as a QSCD"* (requirement SDP-6.5.1-02 of ETSI EN 319411-2), such verification only applies at certificate's issuance and is usually not monitored by the QTSP when it does not issue or manage the user's cryptographic device.

1.1.3 About the effective assurance security level of QSCD (art. 30)

The Commission implementing decision (EU) 2016/650 of 25 April 2016 has postponed the publication of "*a list of standards for the security assessment of information technology products that apply to the certification of qualified electronic signature creation devices or qualified electronic seal creation devices, where a qualified trust service provider manages the electronic signature creation data or electronic seal creation data on behalf of a signatory or of a creator of a seal", and "the certification of such products shall be based on a process […] pursuant to Article 30(3)(b)*". According to the last published list of alternative processes notified to the Commission in accordance with Article 30.3(b) and 39.2 of the eIDAS Regulation[1], France, Netherlands, Italy, Spain, Austria, Germany and Slovakia have notified the Commission of their alternative security evaluation process for remotely operated QSCD.

This implies that (1) discrepancies may exist between these alternative security evaluation processes, and (2) other countries may continue to use national, specific standards, widening the gap between the different assessments.

[1] https://ec.europa.eu/futurium/en/content/list-alternative-processes-notified-commission-accordance-article-303b-and-392-eidas

Moreover, within the current list of QSCD, one can find 28 devices that are qualified for an unbounded duration, and several devices that are in the list because they were SSCD, a long time ago, and whose security is questionable.

In short, 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 QTSP's to keep unsafe devices in order to maintain the certification status,
- Remote patch management should be taken into account,
- 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.

Some TSPs consider that ENISA should define a unique scheme for security certification of devices, shaped around the already existing and accepted international security schemes as *Common Criteria* EAL4+, while others, on the other hand, consider that CC evaluation is too long and costly for QSCD, and that they should rely on alternate methods.

Finally, in any case, the evaluation status of a QSCD is important data that is needed when one validates a QES: The time of signature must be taken into account for the QES validation because one should be able to determine whether the device was indeed a QSCD at the signature's creation time.

1.2 Action recommendations

⇨ Publish baselines rules for the assessment of trustworthy systems and the reliability of the processes supporting them. These rules should address the following subjects: access rights, traceability, vulnerability management, IT system administration, authentication means, cryptographic modules management.

The incoming cybersecurity regulation may help on this matter.

ClubPSCo has published a series of proposals (guidance documents) several years ago on these topics (art. 19, 24…), which may be found there: https://clubpsco.fr/en/livrables-du-clubpsco/

⇨ Adopt a risk-management approach based on usage. TSP's should have liability insurance.

- ⇨ Harmonize evaluation of alternative methods and certification processes, especially for innovation such as remote face to face and new authentication solutions. At the very least, the perimeter of the CC evaluation of QSCD's should be clarified or harmonized.
- ⇨ Evaluate the opportunity of peer review processes for trust services (as eID existing procedures) for the notification of alternative security certification processes of Member States.
- ⇨ Create a (not too long) time limit for the certification period of a given QSCD
- ⇨ Standardize the certification process and requirements for QSCD / HSM: publish an implementing decision referring to the newer ETSI EN 119 431 standards, so as to harmonize the security assessment of remotely used QSCD.
- ⇨ Create "QSCD / HSM end of life plan" to reduce the workload of TSP, better forecast and reduce continuity risks
- ⇨ Make a difference between a QSCD which is under the physical control of the signatory, and a "remotely used QSCD", which may be shared between distinct users and managed by a third-party.
- ⇨ Implement a trusted list for QSCD's and enforce a regulatory assessment of QSCD's.

2 FUNCTIONAL AND SECURITY RECOMMENDATIONS AND ASSESSMENT OF QUALIFIED SIGNATURE SERVICES (ART 19, 24, 29)

2.1 Observation & issues

In the items (51) and (52) of its recitals, the eIDAS Regulation mentions that "*It should be possible for the signatory to entrust qualified electronic signature creation devices to the care of a third party, **provided that appropriate mechanisms and procedures are implemented to ensure that the signatory has sole control over the use of his electronic signature creation data, and the qualified electronic signature requirements are met by the use of the device.***" Accordingly, "*remote electronic signature service providers should apply specific management and administrative security procedures and use trustworthy systems and products, including secure electronic communication channels, in order to **guarantee that the electronic signature creation environment is reliable** and is used under the sole control of the signatory*".

