Joint DTCE-ChamberSign Position Statement

on the proposal for a regulation on electronic identification and trust services

COM(2012) 238/2

15 Sept 2012

An association established in 2011, Digital Trust and Compliance Europe (DTCE) brings together businesses and practitioners with an interest in trust and compliance methods and technologies in Europe. Further information on DTCE is available at: http://www.DTCE & ChamberSign.eu/

ChamberSign is the association of Chambers of Commerce and Industry delivering e-Signature related services. Created in 1999, its mission is to foster the development of an interoperable framework for e-Signature and related applications in Europe. More on http://www.chambersign.com/.

Contents

DTCE & CHAMBERSIGN welcome the European Commission's proposal for a regulation on "electronic identification and trust services for electronic transaction in the internal market". This is a significant step forward in providing a harmonised approach to trusted electronic transactions across Europe. However, DTCE & CHAMBERSIGN wish to bring to the attention of the European Parliament and Council the following points.

1 EU Trust Services within a Global Market

EU providers of trust services play a major role in assuring the security of electronic transactions. It leads the world in adoption online services with over 50% of the population with active mobile broadband subscriptions1 and Europe estimated to account for 56% of the e-invoicing market[2]. Assuring trust in electronic transactions forms a major facilitator to the widespread use of online services by giving users greater confidence in their security.

Europe has a track record of being among the earliest adopters of facilitating legislative frameworks for trusted e-commerce. Indeed, one could argue that the 1999 Electronic Signature Directive preceded significant market use of the technical mechanisms and processes regulated therein. Within the EU, a very dynamic digital trust and compliance sector has grown out of the fundamental legal concepts of the 1999 regime. DTCE & CHAMBERSIGN are deeply appreciative of the European Commission's willingness to take concrete action to modernise this legislative framework and to allow Europe's digital trust and security sector to reap the benefits of almost two decades of lessons learned.

If Europe's approach has generally been to balance the prime objectives of, on the one hand, user choice and innovation with, on the other hand, legal certainty, most other countries and regions have clearly chosen one or the other as the basis for their digital trust and compliance legislative frameworks. Electronic commerce or transactions laws in many countries affected by the common law tradition have generally been based on prioritizing freedom of form over the legislative detail required for legal certainty, while in many civil law countries detailed prescription has often prevailed. Trust and compliance sectors have emerged in all these geographies, however DTCE & CHAMBERSIGN believe that the balanced European approach will in the long term be the most effective for the sustainable growth of the information society. As a corollary, Europe's digital trust and compliance sector has an important role to play in the emerging global marketplace for related products and services - and this key role in turn can have a **significant positive effect on Europe's long-term competitiveness in cutting-edge technology markets**.

With appropriate legislative support the EU trust market can be significantly enhanced. Governmental oversight can re-assure users that the services underpinning the security of electronic transactions can be considered trustworthy. Supervisory schemes which ensure that trust services are operated in line with current best practice can minimise the risks to the everyday user who is unaware of the potential risks and available countermeasures. However, if the rules applied inhibit the trust service from operating in a global marketplace and adopting competitive solutions then such government oversight will have a negative impact with users looking elsewhere for the trust services.

European online services do not operate in isolation from the rest of the world. With the World Wide Web users can switch seamlessly between services based in different parts of the world

[1] See: http://mobithinking.com/mobile-marketing-tools/latest-mobile-stats/a#subscribers
[2] See: E-Invoicing 2010 - European Market Guide
http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=406

and in many cases may be unaware that elements of the service may be based in the opposite ends of the world. Providers of trust services cannot limit themselves to providing services in one part of the world and remain competitive. Global initiatives for trust services such as the CAB Forum[3] and identity services such as Kantara[4] provide a framework in which **European trust services can operate globally**.

