EU digital identity framework: supporting wide uptake for boosting the European digital economy

Mastercard fully supports the objective of a harmonized, interoperable and secure European Digital Identity Wallet (EUDIW). The revised eIDAS Regulation (eIDAS2) is a major step towards creating a digital identity ecosystem that will be a crucial pillar for boosting the European digital economy. As digitalization progresses, ensuring trust among parties will be a key enabling factor for further growth and innovation. This can be supported by a European digital identity wallet that ensures privacy, stability, and security.

As the process for eIDAS2 now moves towards the implementation aspects, Mastercard would like to highlight some important elements that will help to ensure a more rapid roll-out and maximize adoption and acceptance EU-wide and help drive a secure, user-centric and efficient solution. Our aim is to help the EU to realise the economic and social benefits flowing from an effective digital identity ecosystem.

Our key recommendations

1. Enable EUDIW for most used payment methods to combine digital identity with payments and enable innovation.

2. Create a wide acceptance network through industry standards to ensure a cost effective and fast market roll-out.

3. Support age verification as a priority use case to improve the safety of minors in the digital environment.

4. Ensure trust through secure digital identity wallets with the help of industry fraud prevention tools.

Enable EUDI wallets for most used payment methods

Mastercard has been a trailblazer in adopting and scaling technologies to make digital payments more accessible, interoperable and secure. We see EUDI wallets as a next step in this journey and want to ensure that all EU users haven open and free access to their preferred methods for making payments, in person as well as remote.

We are closely following the Large-Scale Pilots (LSP) projects, such as NOBID & EWC and the testing of embedding payment credentials within the wallet. We are also engaging with existing national wallet initiatives, such as mObywatel and others, to explore opportunities to combine digital identity with payment functionalities. We would expect a natural evolution where existing and emerging wallet solutions increasingly combine identity and payment functionalities. EUDI wallets should provide free and open access to all payment functionalities that have user demand. Across Europe, card-based payment credentials and their digital form factors have emerged as one of the most common payment methods for both in-store and e-commerce. Next to these, also innovative payment methods such as open banking / open finance, CBDC, account-to-account and person-to-person payments could be supported in the wallet.

Create a wide acceptance network through industry standards

Building a comprehensive acceptance network and supporting an easy and seamless acceptance process for entities will be a key element of the success of eIDAS2. We believe in scalable solutions based on industry standards that will facilitate the exchange of identity information and data points between relying parties and attribute providers. Leveraging existing trusted infrastructures and standards that have already been put in place at scale, such as solutions for authentication that are delivered via global industry standards, could considerably help in creating the needed wide acceptance network for EUDIW. Building a new acceptance infrastructure for EUDIW from scratch would be very costly and time-consuming.

Attribute providers will connect to relying parties, who are likely to prefer one common standard for the acceptance of EUDIW. Having to agree with providers separately would considerably slow down implementation and adoption. Allowing the use of existing industry standards such as the EMVCo 3DS or the FIDO Alliance passkeys already used for payment and non-payment authentication is needed to ensure a seamless user experience for those verifying identities and users of the EUDIW. EMV is an open standard for globally interoperable, secure payments. It promotes a widespread adoption and access to a seamless and secure online attribute verification, while offering at the same time a cost-effective and fast to-market delivery of data surrounding identity attribute in authentication message flows. In the EU there is already a wide acceptance network for EMVCo 3DS due to the Strong Customer Authentication (SCA) requirements of the second Payment Services Directive (PSD2). All merchants, issuers and their providers in the EEA and the UK, as well as payment schemes support SCA requirements for secure online purchases. As online users are used to authenticating payments in their everyday life, there is no behavioral change necessary to deliver identity attribute assurance through authentication capabilities. Existing national eID schemes (e.g. Itsme in Belgium, BankID in Sweden and MitID in Denmark) are already connected to EMV 3DS for strong customer authentication, making the technology business as usual. Further, EEA citizens travelling to other regions will benefit from the same services with the same experience as the EMVCo 3DS is global.

Consequently, the EMVCo 3DS is a reality, already works at scale and is flexible to support more data points. The footprint of SCA and EMV 3DS in Europe suggest that EUDIW should leverage this highly scaled ecosystem to provided authentication services and identity attribute verification services (see below).

Complementary to the EMVCo 3DS standard are the FIDO Alliance passkey standards, allowing the use of on-device authentication technology (such as fingerprint recognition or facial scanning) for SCA. This widely used industry standard allows to securely confirm possession and inherence/knowledge without the need to connect to the identity provider for every authentication event.

Support age verification as a priority use case

Protecting children when accessing internet or mobile applications is rightly a priority for regulators across Europe. The protection of minors is also part of our corporate social responsibility goals, and we share the urgent need to develop solutions that aim to improve the safety of minors in the digital environment. For this, digital age verification solutions are needed and should be a priority use case for eIDAS2 implementation.

Leveraging existing authentication capabilities, as outlined in the above section, would also greatly help in a timely and efficient way of achieving this simple but key use case of age verification. Supporting age verification on existing rails would allow the timely availability of end solutions to customers with minimal effort and the readiness to connect to future EUDI infrastructures.

To support the development of age verification, the EMVCo 3DS standard has been adapted to support age but also further attributes to be returned by the issuer to the merchant, based on information held by the issuer that will have been validated by the issuer under KYC / AML regulations when the account was opened. Up until now, 23 identity attributes (including but not limited to age, date of birth, citizenship and ID number) are supported by the EMV 3DS standard, which is publicly available. The use of EMVCo 3DS standard would allow for these attributes held in the EUDIW to be shared with the relying party, with the consent of the Data Subject, over the EMV 3DS rails.

Mastercard abides by the Data Privacy by Design principles, including data minimization, anonymization and proportionality. Data minimization ensures the response is "person is over X years old" instead of the actual date of birth or age.

Ensure trust through secure digital identity wallets

With the expected storage of significant amount of Personal Identifiable Information in the EUDIW, ensuring the highest security standards is essential to prevent account takeovers and compromises. Protecting this new digital identity infrastructure, especially ID wallets, is critical. Given that these wallets will store sensitive personal information, they are likely to become prime targets for criminals.

To build a secure EUDIW infrastructure, we recommend leveraging current industry fraud prevention tools for both wallet enrollment and daily usage. As fraud and data breaches increase, it is vital for wallet providers to conduct comprehensive risk assessments using personal data (e.g., name, address, email, phone number), device data, and behavioral biometrics to detect anomalies in user applications. Existing tools can mitigate enrollment risks by validating user-provided data, which is crucial when government documents like passports or driver's licenses are not uploaded and validated during enrollment. These industry solutions can also prevent unauthorised changes to applications, even in tamper-resistant sections of a phone. Many solutions include behavioral biometric features that analyse device usage patterns (e.g., typing speed, orientation, pages visited) to assess risk and to confirm the user's authenticity. This is especially valuable for detecting compromised login credentials, providing an "invisible" layer of risk and fraud prevention. These tools should be standard for all users leveraging the EUDIW to ensure robust security across all use cases.