This is actually the only place where the terms "*remote electronic signature service providers"* (RSSP) and "*remote electronic signature creation device*" (RSCD) are quoted in the eIDAS Regulation. The recitals immediately add that "*where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust service providers set out in this Regulation should apply.*", which was transposed in the Annex II of the regulation: *"Generating or managing electronic signature creation data on behalf of the signatory may only be done by a qualified trust service provider".* Hence, the eIDAS Regulation considers that there is no distinction to be made between a (qualified?) RSCD and a QSCD, or between a qualified RSSP and a QTSP, and does not address the conditions, conformity assessment and supervision procedures required for the initiation and continued provision of such a service. More generally, the eIDAS Regulation did not consider the signer's protection and only focused on the protection of the person/entity relying on the electronic signature.

Conversely, there is a strong business incentive for the implementation of a remote signature service, qualified or not, because such a service relieves the signatory from the technical and procedural burden of managing his/her (Q)SCD, and simplifies the management of the (Q)SCD's life-cycle by the TSP (less handling, shipping, tracking, activation process, renewal, etc.). Moreover, the legal context (for instance, the Directive 2014/55/EU on electronic invoicing in public procurement) also contributes to the development of third-party hosted *QCP-l* and *QCP-l-qscd* certificates. We may also note that, for certificates issued to a legal person, "the signatory" and its "sole control" can usually be interpreted in a much broader or fuzzier sense than for a physical person.

For the same reasons (ease of deployment and usage), on-the-fly certificate issuance on remotely hosted signature creation devices within a signature transaction ("cloud signature service") becomes increasingly common for physical persons in B2C (online banking, insurance, etc.).

For a "signature service provider", there is only one way to provide legal evidence of the trustworthiness of its service: become a QTSP, though it is not necessarily the TSP's original business and may actually create more confusion for the users (for instance, a TSP that has been qualified for a service different from signature and seal may not necessarily possess all the capabilities required to properly manage certificate keys).

This situation creates some legal uncertainty because of the lack of requirements on the signature process and the security of the signature services[2]. Because there is no established standard or baseline for the assessment of the "reliability" of *"the electronic signature creation environment"* or what could be the *"appropriate mechanisms and* [specific management and administrative security] *procedures"*, there is no way for customers and signature recipients to be confident that "all qualified signatures are created equal" between the Member States.

Note that we need to regulate on how the signature service is *operated*, but not on *how to create* a QES; a clear example of some unnecessary implementation detail is the provision of mandatory detailed instructions on how the document to be signed should be displayed before the signature. Another reason for not regulating about the creation process is that legal requirements could vary between seals and signatures, for instance, and that we would unnecessarily complexify the implementation of software solutions. We must remain technologically neutral and take care to not hinder innovation. There is a legal risk if a QES is breached, even once, in court. But if we raise the stakes too high, QES will become too costly or too cumbersome to be used and there will be no market for QES.

2.2 Action recommendations

- ⇨ Standardize the security requirements for remote qualified signature process Officially reference existing CEN and ETSI standards: three technical specifications for cloud-based digital signatures supporting mobile devices: *ETSI TS 119 431-1*, *ETSI TS 119 431-2* and *ETSI TS 119 432*. This new set of standards complements the CEN publications *EN 419241-1:2018 (general requirements for trustworthy systems supporting server signing)* and *EN 419241-2:2019 (protection profile for a qualified electronic signature creation device (QSCD) for server signing)*, which provide the essential core of secure signing in the cloud.
- ⇨ Conformity assessment could be conducted based on *ETSI EN 119 431-1*, which defines the policy and security requirements for TSP service components operating a signature creation device (including a QSCD) on the behalf of a remote signer, and *ETSI EN 119 431-2*, which specifies policy and security requirements for TSP service components creating AdES[3] digital

[2] Note that eIDAS recitals specifically excludes signature applications from the scope of certification standards.

[3] Advanced Electronic Signature, in the technical (ETSI) sense; not to be confused with the notion of "advanced electronic signature" in article 26 of the eIDAS Regulation.

signatures relying either on remote server signing or on a signature creation device in the user's environment.