Importantly, the market for digital trust and compliance services depends to a much larger extent than many other markets on good regulation that allows European trust services to compete effectively in a global market. This means, among other things, that it is critical for market stakeholders and regulators to collaborate closely and continuously to optimize outcomes. **DTCE & CHAMBERSIGN are keen to be part of such an on-going dialogue with relevant public sector stakeholders.**

The following general observations and comments are aimed at ensuring continued competiveness of European trust services in the global market.

[3] https://www.cabforum.org/
[4] http://kantarainitiative.org/

2 General observations on the draft Regulation

2.1 Positive Aspects of the Regulation

As a general remark, the draft Regulation shows a dramatic change in approaching the problems of trust services, a very positive change because

a) the form of legislation establishes a set of common regulatory framework, without the further filters of national implementation. This gives a clear direction for European trust services to follow.
b) by allowing the Commission to reference standards the decision process on detailed technical aspects can be faster and more open, making for better interoperability. Also, this allows the technical details to adapt to the changing market. It makes the technical approach much more likely to be applicable to business and daily life.
This draft regulation deals primarily with electronic identification, electronic signature, but it also introduces other new and interesting concepts such as stamp server, timestamp, electronic delivery of services, signature validation services, electronic storage and website authentication
c) Trust services are placed under harmonisation, that is to say a unified regulation that applies to all. For all these services, the "qualified" level is systematically defined. This is the level which gives the presumption of reliability and mutual recognition between Member States.
d) Its objectives are to accelerate the transition to digital by fighting against the obstacles to mutual acceptance and increasing legal certainty by providing clear and simple rules of recognition. This text will give a great impetus to the European market for the security of digital exchanges if it comes into force, focusing on pragmatic and cheaper solutions.
e) The legislation has been updated before getting obsolete with a view to leverage harmonisation and interoperability in EU trust services, setting the foundation stone of a truly common and wide adopted trust system

2.2 Scope: issues that could have been regulated but are not

2.2.1 Common Framework for European eIdentity validation

The responsibility for the provision of the means to identify individuals and the provision of a free service to validate such identities is left to each Member States (Article 6.1 (d)). If a national law requires at least one of the systems in the list to access a given online service, then that service must accept all systems of the list. Article 8 of the proposed regulation foresees that Member States shall cooperate to ensure interoperability. This is very challenging for on-line services developers and can be very expensive in terms of integration, even if the access to the means of validation is free.

This does not address another issue of interoperability which is how that identity is applied to electronic transactions out of a governmental context. As interoperability outside, as well as inside, the governmental context is a major concern of most users we see a risk that developers of online services move away from notified systems and rather chose identification systems which have not been notified which is the opposite of what is intended.

Recommendation

In order to mitigate this risk, DTCE & CHAMBERSIGN propose that the Commission, with the appropriate European institutions, work on the development of a common framework for authentication of identities associated with electronic transaction which supports interoperability for both governmental and non-governmental use. This framework should include best practices for trusted identity providers and a common means of asserting the authenticity of an identity associated with a particular transaction.

2.2.2 Trust services for eIdentities

The Regulation places a clear division between services which are provided by notified national eID schemes (article 5 to 8) and other services which are supported by supervised trust service providers (article 9 onwards) which primarily involve electronic signature related technologies. The eID services has no provisions for assuring trust whilst trust is the main issue address by the trust services for electronic signatures in the latter part of the regulation. Whilst different technologies may be more appropriate to the two aspects, there is still the need to have assurance that the providers of identity services are trustworthy and to ensure that they apply good security practices which are independently audited. In particular, trust service providers which provide identity assertions (such as adopted by the EU Stork Project) can have a significant role to play in identification authentication internationally.

Recommendation

DTCE & CHAMBERSIGN suggest that many of the principles for the supervision of trust services defined in section 2 of the draft regulation apply also to trust service providers supporting identity authentication (e.g. identity providers issuing assertions based on SAML standard).

2.2.3 European trust services supervision framework

The proposal set the base for a common supervision framework but fails to ensure a genuine European supervision scheme which may be adopted by nations which do not have the resources to operate their own scheme and may be used by trust services which wish to offer on a pan-European service. Furthermore, a common supervision framework would make a significant contribution to interoperability and a common level of trust.

