Free markets. Real solutions.

EXPLAINER

European Union Electronic Identification, Authentication, and Trust Services (eIDAS 2.0)

Cybersecurity Legislative Analysis Series

Bill Summary: Electronic Identification, Authentication, and Trust Services (eIDAS 2.0, also known as Regulation (EU) 2024/1183) amends eIDAS 1.0 (Regulation (EU) 910/2014) to improve its effectiveness, extend its benefits to the private sector, and promote trusted digital identities within the European Union (EU).

Rating: CYBER CONCERNS This regulation aims to create a safe and secure digital identity ecosystem. While benefits exist, removing website authentication from capable organizations with a successful history and giving that authority to government entities is misguided.

Last updated: July 2024

Key Provisions

- Member states must issue European digital identity wallets (EDIWs) to all citizens, residents, and businesses who request them. These wallets allow users to securely and safely identify and authenticate themselves electronically to access various public and private services across the EU.
- eIDAS 2.0 extends the scope of the regulation to include electronic ledgers, diplomas, and professional certificates.
- Trust service providers verify identities and any other attributes of a person's identity and are subject to enhanced security requirements and privacy safeguards to protect user data and prevent identity theft and fraud.
- eIDAS 2.0 provides a legal framework to facilitate electronic transactions by ensuring they have the same legal status as traditional paper-based transactions.
- The regulation requires web browser providers to facilitate the use of qualified certificates for website authentication (QWACs).

Background

Introduced in 2014, eIDAS 1.0 intended to standardize electronic identification and trust services across the EU to facilitate cross-border digital transactions and services. However, it became apparent that the regulation failed to keep up with technological advancements and market demands. These limitations mainly stem from its focus on the public sector, the complex integration options for online private providers, and the insufficient availability of recognized European digital identity (eID) framework solutions across all member states. The regulation also lacked the flexibility to accommodate various use cases, and it had not been widely embraced by the EU population.

Adopted in April 2024 with full implementation planned for 2026, eIDAS 2.0 aims to establish a universal digital identity wallet with improved data security and simplified cross-border interoperability, and to facilitate a broader range of applications. However, stakeholders have expressed concern regarding Articles 45 and 45a, which could compromise internet security by affecting the root store programs and certificate authorities (CAs) of various web browsers and operating systems. Under eIDAS 2.0, government-endorsed CAs issue QWACs to websites. If a web browser company suspects or detects a security issue with the QWACs, they are unable to distrust it—thus creating potential security holes that expose users and websites to cyberattacks or potential government interception or surveillance.

Key Takeaways

- eIDAS 2.0 is rated cyber negative because its flawed Article 45 provisions and push for digital sovereignty could undermine global internet safety. The regulation takes web privacy and security from the hands of capable organizations to a supranational level of government. Industry, technologists, and civil society have discussed at length the security risk Article 45 poses.
- Through its unpopular, mandated QWACs, eIDAS 2.0 attempts to fix a system that is not broken. Some critics have argued that QWACs rely on a "discredited security architecture" that "weakens trust and online security."

Free markets. Real solutions.

EXPLAINER

European Union Electronic Identification, Authentication, and Trust Services (eIDAS 2.0)

Cybersecurity Legislative Analysis Series

Cybersecurity Analysis

FACTORS	ANALYSIS
Applicability	eIDAS 2.0 applies to electronic identification schemes notified by a member state, EDIWs issued by member states, and trust services providers established in the EU.
Impact on cyber actions	Internet browser developers are compelled to trust government-approved certificate authorities despite the potential security shortcomings of the certificates themselves or the standards they adhere to, which could lead to cyberattacks or government interception or surveillance. The regulation introduces a number of new trust services, from electronic registered delivery services to electronic certificates for services and websites to electronic archives and ledgers—all of which broaden the attack surface and widen the possibility of a cyberattack or disruption. While EDIWs must adhere to the "highest level of security," including the EU Cybersecurity Act and the EU General Data Protection Regulation, their cross-border nature and online component make them susceptible to interception, tampering, or extraction. Trust services providers face regular security audits and are liable for damage caused by failure to comply with security and risk management obligations.
Business impact	Web browsers must recognize government-mandated root certificate authorities and cannot deny their authenticity. This could undermine internet security, creating issues across multiple web browsers and impacting many industries including finance, health, and commerce. Compliance costs can impact businesses negatively, especially small- and medium-sized ones.
Data privacy and data security	Data centralization creates security vulnerabilities by introducing a single point of failure. Moreover, combining datasets that should remain segregated for privacy and security reasons (i.e., digital identity and health or financial information) makes any compromising event catastrophic. Further, compromised government-mandated certificate authorities could create security vulnerabilities by intercepting and exploiting an internet user's traffic. Government regulators move more slowly and cannot remove compromised certificates at the speed that private companies do. Potentially, other countries with differing ideologies could follow the EU's example and easily intercept user online traffic by carrying out man-in-the-middle attacks that undermine public key infrastructure worldwide.
Rulemaking or update mechanisms	The European Commission (the EU's executive branch) can initiate the rulemaking process by drafting a proposal for an amended regulation. This can also be done at the request of other EU institutions, member states, or citizens' initiatives.
Exemptions, exceptions, and defenses	Web browser providers defined as microenterprises and small enterprises (SMEs) by Article 2 of the Annex to Commission Recommendation 2003/361/EC are exempt from ensuring support and interoperability with QWACs. Similarly, SMEs are exempt from strong user authentication for online identification or for any reason such authentication is required by contractual obligation, including in the areas of transport, energy, banking, financial services, social security, health, drinking water, postal services, digital infrastructure, education, and telecommunications.

Cybersecurity Analysis (continued)

FACTORS	ANALYSIS
Enforcement mechanism	Regulatory authorities within each EU member state will be responsible for enforcing eIDAS 2.0. From the regulation text: > In order to ensure effective enforcement of this Regulation, a minimum for the maximum of administrative fines for both qualified and non-qualified trust service providers should be established. Member States should provide for effective, proportionate, and dissuasive penalties. When determining the penalties, the size of the affected entities, their business models and the severity of the infringements should be duly take into consideration. Further, eIDAS 2.0 allows member states to outsource enforcement via "mutual assistance" to the supervisory bodies of another member state "where the provider of the European Digital Identity Wallet or the trust service provider is established, where its network and information systems are located, or where its services are provided."

Recommendations

We put forth the following recommendations with the goal of reducing these risks.

SECTION AND SUMMARY	RECOMMENDATION(S)
Amend Article 45.2	The revised Article 45 mandates that web browsers accept government-approved QWACs issued by trust services providers. This means that even if a web browser vendor deems the QWACs' security inadequate, they must accept it. **Ensure that web browser vendors and their security experts drive the website authentication process—not the government.** Revise the language to ensure that web browser vendors can protect users' privacy and security. This will allow the market to decide whether a web browser vendor has earned consumer trust. Further, policymakers should encourage collaboration and knowledge sharing among web browser vendors, trust services providers, and other stakeholders in order to foster innovation while maintaining high security and interoperability standards.
Promote privacy-preserving technologies	Privacy-preserving technology (PPT) is essential to data privacy and security. As written, eIDAS 2.0 encourages PPT use in Section 14 of its recitals: "Member States should integrate different privacy-preserving technologies…" **Provide guidance, assistance, and incentives to drive PPT adoption, especially in the health and finance sectors.** Revise the language to promote PPT adoption, allowing EU citizens to safely and securely share their digital identities and highly sensitive information (e.g., health and finance data) with the private and public sectors.