Dear Members of the Parliament,

We are the scientists who wrote open letters on the eIDAS draft regulation https://eidas-open-letter.org and https://eidas-open-letter.org/statement-23-11-2023.pdf.

The briefing note related to Art. 45 of this regulation was published on the internet yesterday. As it contains highly confusing and sometimes misleading information, we have decided to provide you with some comments and clarifications. We hope that this increases your understanding of the matter. We are always open for discussion.

Sincerely,

Members briefing note on the discussion around Qualified Website Authentication Certificates (QWACs) -Art. 45 of eIDAS Regulation

Despite the successful conclusion of the final trilogue on the eIDAS revision on November 8, an open letter has sparked a controversy around the Article 45 (QWACs) that is threatening to undermine the entire proposal. Subsequent to the publishing of the open letter, an aggressive disinformation campaign has been launched further spreading unfounded accusations.

We have written an open letter and discussed this letter with interested parties. It is unclear why this is called aggressive, as we have only provided inputs based on our technical expertise.

The open letter claims that the current proposal radically expands the ability of governments to surveil both their own citizens and residents across the EU by providing them with the technical means to intercept encrypted web traffic, as well as undermining the existing oversight mechanisms relied on by European citizens. It further claims that the technical implementation of these QWACs could affect the security of the Internet by interfering with the way in which web-browsers manage security and encrypt communication. The open letter claims that by mandating web-browsers to recognize the QWACs, the new Regulation could lead to a breach of encryption and allow it to intercept web-traffic.

On top of this, Mozilla has also engaged in its own campaign trying at all costs to preserve the monopoly of the web browsers to set their own rules outside of any regulatory system.

In view of the vote in ITRE on November 28, with this briefing we seek to revert to the facts-based discussion, to better inform Members and to also help with stakeholder communication.

1. What is a Qualified Website Authentication Certificate (QWAC)?

- A QWAC makes it possible **to authenticate a website** and that confirms that the **person or company behind a website is genuine and legitimate**. In other words, it gives assurance with a high level of confidence in the identity of the entity standing behind the website, irrespective of the platform used to display it.

- As such, **QWACs prevent identity fraud, protect the fundamental rights of European consumers in the digital world and are an important part of the European digital trust framework.**

2. Are QWACS new? Articles 45 and 45a mandate that all web browsers recognize a new form of certificate for the purposes of authenticating websites.

- Qualified Web Authentication Certificates (QWACs) **are not a new form of certificate.** They were defined in the original 2014 eIDAS Regulation in the Article 45 as part of Europe's push for "digital sovereignty" instead of domination by non-European big tech companies. They work in exactly the same way as other forms of website certificates that are also in use.

- **There is no information to suggest that the use of QWACS since 2014 has led to increase in mass surveillance of citizens by the governments, that they have in any way fragmented the Web or in any way undermined internet's trust architecture!!!**

Our open letter never suggests that QWACS are new. But before the current eIDAS regulation proposal browsers were not forced to add the root CA keys selected by Member States to their certificate stores. It is the fact that the regulation mandates that root CA keys signing these QWACs must be accepted in the store which increases the risk of mass surveillance, as pointed out in our letter, and not the existence of QWACs.

We also would like to note however that several governments (including at least one EU member state) have been caught in the past issuing fraudulent certificates to intercept TLS communications. In order to prevent this abuse and to reflect the loss of trust, the corresponding root CA keys were removed from browsers. The new eIDAS regulation would prevent this without the approval of the respective government. These attacks were not facilitated by QWACS, as at that time it was not necessary to add the Member State root CA

keys to the browser certificate stores, but the current proposal will make them easier in the future.

3. Why is eIDAS mandating recognition of web-browsers by the QWACs?

- QWACs are electronic certificates that provide independent assurance of the authenticity of a website by certifying its ownership. **It gives the users the assurances that they are interacting with a genuine website helping prevent internet fraud**. They, thereby, improve the security and transparency of the internet. As QWACs attest the authenticity of websites, they require the technical support of web-browsers to function correctly.

Whether QWACs can give strong assurance to users, and indeed improve their security depends on which security standards are developed and which processes are deployed to govern the QWACs. The fact an article in the body of the regulation restricts the security measures browsers can take with respect to QWACs does not give us confidence that this will be the case.

- Since web browsers have not voluntarily recognised QWACs since their creation by the eIDAS regulation in 2014, the Commission has proposed to make this recognition compulsory.

Like any other CA issuing certificates, providers issuing QWACs were and are free to follow the security processes established by browsers in order to be recognised. Many QTSPs are already recognised by browsers.