Recommendation

Member states should keep the possibility to establish their own supervisory body but a European supervisory body[5] should be set up for substituting the supervision obligation of Member States that do not want to establish one. The supervision scheme should be set up with the objectives of transparency, efficiency, accessibility and flexibility. The supervision should be based on a common standard that would allow mutual recognition.

2.2.4 European eSignature validation tool

While article 25 and 26 set the framework for the development of qualified validation services for qualified electronic signatures, the proposal does not foresee the establishment of a European eSignature validation tool at the pan-European level. The European Commission proposal promotes quality validation and some Trust Service Providers (TSP) will develop a

[5] There is no need to create a new European body for implementing the European supervision. The European Commission could operate the supervision as it does in some matters such as competition and state aids. ENISA could also operate such supervision.

number of high added value services around that framework (integration of automatic validation in various processes, long term archive of validation results, etc.). It opens new niche markets for TSPs, a number of professionals have huge responsibilities as regard the authentication/non repudiation of signed document (notaries, physicians, eProcurement…). But there is no business model for services to citizens, SMEs or small public administrations that rarely face eSignature and will need validation services a few times a year.

Recommendation

To overcome the anticipated market failure, DTCE & CHAMBERSIGN support the promotion or development, by the European Institutions of a European common validation tool for QeS, with on-going support. Such a tool could be based on the work of projects such as SPOCS and PEPPOL as long as it is available for SMEs and citizens in a universal context[6]. The European validation tool should offer a basic service such as the download of a signed document or a certificate and the provision of a yes/no answer. This is the best way to foster cross border eSignature recognition in the short and medium term. Services such as the automated integration of a validation service in processes, the archiving of validation reports and other more sophisticated validation services should be left to private operators.

2.2.5 Remote signing/outsourcing of signing

The outsourcing of keys or user credentials to a third party is a very common practice for many different types of (e-)business applications, however under current rules in EU Member States users often view such outsourcing as a risk where the rules are unclear or non-existent, or as overly burdensome where the rules do not adequately differentiate between varying uses of certificates and keys. See also comment 2.3.3 below.

Recommendation

DTCE & CHAMBERSIGN recommend that the Regulation be more explicit about the ability for users to remotely (including through mobile devices) use keys and certificates for various types of electronic identification, seals and signatures.

2.3 Scope: issues that are regulated but should be improved

2.3.1 Alignment with Global Market

Greater emphasis should be put on ensuring that the requirements of the Regulation and standards adopted by the Commission are aligned with globally accepted practices.

Recommendation

DTCE & CHAMBERSIGN recommend that when establishing reference numbers of standards relating this regulation (e.g. 19(5), 20(7), 21(5), 22(2), 25(3) etc) that the Commission demonstrate alignment with current best practice adopted by the market and where there is divergence give clear reasons for so doing.

[6] The interest for such a service has already been understood by Spain that developed VALIDe, a validation platform for eIdentities and eSignatures, https://valide.redsara.es/valide/?lang=en.

2.3.2 Greater Adoption by Major Players in eTransaction Market

The Commission needs to encourage greater involvement of major players in the Global eTransactions market in the application of the regulation, particularly in the recognition of qualified trust service providers and the use of Trust Lists. As yet none of the major market players such as Adobe, Microsoft and Google have integrated the use of trust lists in their own trust management schemes[7].

Recommendation

The European institutions should encourage the relevant EU bodies (expert groups and European standards organisations) to establish a consensus on the integration of EU trust lists with other vendor specific and standardised trust management schemes.

2.3.3 Recognition of Alternative "Qualified" technologies

The emphasis of the current regulation is still very much centred on PKI technologies with end user certificates issued by trust service providers used with private signing keys held in secure user owned devices. There is little provision for the potential recognition of alternative technologies (e.g. signing using shared "cloud" based service, use of mobile devices) being recognised as having legal equivalence to handwritten signatures.