- ⇨ Extend the EU Trusted List with a new qualified service type (“pure player” signature service).
- ⇨ Extend the EU Trusted List with a new qualified service type (signature service) limited to “remote signature services” (or “QSCD operator”); that is, create a new QTSP type for QTSP who manage the signatory's private key on his/her/its behalf, ensuring that providers of remote signature services are properly supervised by their national supervisory body.

  Alternatively, we should at least restrict the capability to manage private keys exclusively to QTSP’s that have been qualified for Qualified Electronic Signature, Qualified Seals or Qualified Website Authentication Certificates.
- ⇨ In any case, QTSP certificate policies should clearly mention whether the QTSP or a third party manages the signatory's private key or not; no CP should support both modes (distinct OID’s should be used for user-managed keys and cases where private keys are managed by a third-party (the QTSP itself or another entity, like a cloud-based key hosting service)).

See also next point

3 EQUALITY OF NATIONAL QUALIFICATION PROCEDURES AND REQUIREMENTS (ART. 19.1, 20.4, 24.2)

3.1 Observation & issues

According to the eIDAS recitals, "*All Member States should follow common essential supervision requirements to ensure a comparable security level of qualified trust services. To ease the consistent application of those requirements across the Union, Member States should adopt comparable procedures and should exchange information on their supervision activities and best practices in the field.*"

About half of the Member States (15 out of 28) seem to have implemented a national law or a procedure for the qualification of TSP's. This represents about 70% of the active QTSP (October 2019) in Europe. But further examination reveals that among them, less than the half actually reference specific standards (such as ETSI EN 319401 for the coverage of article 24.2) for the conformity assessment by a CAB; other countries also introduce specific technical requirements for TSP's, restricting the interpretation of eIDAS articles.

For the remaining half of Member States that have no defined law or qualification procedure, nothing can be said of: the criteria applied to a TSP; how, on which perimeter and by what kind of entity is the conformity assessment realized; the existence (or inexistence) of a reviewal process by the national supervisory body, nor its content or duration…

At the CAB's level, there are no common auditing rules and processes for the different trust services. In particular, the lack of common sampling rules on registration authorities may create severe discrepancies in the assessment of certification authorities, depending on the size of their customers' base. Thus, in order to create a level playing field for all European QTSP's and to ensure the high quality and trustworthiness of all qualified trust services, the regulation should harmonize rules for the conformity assessment of qualified trust service providers.

On the other hand, if costs become too high because harmonization aims at the highest level, there won't be any market use. For instance, in some countries, QTSP's are actually audited twice: once by the CAB that – with different approaches throughout Europe – performs deep audits on implemented services and processes, and then by the Supervisory Body that, not always fully trusting the CAB report, re-executes the same audits and analysis. 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.

Among the Member States, according to the *list of conformity assessment bodies accredited against the requirements of the eIDAS Regulation*, there are currently 30 accredited CAB's; few Member States

have published their accreditation scheme, and the situation is even less clear where there are QTSP without any (publicly) accredited CAB.

At the European level, notification of security breaches having "*a significant impact on the trust service provided or on the personal data maintained therein*" (art. 19.2) is a requirement that seems to be overlooked by TSP's, qualified and unqualified alike: according to the last annual ENISA reports[4], there would be less than 20 such incidents per year, for more than 200 TSP's in the EU, which seems a rather low figure. In 2019, approximately three quarters of the reported incidents had an impact on qualified services: unsurprisingly, QTSP are more likely to report security breaches than unqualified ones.

3.2 Action recommendations

- ⇨ Standardize the accreditation process for CAB's (using, for instance, ETSI EN 319 403 standards)
- ⇨ All actors have to be liable; in particular, CABs have to be liable for their assessments.
- ⇨ Create a set of baselines of auditing rules / baselines audit plan for each trust service (these baselines rules should complement the "trustworthy systems" baselines rules proposed in 0).
- ⇨ Supervisory bodies should publish guidelines on the kind of "incident" that should be reported, recommended classification methods, etc..., so as to harmonize, at least at the national level, the reporting of security incidents. Clarify which changes have to be reported, and which ones *do not* have to be reported.
- ⇨ Supervisory bodies should randomly audit a sample of the national TSP's on the effectiveness of their notification process of security breaches, focusing on TSP's who have *not* declared any incident during the previous years.

