

Responsibility

TELEKOM COUNCIL
Council WG eIDAS

Subject: Concerns Regarding eIDAS Review and Recent Compromise on Article 45 and Related Recital 32 - **Contradictory Wording**

Dear Madam /Sir,

The European Signature Dialog (ESD) represents the leading Trust Service Providers in Europe and appreciates the collaborative efforts of the Council, Parliament, and Commission in pursuing a feasible and beneficial compromise during the ongoing eIDAS trilogue discussions.

A provisional political agreement on the fundamental aspects was successfully achieved between the Council Presidency and the European Parliament at the end of June. Subsequent technical meetings have worked to implement the shared legislative intent.

However, we must express our **deep-seated concern regarding recent developments within the eIDAS trilogue concerning the provisions on Qualified Web Authentication Certificates (QWACs).**

In particular, our concern pertains to Recital 32, where seemingly simple language inadvertently **contradicts** the essence and intentions of the involved parties concerning the function of a QWAC, particularly its role in authenticating a website.

These contradictions have the potential to severely undermine the viability of QWACs, leading to profoundly detrimental results.

The most recent draft of Recital (32) has two problems as follows:

Text problem (1)

*** Recognition of QWACs means that the providers of web-browsers should not deny the authenticity of qualified certificates for website authentication **attesting the link** between the **website domain name** and the natural or legal **person** to whom the certificate is issued and confirming the identity of that person.

Text problem (2)

Providers of web-browsers should **hence allow for** the user-friendly display of the certified identity data and the other attested attributes to the end-user, in the browser environment, by relying on technical implementations of their choice.

As to text problem (1): Simply “attesting the link” between the website’s domain name and the website owner’s identity does not “authenticate the website”.

eIDAS (2014) stated that QWACs must “authenticate a website”. See Art. 3(38) defining a QWAC and also Recital (67). In the new language, the goal has been reduced to only “attesting a link” between a domain name and the website owner’s identity – which means the website itself is no longer authenticated and the user can be presented with a fake website!

The reasons why a “link” no longer authenticates a website’s identity are complex, and will not be covered in this statement. However, we have a proposal to fix this problem – remove the language about a “link” between the domain and the website owner information:

*** Recognition of QWACs means that the providers of web-browsers should not deny the authenticity of qualified certificates for website authentication ~~attesting the link between the website domain name and~~ *which attest the identity of the entity behind the website as* the natural or legal person to whom the certificate is issued and *provides a means for* confirming the identity of that person *to a high level of confidence*.

Independent of the technical implementation choices and above all else, the new eIDAS language should maintain the primary goal for QWACs as “authenticating the website” as it is today.

As to text problem (2): The current proposal says that browsers “should hence allow for” a user-friendly identity UI. That phrase is extremely ambiguous in the English language, and could be interpreted as giving browsers the choice or option (“allow for”) of whether or not to display a user-friendly UI.

This problem text is easy to fix – change the text to read as follows:

Providers of web-browsers should *show a* ~~hence allow for the~~ user-friendly display of the certified identity data and the other attested attributes to the end-user, in the browser environment, by relying on technical implementations of their choice.

Finally, the most recent draft of Article 45 does not require that QWACs have to confirm the identity to a high level of confidence, which it should. This problem can be fixed as follows:

45.1. Qualified certificates for website authentication shall meet the requirements laid down in Annex IV *and provide a means for confirming the identity of the entity behind the website to a high level of confidence*. Evaluation of compliance with those requirements shall be carried out in accordance with the standards and the specifications referred to in paragraph 3.

We earnestly hope that rectifying the contradictory wording can be achieved by the legislative parties, aligning your expressed intention with all sections of the text.

Yours sincerely

Michael BUTZ

Chair ESD