Recommendation

DTCE & CHAMBERSIGN propose the inclusion of an article to allow the Commission through delegated acts to recognise alternative qualified trust services or devices for securing transactions, for cloud based services and for use with mobile devices, through reference to standards, and where appropriate give them equivalent legal effect to qualified electronic signatures. Also, the Commission should encourage standards for new technologies which are being widely adopted in the market, in particular for mobile devices and cloud services.

2.3.4 Issuance of qualified certificates

There is confusion whether there is a requirement for a face to face identity check for the issuance of a qualified certificate or if the indirect means providing equivalent security is acceptable. DTCE & CHAMBERSIGN fear a multi-speed Europe, with countries imposing face to face and others accepting more flexible systems, enabling a faster development of the digital economy.

Recommendation

A common set of practices for registration of identities needs to be established through the identification of agreed standards (see TS101 456). DTCE & CHAMBERSIGN recommend the integration with national eIdentity schemes.

2.3.5 Advanced eSignatures

The legal effects of electronic signatures are identical to those of the Directive, with a clearer assertion of de facto mutual acceptance between Member States for the qualified signature. Article 20 foresees the concept of security assurance level below qualified electronic signature and the principle of de facto mutual acceptance which also applies to those levels.

[7] On May 2012, DTCE together with a large number of end user associations and public administrations addressed a letter to ADOBE to flag the problem and ask for urgent measures to solve the issue. No solution has been offered yet.

Recommendation

The commission states that it reserves the right, by implementing acts to specify these levels thereafter. DTCE & CHAMBERSIGN recommend the development of such a framework for advanced signature interoperable levels in Europe.

2.3.6 Electronic signatures versus electronic seals; remote application

DTCE & CHAMBERSIGN welcome the proposed clear differentiation between electronic signatures and electronic seals, but sees a need for further determination around the use of the different signatures and seals and requirements related to legal consent. An example would be a natural person using its electronic signature for mere integrity and authenticity purposes with no intention to legally consent to the contents of the data, or a legal person applying its electronic seal in order to enter into a contract, supporting its mandate by combining the seal with a role assertion in a federation. The Regulation must explicitly remove any technical or other detailed rules or supervisory authority guidelines in Member States that have been introduced toward assurance of legal signing and that have created unnecessary complexities for the remote application of electronic seals or signatures used merely for technical assurance. Such rules include artificial constructs for what-you-see-is-what-you-sign assurance and the enforcement of time-windows for natural person key holders to re-enter PIN codes as a condition for acceptable outsourcing of private keys. Many of these rules lead to near-prohibitive and pointless procedures that undermine the security of modern data centers.

Recommendation

Ensure that the Regulation explicitly removes and prohibits requirements aimed for "legal" signing to be applied to use of electronic seals or electronic signatures for which the aim is only to ensure the integrity and authenticity of the data.

3 Article-by-article commentary

3.1 Whereas

Whereas 24

Left aside that everyone shall comply with the Data Protection obligations proportionally to her own activity, there are many cases where a trust service provider is not a controller of personal data; for example, a provider offering long-term preservation services can be a Processor of data for which someone else is Controller.

> ***Recommendation – amend article as follow***
>
> "A trust service provider ~~is a controller~~, *if acting as a controller* of personal data, ~~and therefore~~ has to comply with the obligations set out in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. In particular the collection of data should be minimised as much as possible taking into account the purpose of the service provided."

Whereas 25

> ***Recommendation – amend article as follow***
>
> Supervisory bodies, *when applicable*, should cooperate and exchange information with data protection authorities to ensure proper implementation of data protection legislation by service providers. The exchange of information should in particular cover security incidents and personal data breaches.

Whereas 33

DTCE & CHAMBERSIGN recommend making the data related to qualified trust service provider (QTSP) openly accessible. This will ensure the general availability of the data for the validation of qualified services.