  Conversely, some kind of reward program for security notifications could be designed. Nowadays, the TSPs do not know what is the added value of the reporting.
- ⇨ Create a legal (whistleblowing) obligation for CABs and internal auditors to report security breaches, incidents or conformity violations to the Supervisory body.
- ⇨ The GDPR has created legal obligations for services providers *offering services in Europe* (not only those *localized* in Europe); eIDAS should have the same approach. The CAB forum must not be forgotten in this regard: we should oblige web browsers companies that make business in Europe to accept the eIDAS compliant QWAC's in the same way TL certificates are accepted in the Adobe Reader.

[4] https://www.enisa.europa.eu/publications/trust-services-security-incidents-2018

4 INTEROPERABILITY AND CROSS BORDER DEPLOYMENT OF TRUST SERVICES (ART. 28, 32, 34, 38, 40, 42, 44)

4.1 Observation

4.1.1 Qualified signatures and seals

Cross-border interoperability and recognition of qualified certificates is a precondition for cross-border recognition of qualified electronic signatures. Nowadays, assessing the legal level of an electronic signature or seal (is it qualified or not?) or its validity can be technically and functionally arduous, especially when the TSP's related to it (that is, the certification and timestamping authorities which have issued the certificates, revocation status information and timestamps that appear in the electronic signature/seal) are no longer active. For PAdES (signatures embedded in PDFdocuments), Adobe's Acrobat Reader is a "de facto" standard, but its validation algorithm is not tailored to the validation of eIDAS signatures/seals and is subject to unpredictable changes. For other signature formats, there is no well-established software.

Although one may expect, in the future, public validation services for QES, we are not safe from discrepancies between these would-be public services. For instance, allowed cryptographic algorithms (for QES) are not the same in all countries; some countries require a qualified timestamp for a QES, some do not. Thus, one would get different validation results depending on the service used for QES validation, which is legally absurd. Once a signature has been validated (by some public/national service), it must be accepted by all EU member states; this should be legally enforced. Another reason why QES validation should be a public service is that there is no business model for signature validation.

An issue with eIDAS is that supervisory bodies do not have the legal enforcing authority in their own country (contrary to the RGPD case, for instance).

On the other hand, remember that eIDAS is technologically neutral. A public, single QES validation service may have difficulties in supporting new, innovative signature solutions (that is, ones that do not use the CAdES/XAdES/PAdES formats). Such a service must also not impede new solutions. Finally, we must not forget that a centralized validation service would have a privileged access to a huge amount of signature metadata, which would be a severe issue, and could create a single point of failure.

Moreover, the legal timeframe far exceeds the technical duration of certificates and trust services, which renders the publicly available tools impracticable in legal procedures. For instance, most software tools only address the question whether a given certificate is currently valid, whereas in a legal procedure, the question is rather "Was that certificate valid at some point in the past?". The "History" section of the Trusted List and the fact that QTSP's are required to implement a termination plan are a first step towards an effective solution, but definitely not the last one.

4.1.2 On identification methods for qualified certificates

Article 24 (Requirements for qualified trust service providers), first paragraph, item (d), allows QTSP's to verify the identity of *"the natural or legal person to whom the qualified certificate is issued […] by using other identification methods recognized at national level which provide equivalent assurance in terms of reliability to physical presence. The equivalent assurance shall be confirmed by a conformity assessment body."* This allows different identity verification methods to be used in different member states depending on national legislation, which damages competition and results in an unfair market for certificate issuance, and also results in unequal levels of assurance in qualified certificates.

There are currently 204 QTSP for ESig or ESeal, some of which use various "identification methods" with variable "equivalent assurance" to physical presence. For instance, the following excerpts come from certificate policies of actual QTSP:

- one may "*ensure the physical presence of the subscriber at the moment of the registration, unless there is already a trust relation previously based on that physical presence of the subscriber*"
- The "face-to-face" can be based on "*registered mail with hand delivery; the titleholder's identity being verified at the delivery (a photocopy of a legally accepted identity document is returned to the CA)*"
- "[The registration authority] *can establish the natural person identity* […] *by using a specialized mobile or other application and after an automated identification of the natural person or by [an] employee.*"

While the eIDAS regulation creates an obligation for Member States to indiscriminately recognize qualified certificates and signatures, the public may benefit from a clearer view of the conditions under which a qualified certificate has been issued.