- Recognition means that web browsers are required to **ensure support and interoperability for the QWACs for the sole purpose of displaying identity data in a user-friendly manner.**

This is misleading for the following reasons. Currently QWACs are TLS certificates. The expression "for the sole purpose" suggests that in a TLS connection displaying identity data in a user-friendly way can be decoupled from securing the communication. In the TLS protocol, the server provides a certificate and the public key in this certificate serves to both authenticate the identity of the server **and to derive an encryption key** to be used during the browsing session. In the current version of the TLS standard, the derivation of the session key and the identity are strictly coupled.

Second, there have been efforts to clearly show identity data in browsers (Extended Validation). They have been abandoned as it was demonstrated that they did not improve security - to the contrary, they were used by fraudsters to mislead users.

- Recognition of QWACs implies that browsers shouldn't question the origin, integrity or data in the certificate.

QWACs include public keys that are used for authentication. Not questioning the data of QWACs means that browsers must accept web authentication based on these keys. As we explained before, due to the operation of TLS in which authentication and creation for encryption keys is entangled, mandating the recognition of authentication opens the door to interception attacks.

Currently, browers, with the support of the security community, continuously monitor the security requirements of certificates. Browsers have the responsibility to impose minimum security requirements to all certificates trusted by them. If the EU wants to impose stricter requirements, that is not a concern. But if the eIDAS regulation disallows existing security checks such as Certificate Transparency, or does not permit the addition of new verification means in the future, that would be highly problematic. The current draft leaves the door open to do so and this is one of the reasons for our concern.

4. Who issues QWACs?

- QWACS are issued by Qualified Trust Service Providers (QTSPs), under the close supervision of the Member States' authorities, similarly to all other qualified trust services. National trusted lists may be used to confirm the qualified status of QAWCs and of their trust service providers, including their full compliance with the requirements of this Regulation with regards to the issuance of qualified certificates for website authentication.

See also the last comment under point 3 with respect to these requirements. As the standards are not defined, it is unclear what the requirements will be. It has been decided to NOT include certain guarantees in the main body of the draft regulation, but to leave them to Recital 32. It is unclear what the legal status is of a guarantee in the recital if it contradicts the main body. Note the recent judgment of ECJ Case C-307/22: "the Court reminded that recitals cannot restrict the scope of rights granted in the GDPR (paras. 43-44)." This is a different case but it highlights the limitations of recitals.

5. Who are Qualified Trust Service Providers (QTSPs)? How do they get their qualified status?

- QTSPs are trust service providers who provide **one or more qualified trust services** and are granted the *qualified* status by the Member States' supervisory bodies. Put simply, they are providers of trust services whose **high level of security, data protection, and compliance** are subject to regular independent audits and certifications. As a result, there is greater assurance of the legal validity of their services.

- Before a trust services provider is granted a qualified status (QTSP/QTS), it will be subject to a pre-authorization process — the so-called initiation process. QTSPs may only begin to provide the qualified trust service after the qualified status has been granted by the competent supervisory body and indicated in the national trusted list. Before being granted the qualified statues, the QTSP must successfully pass an external assessment (audit) to confirm it fulfills the eIDAS requirements. That audit must be conducted by a conformity assessment body specifically accredited to carry out assessments of a QTSP.

- For example: a qualified status in Germany is only granted by the independent supervisory body (e.g. Federal Security Office in Germany) after auditing is completed by a conformity assessment body (e.g. TÜV).

While audits can help, it is unclear what is being compared to ("greater assurance"). If this suggests that this system will provide higher assurance than the current webPKI: in our view this case has not been made and the premise remains highly questionable. The above paragraphs make it sound like these audits offer a watertight guarantee, which is misleading. For example, DigiNotar was issuing qualified certificates and it was hacked leading to its bankruptcy. Infineon chips were shown by academic researchers to be vulnerable (the ROCA vulnerability) even if they were evaluated by an accredited assessment body and used in identity cards in a Member State. The Member State was only informed of the vulnerability after a long delay in spite of all the processes.

While we recognize the potential added value of these auditing processes, it is crucial to highlight their current lack of transparency. Enhancing the transparency of both the processes and outcomes of these audits would be beneficial, fostering a greater understanding and trust in the overall procedure.

6. Will all European websites be government mandated to use QWACs?

- No. The provision and the use of website authentication services, including QWACs, is entirely voluntary and subject to market competition in the domain of website certificates. The use of QWACs is **not subject to a government mandate -natural and legal persons are free to choose from a number of different browser certificates currently available on the market,** such as EV, OV or DV certificates.