> ***Recommendation – amend article as follow***
>
> To ensure sustainability and durability of qualified trust services and to boost users' confidence in the continuity of qualified trust services, supervisory bodies should ensure that the data of qualified trust service providers are preserved and kept accessible *openly* for an appropriate period of time even if a qualified trust service provider ceases to exist.

Whereas 37 and 38

Whereas 37 and 38 seem wrong and the same applies to the corresponding article 17. Indeed, it seems that a QTSP can start its service without being in any trusted list. How could a relying party validate a transaction involving such QTSP? Also the wording is not clear, since a QTSP notifies and is not subject to a notification.

See recommendation against article 17.

Whereas 51

Whilst the explanatory memorandum mentions the need to "engage discussions with third countries in view of achieving eIAS interoperability at global level", the regulation itself does little to encourage such discussion to encourage global interoperability, particularly at the detailed technical level.

Recommendation – amend article as follow

In order to ensure uniform conditions for the implementation of this Regulation, implementing powers should be conferred on the Commission, in particular for specifying reference numbers of standards which use would give a presumption of compliance with certain requirements laid down in this Regulation or defined in delegated acts. *The standards shall be aligned with current global standards or best practice specifications.* Those powers should be exercised in accordance with Regulation (EU) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers.

3.2 Articles

Article 3(11), 3(24), 3(30)

Recommendation – amend article as follow

(11) 'qualified certificate for electronic signature' means an ~~attestation~~ *certificate* which is used to support electronic signatures, is issued by a qualified trust service provider and meet the requirements laid down in Annex I;

(24) 'qualified certificate for electronic seal' means an ~~attestation~~ *certificate* which is used to support an electronic seal, is issued by a qualified trust service provider and meet the requirements laid down in Annex III;

(30) 'qualified certificate for website authentication' means an ~~attestation~~ *certificate* which makes it possible to authenticate a website and links the website to the person to whom the certificate is issued, which is issued by a qualified trust service provider and meets the requirements laid down in Annex IV;

Article 3(31)

The use of the term "validation data" covers the basic keys to verify the cryptographic protection, but "validation" is used to the whole process of checking the signature which also include checks on the validity of the certificates and on the compliance of the signature with policies (e.g. algorithm used is strong enough for the age of the signature). In line with standards for electronic signatures it is suggested that the term "verification" is used for the basic cryptographic checks and validation is used for the full checks on signature validity.

Recommendation – amend article as follow

The regulation should use the earlier definition in Directive 1999/93 of signature verification data:

'verification-data' means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature or an electronic seal;

Also, articles 3(10), 25.1 (c), 27.1, Annex I (d) (j) , Annex III (d) (j) should be updated to use the term *verification data*.

Article 8(2)

The application of the "peer review" process to notified electronic identification schemes should be clarified. Does this imply that one EU Member Sate will be able to inspect another EU Member Sate identification scheme without any framework? If it is so, this is arguably acceptable even though the alternative (a Member State shall accept a weak identification scheme just because it has been notified by another member state) is not particularly appealing. It is suggested that a more rigorous approach based on independent audit is applied as for trust services.

Article 13.3 b)

Summaries on breach notifications should also be made available to Trust Service Providers to ensure that appropriate countermeasures are applied by other TSPs.

Article 14(3) second paragraph

Recommendation – amend article as follow

3. Where appropriate, supervisory bodies may carry out joint investigations in which staff from other Member States' supervisory bodies is involved.
The supervisory body of the Member State where the investigation is to take place, in compliance with its own national law, may devolve investigative tasks to the ~~assisted~~ *assisting* supervisory body's staff. Such powers may be exercised only under the guidance and in the presence of staff from the host supervisory body. The assisted supervisory body's staff shall be subject to the host supervisory body's national law. The host supervisory body shall assume responsibility for the assisted supervisory body staff's actions.

Article 15(1) second paragraph

The article introduces the concept of "recognised independent body" but it is not clear who should recognise it. It is recommended that this is based upon the framework for accreditation of audit bodies established by the European co-operation for accreditation.

Article 16.1

This needs to be more precise about how the auditors are to be recognized. The auditor's must have demonstrated competence to carry out the audit.

