AmCham EU
SPEAKING FOR AMERICAN BUSINESS IN EUROPE

Our position

Electronic identification scheme (eID) proposal

AmCham EU speaks for American companies committed to Europe on trade, investment and competitiveness issues. It aims to ensure a growth-orientated business and investment climate in Europe. AmCham EU facilitates the resolution of transatlantic issues that impact business and plays a role in creating better understanding of EU and US positions on business matters. Aggregate US investment in Europe totalled more than €3 trillion in 2020, directly supports more than 4.8 million jobs in Europe, and generates billions of euros annually in income, trade and research and development.

American Chamber of Commerce to the European Union
Speaking for American business in Europe

Avenue des Arts/Kunstlaan 53, 1000 Brussels, Belgium • **T** +32 2 513 68 92
info@amchameu.eu • amchameu.eu • European Transparency Register: 5265780509-97

Introduction

AmCham EU represents a broad variety of industries with first-hand experience in developing private digital wallets and using digital attributes to provide consumers with innovative services. The EU needs a common framework and technological architecture for a European Digital Identity wallet so that both citizens and businesses can prove identities and harness the benefits of boosted efficiencies, lower costs and a more favorable digital customer experience. Building on our existing knowledge around digital ID, AmCham EU members welcome the opportunity to inform the policy debate and help foster the development of a robust and practicable framework. We recommend that policymakers:

- Leverage the existing **international standards** as building blocks to foster harmonisation and interoperability between Member States.
- Establish a **stakeholder consultation process** to inform the development of the **'common toolbox'.**
- Develop digital solutions that are safe, user-friendly and convenient - readily encouraging user uptake and private sector involvement without resorting to a mandatory acceptance approach.
- Ensure a **high degree of data protection**, especially by limiting data collection to a minimum, avoiding intermediaries and giving individuals control over their data.
- Provide stakeholders with clarity and predictability on the **interplay with draft regulations, such as the Digital Markets Act (DMA), Revision of the Network Information Systems Directive (NIS2) and Cyber Security Act (CSA).**
- **Withdraw** proposals for **automatic recognition** by web-browsers of and interoperability with **Qualified Website Authentication Certificates.** The use of these attribute certificates may raise significant security, privacy and interoperability concerns for web browsers.

Building a harmonised approach relying on international standards

The EU needs a common framework and technological architecture for a European Digital Identity wallet so that both citizens and businesses can prove identities and harness the benefits of boosted efficiencies, lower costs and a more favorable digital customer experience. Despite the existing electronic identification and trust services (eIDAS) framework, national rules on provision of digital identity services remain fragmented or undeveloped across the EU. As policymakers consider their position on the eID review proposal, we strongly **encourage policymakers to adopt international standards, such as the International Organization for Standardization (ISO) 18013-5 (Mobile driving license [mDL]) and 23220 (eID),** as building blocks, where relevant, for the EU Digital Identity Framework and Toolbox. The building process should also engage in dialogue with all relevant stakeholders. Doing so would bring substantial benefits, including:

- **Harmonisation and acceptance**: ISO standards facilitate the establishment of a standardised identity payload for relying parties and ease the integration of digital identities issued by different Member States.
- **Avoid fragmentation in and between Member States**: The regulation should facilitate the development of eID systems that are applicable across Member States and avoid development of multiple and, possibly competing national eID systems. This also reduces burdens for private entities that have to ensure interoperability.

- **Identity proof and authentication**: ISO standards ensure that the EU meets sufficient levels of assurance to authenticate identities, enable proof of real identity and its ownership.

- **Governance and trust**: Standards also provide a process to authenticate relying parties, which fosters trust in the EU eID.

The current proposal can lead to a coordinated approach, through a common "toolbox" and by, relying on a technical architecture and reference framework, as well as a set of common standards, technical references, guidelines and best practices. Work is entrusted to national experts, members of the eIDAS expert group, who are expected to publish a draft by October 2022. At this point, it is still unclear how and when stakeholders will be consulted. **AmCham EU strongly recommends a more inclusive approach through regular consultations and expert input that can lead to structural cooperation.** The complexity and global reach of the proposal calls for a collaborative multi-stakeholder's approach. Several AmCham EU members have gained first-hand knowledge of how to develop and operate eID in an international context and are keen to further contribute to this debate.

When developing the Toolbox, the EU institutions should use an approach that balances various interests. Ongoing work should ensure that the proposed measures are proportionate, that they protect intellectual property rights, ensure robustness of authentication to avoid fraud and do not detrimentally affect privacy and security features and reduce competition or innovation.