But the current eIDAS draft specifies that all browsers are mandated to recognise certain CAs issuing QWACs. Hence the freedom of choice for the citizen is suddenly reduced and restricted by the text because the citizens suddenly cannot choose a browser that enforces stricter security checks which would result in the browser not including some of the root certificates that issue QWACs.

7. Does the eIDAS Regulation intend to change the way browsers ensure web security?

- No. The requirement to recognise QWACs **does not, in any way, affect browsers own security policies.** Art. 45 leaves it up to the web-browsers to preserve and follow their own procedures and criteria for encryption and authentication of certificates in line with best industry practices.

This is factually incorrect. The requirement to recognise QWACS does affect and restrict browsers in terms of security policies. Art. 45 does state that browsers cannot impose their own procedures and criteria:

> "Art 45a. 1. Web-browsers shall not take any measures contrary to their obligations set out in Art 45, notably the requirement to recognise Qualified Certificates for Web Authentication, and to display the identity data provided in a user friendly manner."

- Amended recital 32 explicitly states that "**The obligation of recognition, interoperability and support of QWACs is not to affect the freedom of web-browser providers to ensure web security, domain authentication and the encryption of web traffic in the manner and with the technology they consider most appropriate**."

We are pleased with the clarification provided by Recital 32, but in our view this recital contradicts the main body of the text. In view of a comment made above, this creates serious doubts about the legal value (e.g., ECJ Case C-307/22).

8. Do the rules on QWACs facilitate government surveillance of citizens and the interception of web traffic?

- No. QWACs are certificates that allow to identify the entity behind a certain website. These certificates are issued by public or private trust service providers as a commercial service. **QWACs have no other function than to attest the identity behind a website.** Browsers are required to recognize them for the sole purpose of displaying this identity.

The statement "**QWACs have no other function than to attest the identity behind a website."** is technically wrong. In TLS, QWACs are also used to establish an encryption key and if QWACS are issued with an incorrect public key, the owner of the corresponding private key can intercept and read the communications sent to this server. At this moment, there is no standard to separate these concerns, for example where one (QWACs) certificate specifies an identity and another one a public key for confidentiality.

- The recognition of QWACs does not oblige web-browsers to grant QWACs automatic access to their root stores. The obligation to recognise QWACs does not, therefore, affect

browser security policies and leaves them complete freedom to preserve their own procedures and criteria for encryption and authentication of other certificates.

This paragraph is misleading and technically incorrect. Web-browsers have to grant access not based on their own procedures but based on procedures established by others. It does leave them indeed freedom for security checks for other certificates, but not for QWACs. The problem of the webPKI ecosystem is that the bad behavior of a single root CA (including an accredited CA issuing QWACs) is sufficient to undermine the security of all the websites on the Internet.

9. Does the requirement to recognize QWACs in Article 45 make it impossible for web browsers to raise security issues with QWACs?

- No. QWACs are trusted electronic certificates issued to common standards by accredited EU trust service providers. The issuance is supervised by national authorities which should act in full compliance with the requirements of the Regulation.
- In order to ensure a fully harmonized approach to national supervision and avoid that any Member State would follow lower supervision standards, the eIDAS Regulation foresees the development of specific standards and procedures that will need to be followed by all national supervisory bodies within 12 months of the entering into force of the Regulation.
- Should there be security incidents, web-browsers are free to take precautionary measures to protect the security of the Internet. This has (be)en clarified in Recital 32.
- It is important to ensure the correct functioning of QWACS. For this reason, the Regulation does not allow Member States or private parties to impose additional requirements to those set in the Regulation. [Article 45(2a)].
- The prohibition of additional requirements is of course without prejudice to the responsibility of web-browsers to ensure web security, domain authentication and the encryption of web traffic.This has been clarified by co-legislators in recital 32 which includes a provision that the rules on QWACs shall not affect the freedom of web browsers to ensure web security, domain authentication and the encryption of web traffic in the manner and with the technology they consider most appropriate.

It was never stated (and definitely not in our letter or statement) that browsers cannot raise security issues. This is the wrong question.

It is correct that the current eIDAS draft allows web-browsers to take **temporary** cautionary measures, but that the ultimate decision lies with the national supervisory authority. This authority may well base itself on national security reasons to force browsers to stop the

temporary cautionary measures. Hence the ultimate decision does NOT lie with the browsers. In view of this, the whole paragraph 9 is misleading.