Recommendation – amend article as follow

It is recommended that this article is amended as follows:
Qualified trust service providers shall be audited by *an independent body whose competence to carry out the audit has been demonstrated* ~~a recognised independent body~~once a year to confirm that they and the qualified trust services provided by them fulfil the requirements set out in this Regulation, and shall submit the resulting security audit report to the supervisory body.

Also, it is recommended to add to article 16.6 "audit criteria and guidance"

Article 17(1)

Article 17(1) states that, after the notification, the QTSP can start to provide its services, in line with the old Directive, where no pre-emptive authorization was required. But it is at odds with the idea of the Trusted List as the only way a relying party can check the status of a QTSP.

Recommendation

Add requirement that the trusted list includes the QTSP but with indication that awaiting confirmation of conformity by the supervisory body.

Article 17(3)

Time periods should be expressed as a precise multiple of the basic time unit (i.e. the second, as per the International System of Units). A month can mean 28, 29, 30, 31 days. It is safer to specify the period in days.

Article 18(1)

It may be that a member state may wish to save on the costs of the resources needed to carry

out this function by delegating this responsibility to another Member State. Similarly, a member state may wish to wish to delegate responsibilities for supervision on a regional basis..

Recommendation – amend article as follow

Each Member State shall establish, maintain and publish trusted lists with information related to the qualified trust service providers for which it is competent together with information related to the qualified trust services provided by them.

Upon mutual agreement, a Member State may delegate its responsibility under this article to another Member State or regional institution.

Article 18(3)

The technical details of this clause are incorrect as certificates, which contain signature verification data, are never used to sign, but for the validation of signature.

Recommendation – amend article as follow

Member States shall notify to the Commission, without undue delay, information on the body responsible for establishing, maintaining and publishing national trusted lists, and details of where such lists are published, the certificate *to be* used to ~~sign~~ *validate the signature* or seal *applied to* the trusted lists and any changes thereto.

Article 19.2.d)

It is not appropriate to protect the whole system against any kind of modification. Changes will need to be made to the system and its data over time.

Recommendation – amend article as follow

(d) use trustworthy systems and products which are protected against *unauthorised* modification and guarantee the technical security and reliability of the process supported by them;

Article 19(3)

The article 19(3) is unclear, implies specific implementation through a database and uses different wording to the related article 19(4). It is suggested that this article is re-worded in terms of the objectives linked to article 19(4). The technical details should be left to reference to standards as in article 19.5.

Recommendation – amend article as follow

Qualified trust service shall update the revocation status information provided to relying parties shall be updated within 10 minutes of the decision that a certificate has been revoked.

Article *19(4bis)*

DTCE & CHAMBERSIGN recommend adding a new provision to article 19 to meet privacy requirements. The wording is taken verbatim from the current Directive.

Recommendation – amend article as follow

19(4bis) certificates are publicly available for retrieval in only those cases for which the certificate-holder's consent has been obtained.

Article 20(4)

It introduces the undefined concept of security assurance levels. Are they the Common Criteria levels? Or are we talking about the EU security classification (restricted, secret and so forth). It is impractical for a system to assess the security assurance and validate "all electronic

signatures".

Recommendation

The concept of security assurance level should be defined or, if the scope is much more limited, the clause should read explicitly that a qualified signature shall be accepted in every process requiring a basic electronic signature.

DTCE & CHAMBERSIGN suggest that the Commission endorses some schemes for cross EU Advanced Signature proposed by representative organizations, provided that those scheme implement sufficiently secure methods for user authentication and digital signature (ETSI TS 102 042 without face to face but with authentication methods issued through a "Know Your Customer" process could for instance be quite relevant). A good example of this approach for payment transactions is the 3D Secure model assessed by Visa & MasterCard. A similar approach could be adopted in the scope of article 20 for Advanced Digital Signature.

