# DTCE position paper – eIDAS Secondary legislation on Server Signing

Thursday 3 July 2014

## Introduction

Several members of the DTCE association directly follow the standardisation work in CEN / TC224 WG17 (460 mandate) on the Protection Profile "server signing". This Protection Profile aims to define conditions on the server software signature, according to which such a signature method, implemented by a QTSP, will enable to produce qualified signature under the signification of the eIDAS Regulation.

A question has been raised by CEN asking for clarification on whether the local component supporting authentication and remote control of the signing key needs to be certified under Article 29 of the eIDAS regulation.

Three cases have been envisaged by the CEN working group: (1) one involving a local user device using a specific hardware to support remote signing, (2) the second using a local user device with a software to support remote signing, (3) the last based around more general purpose two factor authentication mechanisms with no specific local user device certification requirements with regards to remote signing.

DTCE believes that it is important to equally allow those 3 Cases. **If the development of specially certified user devices or the integration of dedicated hardware is required for remote signing, this will have inevitable implications on the cost and time to market (notably due to very frequent changes of client side platforms like PCs+Applets, mobile phones versions and operating systems, tablets, etc.) and so inhibit the general availability of pan European remote signing services.** If there are no specific certification requirements for remote signing, particularly with the potential general availability of interoperable eIDs through the provisions of the eIDAS regulation, it is believed that pan European market solutions can be made readily available.

The following document further analysis on the issues relating to these three cases.

Table of Content

# Most Relevant eIDAS Articles

*Whereas [...]*
*(52) The creation of remote electronic signatures, where the electronic signature creation environment is managed by a trust services provider on behalf of the signatory, is set to increase in the light of its multiple economic benefits. However, in order to ensure that such electronic signatures receive the same legal recognition as electronic signatures created in an entirely user-managed environment, remote signature services providers should apply specific management and administrative security procedures, and use reliable 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. Where a qualified electronic signature has been created using a remote electronic signature creation device, the requirements applicable to qualified trust services providers set out in this Regulation should apply.*
*[...]*

*Article 29.1*
*Certification of qualified electronic signature creation devices*
*1. Conformity of qualified electronic signature creation devices with Annex II shall be certified by appropriate public or private bodies designated by Member States.*

*Annex II [...]*
*3. Generating establishment or managing electronic signing data on Behalf of the signatory may only be done by a qualified trust service provider.*
*[...]*

# DTCE Analysis

DTCE members have issued a warning to the industry about the ongoing work in CEN TC 224 WG17 on certification requirements for remote signing, and we, as DTCE, wish to offer the following analysis of the situation and issue recommendations for decision makers.

If we acknowledge the need to certify the server to ensure a good level of security assurance and to avoid poor solutions, we however wish to draw the attention of the Commission on the risk of escalating security in developing of this standard, under the impetus of industrial interests, which could lead to miss the target of generalising electronic signatures in Europe.

Discussions within the WG17 have showcased three possible technical approaches:

- Case 1: the solution is based on a certified server in which signing keys are activated by a client component using hardware, itself certified, with security requirements that tend to forbid any solution other than a "secure element"

- Case 2 : the solution is based on a certified server in which signing keys are activated by a client component using software, itself certified

- Case 3: The solution is based on a certified server in which signing keys are activated by a 2-factor authentication (such as ISO level 3, for example a PIN + random code received by SMS or a physical device generating a random one time code, etc…),

These three approaches present a very good level of security with regards to the risk associated to the electronic signature operations, and can cover the market with a broad consensus for both suppliers and users. Despite this, the representatives of the smart card industry, which participate in the group as main editor of the standard, try to exclude, through convoluted writing, any possibility of achieving qualified signature otherwise than using a certified client component, which would lead to impose again a “secure element”.

Faced to this situation, we, as industry representatives, feel the great necessity to:

- Maintain the possibility of using all cases for qualified signature. It may be that a generic drafting would encompass all cases within a simpler standard

- Show that restricting to Case 1 would be, by our experience, a strategic error, which can cause serious harm to the market in the coming years

Service Providers who are willing to implement electronic signatures on a large scale do not want to stay in the legal uncertainty where they are today with the advanced signature ; they rather need to obtain (at last) the equivalent probative force between electronic signature and an handwritten signature provided by the eIDAS regulation in article 25-2, and they also need to benefit from a recognition of signatures across Europe. They want, as well as the European legislator, a generalisation of the use of qualified electronic signatures, that can also rely on remote signing technique, which is today the only one that can be immediately deployed on a large scale, particularly in Member States where citizens are not equipped with (or do not have the ability to use) a personal signature device based on a secure element.

