Cloud Signature Consortium and the main organizations in qualified trust service sector warn of grave risks in article 24 of the eIDAS 2 regulation in the ITRE Committee Report

The Cloud Signature Consortium (CSC) and the other organisations representing stakeholders in the qualified trust services sector, wish to express their grave concerns over proposed amendments in the eIDAS 2 regulation that will negatively impact consumers and the trust services sector.

The ITRE Committee Report mandates the elimination of assurance level "substantial" in article 24 of the eIDAS 2 regulation. The original text of the eIDAS 2 proposal allowed the verification of the identity of a user for the issuance of a qualified electronic signature and qualified electronic attestation of attributes using an eID scheme with a level of assurance "substantial" or "high", while the final version of the text adopted by the ITRE Committeeremoves references to "substantial".

While we understand the best intentions of Members of the European Parliament in the ITRE Committee, the qualified trust services sector has grave concerns over this move and of the consequences for the citizens. A number of widely used eID schemes in Europe have an assurance level "substantial" and are the preferred method of identity verification for citizens, driven by increased user-friendliness.

Even for countries with notified eIDs level of assurance (LoA) high, the most widely used eID systems throughout Europe are fully digital and with a LoA substantial. Some examples are the SPID identification scheme in Italy that is arguably one of the most widely used systems in Europe, with 33 million active citizens. Other successful LoA substantial systems are the Swedish BankID and FrejaID+[1], that counts more than 8 million users, the Danish NemID/MitID (more than 5 million citizens) and the French FranceConnect that counts more than 41 million users and is in the phase of update from LoA low to LoA substantial[2]. These numbers and statistics show that countries with a LoA substantial eID scheme saw a rocketing adoption and use of it, creating value to the citizens and a fertile environment for Qualified Trust Service Providers (QTSPs) for the issuance of Qualified Certificates, that enhance the overall level of security of electronic transactions.

Although other schemes with LoA high exist, such as the Italian Electronic Identity Card CIE and the German Personalausweis, these are hampered by a lack of user-friendliness: many citizens have these identity cards as well, but they are not actively using them for qualified signatures or for accessing public services. **A LoA high eID scheme relies on a physical card with a chip, generally with NFC function, that can be read only with compatible handsets or smart-card readers**. To be concretely used to generate qualified signatures, citizens shall activate the eID function creating a PIN code that shall be remembered and inserted at every signature. The smart-card reader needs additional installations and periodically updates of middleware software in order to properly function with the computers.

The complexity of the process is shown by the statistics: in Germany every citizen has an identity card (more than 60 million) but in 2021 the eID function has been used only 11 million times[3], a tiny number compared to the usage of SPID, that reached 1 billion transactions[4].

Members of our organizations are very concerned that, if LoA "substantial" is removed, existing popular schemes will have to stop being used. The direction in the EU is that Qualified Electronic Signatures (QES) are the preferred signature level both nationally and in particular for cross-border communication. The current text proposed for the Art.24 will jeopardize mainstream availability of QES with severe consequences for the citizens and stakeholders (banks, insurance companies, utility providers, health care providers). Despite the expectation of policy makers in the ITRE Committee that this move will result in a wider adoption of schemes with LoA "high", such as the eIDAS 2 wallet, our experience suggests that citizens and the market will opt for user friendliness and shift away from qualified trust services, which will become less easy to obtain, towards

[1] source: https://www.bankid.com/en/om-oss/statistik
[2] source: https://franceconnect.gouv.fr
[3] source: https://dashboard.ozg-umsetzung.de/
[4] source https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2023/01/11/piu-miliardo-accessi-tramite-spid-2022

less regulated options with a reduced level of security (advanced signatures). The main driver behind this shift will be simplicity in the identification process, at the expense of security.

Moreover, the elimination of LoA “substantial” means that numerous well-established identification schemes used by millions of European citizens can no longer be used for the issuance of Qualified Electronic Signatures, Qualified Electonic Seals, Qualified Webserver Authentication Certificates and other trust services.

In addition, although the draft eIDAS text envisages a transition period for this switch, this will most likely result in a lack of harmonisation in the EU, as different Member States are likely to deploy eID schemes at different speeds, while putting increased pressure on conformity assessment bodies, who would have to certify the new schemes.

For the reasons mentioned above, we urge Members of the European Parliament to reinstate the assurance level “substantial” in article 24 (in line with the **European** Commission’s initial proposal), and revisit the issue in the future, following further assessment of the feasibility of LoA “high”.

We remain at the disposal of Members of the European Parliament for any clarifications and are keen to work with them to ensure a balanced text that offers strong consumer protection coupled with user-friendliness, in line with the wording and the spirit of the European Commission’s proposal. This balance will be necessary to make the goal of eIDAS 2 to boost the rollout of electronic identity schemes in Europe, a success.

Signed

Cloud Signature Consortium

CLOUD SIGNATURE CONSORTIUM

AssoCertificatori

Associazione dei Prestatori Italiani di Servizi Fiduciari Qualificati e dei Gestori Accreditati - Italy

AssoCertificatori

ESD – European Signature Dialogue

European Signature Dialog

ASEPEC - Asociación de Prestadores Cualificados de Servicios de Confianza de España - Spain

ASEPEC

Club PSCO – Club des Prestataires de Services de Confiance - France

ClubPSCo

Le club des Prestataires de Services de Confiance