Article 21(3)

It's not clear if suspending a certificate (revocation reason "onHold") is still allowed. If yes, the clause should be changed, from "revoked" to "definitively revoked". Moreover, it should make clear that the loss of validity starts from the revocation time (i.e. signatures applied before the revocation time are still valid).

Recommendation – amend article as follow

If a qualified certificate for electronic signature has been *definitively* revoked after initial activation, it shall lose its validity *after the revocation time*, and its status shall not in any circumstances be reverted by renewing its validity.

Article 23(1)

If something "may be certified", no one will certify anything[8]. The certification process is expensive and the savings will be quite large for the TSP that does no go through the process. Moreover, if a company decides to spend a lot of money in a formal certification, for sure it does not need any law allowing it.

A relying party validating a QES needs to know if the issuing signature creation device is trustable, which can be achieved only if this party can trust that an independent evaluation of such device has been done. At the same time, it's quite risky to switch from a highly regulated status, with strong security requirements, to a completely unregulated situation.

Recommendation – amend article as follow

Qualified electronic signature creation devices ~~may be certified~~ *shall be assessed against the requirements listed in the Annex II* by appropriate public or private bodies designated by Member States provided that they have been submitted to a security evaluation process carried out in accordance with one of the standards for the security assessment of information technology products included in a list that shall be established by the Commission by means of implementing acts. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). The Commission shall publish those acts in the *Official Journal of the European Union*.

Article 25.1

The annex IV of Directive 1999/93/E requires a "reasonable certainty" level. The annex II 1.c) of the proposed Regulation requires "reasonable assurance". But this article 25 foresees a "high level of certainty" which is tricky to put in practice.

[8] This assumption is largely documented by Akerloff (see http://en.wikipedia.org/wiki/The_Market_for_Lemons) and confirmed with the Italian experience regarding HSM security certifications.

Recommendation – amend article as follow

A qualified electronic signature shall be considered as valid provided that it can be established with a ~~high~~ *reasonable* level of certainty, that at the time of signing: (…)

Article 25(1)b

DTCE & CHAMBERSIGN recommend being more explicit with what is a valid certificate by adding not expired and not revoked.

Recommendation – amend article as follow

(b) the qualified certificate required is authentic and valid, *i.e. not expired and not revoked*;

Article 25(1)c

This point is confusing. Firstly, it confuses verification with validation (see comment on 3(31). Also, the verification data (public key) corresponds to the signing key (private key) not the data itself.

Recommendation – amend article as follow

(c) the signature verification data corresponds *to the signature creation data that were used to sign* the data provided to the relying party;

Article 27: eArchiving vs Preservation of signatures

The Regulation introduces the archiving service but does not give much detail at this stage. The preservation of qualified electronic signatures is a necessary tool but not sufficient….

The preservation of QeS is a piece of a much larger pie which is document preservation and DTCE & CHAMBERSIGN question the absence of provision supporting the development of such a service.

Article 27(1)

A trustable preservation service does not need necessarily to implement the various long term signature formats as specified in CAdES/XAdES/PAdES. If it is trustable, its assertion that one certain document was submitted to no change during the preservation period is enough, even without implementing the above mentioned long term signature formats.

Recommendation – amend article as follow

A qualified electronic signature preservation service shall be provided by a qualified trust service provider who uses procedures and technologies capable of *ensuring the reliability and the validity of the electronic signed data for the entire storage period* ~~extending the trustworthiness of the qualified electronic signature validation data beyond the technological validity period~~.

Article 29(3)

Same as above (Art. 21), it's not clear if suspending a certificate (revocation reason "onHold") is still allowed. If yes, the clause should be changed, from "revoked" to "*definitively* revoked"). Moreover, it should make clear that the loss of validity starts from the revocation time (i.e. signatures applied before the revocation time are still valid).

Recommendation – amend article as follow

If a qualified certificate for electronic seal has been *definitively* revoked after initial activation, it shall lose its validity *after the revocation time*, and its status shall not in any circumstances be reverted by renewing its validity.