Case 1 is at risk of not being large-scale deployable at short-term throughout the Union:

- Case 1 using a physical secure element requires that:
    - manufacturers have developed products
    - the products are brought to maturity
    - software (middleware) are stably supported on all types of devices (PCs, tablets, smartphones)
    - devices can be connected to all types of terminals (PCs, tablets, smartphones), being understood that the use of electronic signatures currently migrates rapidly from the traditional PC to tablet terminals (point of sale or home) and tomorrow even to smartphones
    - in all Member States, these devices are widely deployed to citizens
    - the offer of services associated with these devices is sufficiently mature and attractive for citizens to see value in using them frequently

    It is unthinkable that it takes less than 5 years, and more likely 10 years

Thus, restricting the use of server-based qualified signature to Case 1 would create a situation of vacuum of offer for at least 5 years. From our point of view, this would create a great disappointment from the stakeholders vis-à-vis the eIDAS Regulation and the final abandonment of electronic signatures in favour of alternatives solution (graphometric pad, signature in the cloud without authentication, etc ... ) ; the European industry would take no benefit out of it, and the Member States would gain no advantages in improving security of digital transactions.

Contrariwise, allowing Case 3, and also Case 2 with the use of the security mechanism that are currently deployed (for example the Samsung Knox solution which it has recently being announced will be integrated in the next major version of Android), can guarantee to encompass solutions that can be deployed immediately at large scale, and brings together a broad consensus among European TSP and Service Providers. In addition, it enables:

- Massive and quick improvement of the level of security of digital transaction by urging Service Providers to use strengthened authentication methods and certified server solutions with the reward of benefitting from a genuine legal security.
- Preparation of the ground for a more widespread use of electronic signatures in Europe, allowing multi-application and multi-sectorial solutions, such as those promoted by the smart card industry
- Easy integration of signature services with the range of European electronic identity schemes which are to be interconnected under the eIDAS regulation
- More flexible capability to adapt to new threats or new technology context by being more technology neutral (compared to the replacement of massive sets of secure element rolled out on the field)

It is also important to remind that within eIDAS, Qualified Signature in server mode does not only require a certified server software but also a service operation performed by a Qualified Trust Service Provider (which will be subject to a third part audit by a Conformity Assessment Body against security requirements under the national supervision scheme), and the issuance of a Qualified Certificate, which are strong additional guaranties for global security of the service.

As an example, there are already countries like Austria and Italy where solutions corresponding to Case 3 are widely deployed, under the supervision of the national authorities, and even after its widespread use, no relevant security issue is reported.

Finally, we believe that it would be a strategic mistake to think that one can protect industrial interests by blocking the situation for several years. This situation is already that of the 1999/93 Directive (which requires the secure element for qualified signature), and the use of the signature of this type is actually nonexistent today for citizens / individuals in most states members. We believe that the solutions requiring dedicated hardware component or dedicated hardware supported security may develop over time due to their intrinsic qualities that include:

- The ability to use a single credential for all types of transactions; this advantage becomes crucial when the use has become frequent (we can estimate “frequent” as at least 1 transactions per week per user); we can also expect a future generalisation of the NFC technology that could solve the current problems of connectivity

- Minimising the number of face to face with a transitive trust model, face to face is a mandatory condition for issuing a qualified certificate and therefore a qualified signature; this advantage becomes crucial when there is a large number of acceptors of electronic signature

- Cost reduction when use becomes massive (for example, an SMS costs between 6 and 10 cents for each transaction)

But for those qualities to become effective, it is needed the time required for maturity of offers (including the connections on mobile devices) and the widespread usage. Let us recall in this regard that the eIDAS regulation allows the revision of implementing acts, and includes a provision for review every 4 years, under a progress report, which will enable to make a regular assessment of the quality of offers and the development of uses.

# About DTCE

DTCE is a trade association formally registered under Belgian law that represent the interests of ICT trust and compliance vendors and practitioners in Europe.

DTCE's member companies want to ensure that the views and expertise of those who have invested in innovation and high quality delivery of ICT trust and compliance products and services are appropriately presented and taken into account in European policy debates about e-signatures, e-ID, e-procurement, e-invoicing and many other topics.

The products and services provided or used by DTCE members enhance the reliability billions and interactions on the Internet and other electronic networks every year. We believe that Europe can and must be a leading force in the continuous development of ICT trust and compliance as a necessary condition for the sustainable growth of e-commerce, e-business and e-government.