10. What is the procedure for web-browsers to raise security concerns on QWACs? [Article 45a, Recital 32]

- In case of substantiated security concerns regarding security or integrity breaches of QWACs, web browsers may take precautionary measures to protect the integrity and security of the internet. **Taking such precautionary measures is fully at the discretion of web-browsers and not a specific obligation set in the Regulation.**
- When taking these precautionary measures, **web browsers shall notify all concerned parties and notably the national supervisory body of its concerns and the measures taken**.
- The national supervisory body will take a decision on the integrity of the QWAC in question and may request it to be withdrawn.
- This process is only intended to secure the correct functioning of QWACs in the web environment and does therefore not cover other certificates used by web-browsers to ensure web security, domain authentication and the encryption of web traffic, such as TLS certificates. The Regulation does not introduce general reporting obligations on certificates used by web-browsers.

- The independence of web-browsers when it comes to the management of web-security has been clarified by amendments to recital 32. These amendments state that the rules on QWACs shall not affect the freedom of web browsers to ensure web security, domain authentication and the encryption of web traffic in the manner and with the technology they consider most appropriate.

The third bullet point: the national supervisory body may also decide that the QWAC should not be withdrawn.

The fourth bullet is very misleading. If QWACS are used to identify the servers in TLS, the current standard means that they bootstrap web security, domain authentication **and encryptio**n of web traffic. And as stated before, the webPKI is such that a single malicious CA (including a CA issuing QWACS) can undermine the security of all the internet users who have this CA in their browser trust store (even when they visit websites that have certificates from other CAs or non-QWACS certificates).

11. The current system works -why change it?

- Amended eIDAS Regulation creates a balance between the EU and the browsers. Right now, **there is no recourse or oversight to browsers' decisions**. Browsers are BOTH **competitors of EU Qualified Trust Service Providers (QTSPs)** – browsers also issue website certificates to their cloud hosting customers -**AND regulators of QTSPs through the browsers' own root program rules.**

- Browsers have abused their monopoly regulatory powers in the past and are in the process of doing so again by forcing all website owners and QTSPs to move to automated 90-day website certificates (instead of the current 13-month certificate limit), even though there is widespread opposition in the internet ecosystem.

- Under eIDAS, the EU is able to exercise its digital sovereignty to protect EU citizens, but the browsers are also able to (1) participate in future rulemaking and (2) report any certificate problems they encounter from QTSPs to regulatory bodies for investigation. Browsers can participate in standardization forums like ETSI at any time – and some already do this – to strengthen the rules for the issuance of QWACs if they deem this necessary.

- Right now, the browsers just do what they want, and there is no recourse or oversight to theirdecisions.New eIDASchanges that.

Our open letter does not discuss whether or not browsers should be regulated. Our only point is that they should not be regulated through a regulation that deals with electronic identification, and definitely not by forbidding browsers, or leaving the door open to forbid them, from using strong security measures such as for example certificate transparency.

What definitely should not be done is regulating browsers through changes introduced during the trilogue process that are made public only very briefly before the final votes.

Most technical experts seem to agree that certificates with a shorter validity period have benefits as the difficulties with revocation are reduced and as this is an incentive to bring more automation to the process. We find it difficult to see any other motives than purely commercial ones to have a validity period of 13 months in order to be aligned with an annual billing cycle. Moreover, recent research shows that about about 60% of existing TLS certs already have lifetimes of 90 days or less according to Certificate Transparency Data (https://search.censys.io/search/report?resource=certificates&q=labels%3Dunexpired+and+labels%3Dleaf+and+labels%3Dtrusted&field=parsed.validity_period.length_seconds&num_buckets=10) and that shortening certificate lifetimes from 13 months to 90 days can yield a substantial decrease in stale (that is invalid) TLS keys (https://zanema.com/papers/imc23_stale_certs.pdf), which is a clear improvement for the WebPKI ecosystem.

12. The eIDAS Regulation is a law to ensure the digital sovereignty of the EU and to enable the European Digital Single Market. The eIDAS is not a security law and does not give police and security authorities more rights and powers, nor does it lay the foundation for surveillance and data access rights.

- The aim of eIDAS is to create trust anchors for digital transactions through strict, comprehensive regulation, which can be trusted comprehensively and generally by anyone involved in legal and business transactions. Any impairment of the status as an anchor of trust and weakening of the level of security is therefore unlawful.

- The accusation that EU member states would use this regulation to spy on their citizens is completely absurd.

- The suggested danger is purely hypothetical because a system of independent bodies guarantees security. The actions that would need to be taken for this would be costly (there are much simpler procedures for spying on citizens).

- An EU member would have to take illegal actions and ruin its reputation. In addition, there would be a high risk of detection of any such attempt.

- First of all, the approval of a QTSP already offers a high level of protection: it is only granted by the independent supervisory body (e.g. Federal Security Office in Germany)after auditing by a conformity assessment body (e.g. TÜV). This means that independent parties are still involved.