Article 33(1)

Recommendation – amend article as follow

A qualified electronic time stamp shall meet the following requirements:

a) it is accurately linked to Coordinated Universal Time (UTC);
b) it shall be unfeasible to change the data undetectably;
c) it is based on an accurate time source;
d) it is issued by a qualified trust service provider;
e) it is signed using an advanced electronic signature or an advanced electronic seal of the qualified trust service provider, or by some equivalent method.

Article 34(4)

It is important that formats of eSignatures and eSeals are defined otherwise we will be back to the actual difficulties. Also, guidance on the applicability of Seals is needed to better understand its implications for users and trust services.

Recommendation – amend article as follow

The Commission *shall* ~~may~~, by means of implementing acts, define formats of electronic signatures and seals that shall be accepted whenever a signed or sealed document is requested by a Member State for the provision of a service online offered by a public sector body referred to in paragraph 2. Those implementing acts shall be adopted in accordance with the examination procedure referred to in Article 39(2). Also, further guidance may be provided by the Commission on the applicability of electronic seals.

Article 35(1)

This provision is too soft. It seems that any e-mail service is acceptable, even plain e-mail, worse if gmail, Yahoo! and the likes are used.

Recommendation – amend article as follow

Data sent ore received using an electronic delivery service shall ~~be admissible~~ *not be denied legal effectiveness and admissibility* as evidence in legal proceedings *solely on the grounds that it is not a qualified electronic delivery service* ~~*with regards to the integrity of the data and the certainty of the date and time at which the data were sent to or received y a specified addressee.*~~"

Article 36(1)b

What does unambiguous identification mean? Is that a requirement for a strong correspondence of an email address and a physical/legal person?

Recommendation

This point should be clarified.

Article 36(1)c

DTCE & CHAMBERSIGN recommend making the article clearer.

Recommendation – amend article as follow

(c) the process of sending or receiving of data must be secured *at least* by an advanced electronic signature or an advanced electronic seal of qualified trust service provider in such a manner as to preclude the possibility of the data being changed undetectably;

Article 42

There are only twenty days from the publication in the EUOJ for the entrance in force of the Regulation. It looks a very short time for implementing technically all the changes to the status

quo. DTCE & CHAMBERSIGN recommend a longer migration period. Also, pre-publication of a revised draft indicating the likely form of the final Regulation would assist all parties in better preparing for migration.

3.3 Annexes

Annex I, II & IV
At least in the UK, not all legal persons need necessarily to have a registration (e.g. sole trader).

Annex I

Recommendation – amend article as follow
Qualified certificates for electronic signatures shall contain *as a minimum*:

Annex I letter h
It makes no sense. The certificate to be used to validate the signature on a certificate shall be in the trusted list and putting it into the certificate can be only confusing.

Recommendation – amend article as follow
~~the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;~~

Annex II (1) letter b
It is impossible to verify this requirement.

Recommendation – amend article as follow
the probability that the electronic signature creation data used for electronic signature generation can occur ~~only once~~ *more than once shall be negligible;*

Annex II (4) letter a

Recommendation – amend article as follow
the security of the duplicated datasets must be *at least* at the same level as for the original datasets;

Annex III

Recommendation – amend article as follow
Qualified certificates for electronic seals shall contain *as a minimum*:

Annex III letter h
It makes no sense. The certificate to be used to validate the signature on a certificate shall be in the trusted list and putting it into the certificate can be only confusing. To be removed.

Recommendation – amend article as follow
~~the location where the certificate supporting the advanced electronic signature or advanced electronic seal referred to in point (g) is available free of charge;~~

Annex IV letter i
It makes no sense. The certificate to be used to validate the signature on a certificate shall be in the trusted list and putting it into the certificate can be only confusing. To be removed.

Recommendation – amend article as follow

~~the location of the certificate validity status services that can be used to enquire the validity status of the qualified certificate;~~

Annex IV letter j

In line with standard practice (RFC 4366, CAB baseline) this is not necessary if the OCSP is "stapled" to the web access protocol.