Developing attractive solutions instead of requiring acceptance of EU digital identity wallets

AmCham EU's members believe in the creation of a European model which is proportionate, equitable, risk-based, scalable and would encourage the use of identity solutions in appropriate circumstances. The Commission's proposal pushes for a broad application and mandatory acceptance of EU Digital Wallet where strong user authentication is required and for all Very Large Online Platforms. VLOPs under the Digital Services Act (DSA) is a specific category of services defined by reference to asymmetric risks around illegal content. It is wholly inappropriate to then transpose this to a category where "must carry" obligations are being proposed as if these are regulated utilities. We support the wider use and acceptance of EU Digital Identity Wallets of digital ID services in various sectors (eg, transportation, energy, and financial services, etc) and EU Digital Identity Wallets. However, as currently drafted, the Commission's proposal risks to requiring organisations that operate in the EU to integrate with and provide ongoing support for EU Digital Identity Wallets across all Member States raises significant concerns for the private sector. Firstly, the proposed requirements would impede the use of alternative solutions– and may even deter some (including smaller companies) from developing innovative products in this space. Secondly, under Article 6b companies will be made to assume responsibility for the use of any authentication systems, even though the Commission has obligated them to offer such systems. The Commission and member states must ensure that any eID system in use meets robust authentication criteria. **We believe that the proposal should be amended to ensure that private relying parties are not required to accept EU Digital Identity Wallets given the concerns described**. Instead, the European Institutions should encourage Member States to offer digital ID solutions that are safe, user-friendly and convenient – making them attractive for users and the private sector service or product providers.

Ensuring data protection

Consumers must be able to trust that their personal information is safe, secure, and protected., this is key to achieve the digital transformation of our society and economy. More than ever trust is required to deepen the use of digital tools and services. Based on our experience in Europe and beyond, we recommend the following key principles to be promoted in the context of the current proposal:

- **Limit data collection to a minimum**: In line with the General Data Protection Regulation (GDPR), do not allow third parties to collect or access to data that would not have been gathered beyond what is necessary for service delivery and in line with the GDPR.
- **Ensure a targeted approach to specific needs**: For example, if a particular service requires the relying party to verify that a user is over the age of 18, only that piece of identity data should be shared, rather than any additional identity elements such as the user's date of birth.
- **Avoid mandated intermediaries** between data collection and the relevant relying party. Identity data should only be shared directly between the user's electronic device and the relevant relying party.
- Given that ID verification can reveal sensitive information, the individual **should be entitled to have control over their data.**

The draft proposal should further **clarify how it will comply with the GDPR and how it will ensure the protection of identity data,** including access from third-parties**.**

Fostering consistency with the broader regulatory landscape

The eID proposal interplays and builds upon pieces of regulation that are currently being discussed by the co-legislators. It is, thus, critical to provide stakeholders with regulatory predictability and transparency.

Digital Markets Act (DMA): The Commission has proposed that the EU Digital Identity Framework builds on the DMA to ensure that business users and providers of ancillary services have access to certain hardware and software features and that they interoperate with them through the EU Digital Identity Wallets or the Member States' notified electronic identification means. The Digital Markets Act Proposal is still being reviewed by the co-legislators and has yet to be adopted. At this point, it would be premature to anticipate interpretation and application of draft provisions.

Network and Information Security Directive (NIS) and Cyber Security Act (CSA): The proposal rightfully refers to the revised NIS Directive (NIS2) and CSA on several occasions. We propose to further clarify the roles and coordination between the (national) competent authorities responsible for complying with NIS2 and the revised E-IDAS. Regarding the references made to the Cybersecurity Act and certifications, we invite the Commission to clarify its intentions regarding future certifications under the CSA, as the current Union Rolling Work Programme has not identified a scheme for trust services to be developed by the European Union Agency for Cybersecurity (ENISA).

Safeguarding security, privacy and interoperability of web browsers

The legislative proposal touches upon website certificates which play a critical role in allowing encryption and privacy on websites. To operate, website authentication relies on a digital certificate, a document that links the website server's name to a unique cryptographic key. In 2014, the eIDAS regulation established a parallel framework for website certificates and authentication, known as Qualified Website Authentication Certificates (QWACs). The use of these attribute certificates may raise significant security, privacy and interoperability concerns for web browsers. It also creates a problematic global precedent that eliminates the ability of browsers to repel malicious attacks. Consequently, we encourage the European Institutions to **withdraw these proposals for automatic recognition of and interoperability with Qualified Website Authentication Certificates by web-browsers.**

Recognition of commercial documentation in electronic format

The eID proposal builds on the eIDAS Regulation which is in itself a further evolution of the E-Signature Directive of 2002.

While much of the focus of the use of the proposal is on EU Digital Identity Wallets, it also relates to the recognition of documents in electronic form for legal purposes. Articles 25 and Article 46 of the eIDAS Regulation explicitly state that digital documents should have equal legal status. This mirrors Article 25 relating to electronic signatures, which has been successful in legitimising electronic signatures. However, in relation to electronic documents, a survey of key EU jurisdictions has shown that Article 46 has been ineffective in giving legal validity to digital instruments. Equally, Article 25 of the eIDAS Regulation provides for non-discrimination of e-signatures, but only where a digital document is already recognised as a legal document.