- Second, in order for the suggested danger to occur, an EU member state would have to completely and deliberately put itself in the wrong: It would first have to compromise a QTSP. In addition, the EU Member State would have to ensure that the independent conformity assessment body and (!) the independent supervisory body does not fulfill their inspection and supervisory duties.

- Finally, there would also be a risk that the European Commission, which must always be informed, would initiate infringement proceedings against the Member State if the browsers were reported due to security concerns.

- Incidentally, browsers are obliged under the US Homeland Security Act to provide data to US intelligence agencies on request.

We wholeheartedly agree that eIDAS is not a security law and that it should not give authorities more rights and power regarding security decisions. Our open letter clearly points out that this is exactly what the current draft does, and this is the reason why so many scientists and NGOs have signed the open letter.

For the first item: if this is the case, why does the regulation open the door to browsers being forced to reduce security requirements in a way that may well undermine the security of all the internet users?

For the second item: our letter shows that the current draft regulation opens this door to spying on citizens by putting restrictions on security rules by browsers in the body and softening those a little in the recital (but not in the main text) and by allowing that national supervision authorities can overrule temporary measures by browsers to protect the security of browser users. See also the comments on point 13.

For the third and fifth item: see DigiNotar and ROCA as discussed above.

For the fourth item: mentioning Pegasus may be sufficient to refute this point.

For the sixth and seventh item (starting with “Second”): And what would happen if an EU Member State would invoke national security to justify the situation? Would the national supervisory body or the European Commission be able to overrule this? We have serious reservations about this.

For the eighth item: incidentally, there are similar legal provisions in EU Member states that force service providers to deliver data and/or to collaborate for criminal investigations and national security purposes.

Finally, we would like to point out that if EU Member states use a regulation to force browsers to add additional CAs to their trust stores, without taking into account the minimum security requirements imposed by the browsers, other countries (including less democratic countries) will likely follow this example. This will result without any doubt in a further deterioration of the WebPKI ecosystem with disastrous consequences for all internet users worldwide.

13. Can Member States follow different security approaches for the Wallet? What is the added value of eIDAS 2.0?

- No. Member States cannot follow different security approaches for the Wallet.
- New rules provide for a fully harmonized framework which is implemented on the basis of common standards and technical specifications in the same way in all the Member States.
- All key features and requirements of the Wallet **will be implemented following common EU technical standards and specifications.** This is one of the main innovations of the Regulation for a European Digital Identity Framework. It means that it will become possible to use the Wallet in the same way in all Member States and offer users the same basic services and functionalities irrespective of which MemberState issues it.

- Currently existing national solutions are built on different solutions offering different levels of privacy and security protections.
- **A harmonized EU approach to digital identity management will also ensure compliance with data protection rules all over Europe** and include features, such as a dashboard to see the log of all interactions of the wallet, a possibility to download and transfer data and a possibility to directly lodge a complaint in case of data breaches.
- All technical specifications for the Wallet are being developed together with a group of experts from the Member States. In addition, the progress of this work is put to public scrutiny and feedback. First sets have already been published on Github.
- Once the technical specifications are finalized, they will be made mandatory through implementing acts following the usual process of public consultation.
- To ensure that these requirements are observed by all Member States, all Wallets must be independently certified to the highest security standards.The certification system will also follow harmonized standards and follow the EU Cybersecurity Act.
- Until this system is fully operational [estimate 2027/2028], Wallets will be certified at national level. However also in this transition period, standards will be the same and the certification by national bodies will follow common standards established by the implementing acts.
- In addition, all certification schemes will be submitted for opinion and recommendations to a joint group (European Digital Identity Cooperation Group) as an additional safeguard to ensure a harmonized approach and the highest degree of security. [Reference: Art. 6c(2a) (revised) and Article 46e(5)]

- **An important safeguard for security and harmonization is transparency: the colegislators have decided that the European Digital Identity Wallet will be open-source licensed.** This will contribute to public trust and improve the functionality and security of the Wallet as everybody can scrutinize the technological set-up proposed and provide feedback on the choices made. [Article 6a(2a), Recital 11d]

This paragraph ignores the fact pointed out in our letter that in the current draft, providing unlinkability and unobservability (w.r.t. service providers) is optional - Member States can decide to not offer unlinkability. Perhaps in the interpretation of the authors of this briefing note, unlinkability and unobservability are privacy properties and not security properties. Independent of this interpretation, we do believe that these are essential minimum requirements for such a large scale system affecting all EU citizens and both the public and the private sector.