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*. Indeed, QTSP's 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.

4.1.3 Cross-border e-delivery

While the eIDAS recitals recognize that "*It is essential to provide for a legal framework to facilitate cross-border recognition between existing national legal systems related to electronic registered delivery services*", the two following statements from its article 44 are particularly subject to incompatible interpretations by each Member State: "*Qualified electronic registered delivery services shall […] ensure with a high level of confidence the identification of the sender [and] ensure the identification of the*

addressee". Whereas these requirements induce a natural relationship between electronic identification services and registered delivery ones, that relationship is left unspecified in the Regulation.

Does a "high level of confidence" correspond to a "high level of assurance of the electronic identification means" used by the sender? Conversely, is there a minimal level assurance for the "identification of the addressee"? Each of the Member States that have qualified electronic registered delivery services have, explicitly or implicitly, already answered these questions, but not necessarily the same way. And because a QERD's policy defines requirements on both the sender and addressee's identification, incompatible requirements between policies (possibly because of some national interpretation of article 44) imply the impossibility for two QERD's to collaborate.

Moreover, some supervisory bodies have issued rules conflicting with the postal (paper) rules on registered mail; this not only confuses the public on the functioning of that new trust service but also lay ground for future legal debates. For instance, postal rules commonly allow for the sender and the addressee to delegate the sending and receiving of a delivery to a third-party; secure delegation mechanisms are indeed a complex issue, which is frequently not addressed in qualified electronic registered delivery policies, and sometimes, simply forbidden.

4.2 Action recommendations

- ⇨ Create a way to simply validate an electronic signature without relying on private software
- ⇨ Each supervisory body should be in charge of the archival and post-mortem availability of QTSP's revocation lists (or revocation status information)[5]
- ⇨ CAB (or supervisory body) should publish under which item of article 24, alinea 1 (a, b, c or d) "*the identity (and, if applicable, any specific attributes) of the natural or legal person to whom the qualified certificate is issued*" was verified. Such information could be included in the TL or the CP (using a specific OID).
- ⇨ Recommend (or enforce) participation to ETSI plug tests, achieve results of the other workshop panels to reach legal interoperability.
- ⇨ Publish implementing acts to, at least, relate the requirements of article 44, alinea 1, items (b) and (c), to the three assurance level of the electronic identification means defined in article 8 of the eIDAS Regulation.
- ⇨ 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.

[5] Note that certificate suspension complicates the matter, because one has to keep track of the certificate's revocation status over time rather than once for all (inducing a increase of storage needs).

5 GLOSSARY

AdES	Advanced Electronic Signature (in a technical sense; never in the sense of article 26 of eIDAS)
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
B2B	Business to Business
B2C	Business to Customer
B2G	Business to Government
CAB	Conformity Assessment Body
CAdES	CMS Advanced Electronic Signature
CP	Certification policy
eIDAS	Electronic identification and trust services
ETSI	European Telecommunications Standards Institute
GDPR	General Data Protection Regulation ("RGPD" in French)
HSM	Hardware Security Module
MS	Member State
OTP	One Time Password
PAdES	PDF Advanced Electronic Signature
QCP-l	ETSI Policy (requirements) for qualified certificates for a legal person
QCP-l-qscd	ETSI Policy (requirements) for qualified certificates for a legal person on a QSCD
QCP-n	ETSI Policy (requirements) for qualified certificates for a natural person
QCP-n-qscd	ETSI Policy (requirements) for qualified certificates for a natural person on a QSCD
QES	Qualified electronic signature (or seal)
QSCD	Qualified Signature Creation Device
RGPD	Règlement Général sur la Protection des Données
RGS	Référentiel Général de Sécurité
SCAL	Sole Control Assurance Level
SCD	Signature Creation Device
SCP	SSASC policy
SSASC	Server Signing Application Service Component
TL	Trusted List
TSP	Trust service provider
XAdES	XML Advanced Electronic Signature