eIDAS - Certification of SSCD

Article 23 - Proposal for a regulation on electronic identification and trust services
COM(2012) 238/2

Summary message:
The proposed regulation should make the certification of SSCD mandatory. The security level of each components of the SSCD should be left to delegated acts and implementing acts.

European Commission proposal Article 23 - Certification of qualified electronic signature creation devices

> 1. Qualified electronic signature creation devices may be certified 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.

Our assessment on optional/mandatory certification of SSCD

The eID and eTrust services Proposal for Regulation foresees that the security certification of SSCD is optional. Experience shows that optional certification is not the right option.

1. If something "may be certified", no one will certify anything. The certification process is expensive and the savings will be quite large for the TSP that does not go through the process. An optional certification will lower cybersecurity in Europe.
2. End users of eIDAS products and services don't know/understand what certification of an SSCD means. In absence of a standardised security certification framework for technical devices, the end users will either trust any certificates without understanding the difference of quality or in contrary refuse to trust any certificates that they don't know. In the past, such confusion has led some Member States to introduce national regulation on top of the eSignature Directive which led to severe interoperability difficulties.
3. European leading industries in comparison to US industries have invested in strong security for over a decade and have a competitive edge.

How to organise mandatory certification of SSCDs

Transforming the optional certification of SSCD into a mandatory certification of SSCD is not without risk. The definition of SSCD in the proposal for regulation is very wide. Actually, an SSCD is made of hardware (1), card/device Operating System (2), Card/device application (3).

The level of certification expected for each of these 3 layers should be different. Layers (1) & (2) are produced at large scale and have pretty long product cycle. Layer (3) is produced at lower scale and sometimes address very regional/small markets. The software life cycle is also shorter as regular updates of the software are release to offer innovation or simply mitigate software bugs. Therefore we recommend that:

1. The certification of hardware and card/device OS shall be relatively high
2. The certification of device applications shall be made mandatory but at a much lower level (e.g. CC EAL1 vs EAL4)

Please note that certification at high level should be also required for the solutions where personal cryptographic material (such as private key) is kept within shared environment and therefore the logical access to the system is essential (e.g. server side signature). It is necessary that in these solutions the application used is certified at higher level and that the organisational measures managing the application are routinely audited by external audits. Example of such a solution where we find these requirements adequate would be server side signatures.

The detailed requirements for the level of certification are very difficult to get right defined in basic legal act (proposed regulation). The appropriate balance between security and what can be achieved in a practical cost effective manner would require more detailed technical discussion that may be conducted by the European standardisation bodies. We urge the European legislator to postpone the definition of security level for secondary legislation. (delegated acts and implementing acts). The current regulation should keep it to the basic which is: SSCD shall be certified.

On a broader level, we wish the European Institution to promote the recognition of the EU certification standards, based on the ISO Common Criteria framework and the SOG-IS MRA, in the US.

* *
*

For more information, please contact:

Vincent Tilman
Senior advisor EUROCHAMBRES
Managing Director ChamberSign
Board Director DTCE
tilman@eurochambres.eu
+32 2 282 08 67

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.*

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.eu.*

EUROCHAMBRES *is the association of European Chambers of Commerce and Industry. EUROCHAMBRES voices the interests of over 20 million member enterprises in 45 European countries through a network of 2000 regional and local Chambers represented by 45 national and two transnational organisations. More than 93% of these enterprises are Small or Medium Enterprises. Chamber members employ over 120 million employees.*