THE PAYPERS

Insights into Payments and Beyond

Financial Crime and Fraud Report 2022

Best Practices into Fraud and Risk Management

Endorsement partners: consult hyperion securing tomorrow's transactions; FINTECH FINCRIME EXCHANGE; FINTRAIL; kuppingercole ANALYSTS

Key media partners: IDENTITYWEEK; Liminal; RiskConnect VIRTUAL; transform finance; QUBE

SGM Consulting & Quali-Sign

Securing Digital Payments with Identity Wallets

Stéphane Mouy is a financial services consultant focusing on regulatory aspects of the digital transition. He is also a member of the eWallet Network gathering European experts in digital identity and payment-enabling wallets.

Stéphane Mouy ▪ *Senior Consultant* ▪ SGM Consulting

Michael Adams is a payments consultant at Quali-Sign, focusing on regulatory aspects of the digital transition. He is also a member of the eWallet Network gathering European experts in digital identity and payment-enabling wallets.

Michael Adams ▪ *Payments Consultant* ▪ Quali-Sign

Digital identity wallets, expected to play a major role in digital interactions in the coming years, are now well documented, especially with the driving licence or state ID mobile wallet project in the USA and, in the EU, the eIDAS 2.0 proposal centred around European Digital Identity (EUDI) wallets. Less well known is the impact these could have on payment methods, especially as an alternative to cash which is in structural decline for day-to-day payments. Could digital identity wallets leverage their high level of assurance and trusted environment into the payment area and foster a more competitive and fraud-proof environment?

The debate is now open in the EU with the eIDAS 2.0 proposal requiring large online platforms and major service providers to accept EUDI wallets, including banks and financial service providers who will therefore rely on the high level of assurance offered by EUDI wallets for onboarding processes. These will also be deemed to meet applicable Customer Due Diligence requirements under applicable AML/CFT rules, as would be expected from a multi-purpose high-quality digital identity wallet under the control of its user. The eIDAS 2.0 proposal also mandates that EUDI wallets support offline connectivity and comply with Strong Customer Authentication (SCA) requirements applicable in banking and financial matters, therefore enabling the payment use case of digital identity wallets and facilitating payment authentication with a high degree of security. Whilst much work remains to be done before this becomes a reality, the trend nevertheless illustrates a tectonic shift in digital interactions where high-quality identity and payment attributes are combined to offer a value-added and secure experience to customers.

Mutual authentication – the key to trustworthiness and interoperability

Digital identity wallets are inherently multi-purpose and meant to offer interoperability, i.e. connect with different service providers, not just those affiliated to, or members of, a given identity network or scheme. Users must be able to interact securely with other user wallets and different terminals from different relying parties. However, interoperability also implies that data exchanges are expected to be made with third parties that are not immediately recognisable or known to the wallet user and cannot be assumed by him/her to be trusted. This has structural implications:

- Interacting with relying parties where identity or other attributes/credentials are to be exchanged must imply a two-way authentication (ie, of the relying party by the wallet user and of the wallet user by the relying party) so that each party can satisfy itself that it is dealing with the right person or organisation. If this is not done, users risk passing sensitive personal data to malevolent actors; →

- In addition, the authentication process can – indeed should – meet strong two-factor requirements to guarantee the trustworthiness of the identities of the wallet user and relying party;
- Last but not least, this applies irrespective of whether the interaction occurs online or offline, ie, when a proximity connection (QR code, BLE, or NFC) is used between the mobile phone and merchant terminal.

The two-way authentication procedure that is a prerequisite for wallet-based payments also brings added security benefits. Instead of a payment transaction containing payee and payer IBANs, it can contain a variety of bank-issued attribute attestations representing both the payee and payer account and, for example, the payee name displayed to the payer during the dynamic linking procedure. In addition, the payment transaction can be electronically signed by both the payee and payer, therefore offering a new level of security and legal robustness to payment interactions.

Combining identity and payment attribute attestations for value-added secure interactions

The use of identity attributes in payment-related environments is not new and already embedded in PSD2 requirements, especially for 'dynamic linking' where the amount and name of the payee are required to be provided.

Beyond these core use cases, there are countless other interactions where identity or status attributes are required to be communicated together, therefore opening a clear path towards the deployment of digital identity wallets with enhanced payment functionalities. Let's just give two examples:

- A person purchases cigarettes or alcohol at a vending machine. He/she uses his/her EUDI wallet to perform SCA and supply both his/her IBAN Account attribute and proof of age attribute within the signed package; and
- A person signs up for a utility contract. Using his/her EUDI wallet, he/she signs the terms and conditions and performs SCA on a Direct Debit mandate at the same time, supplying the IBANaccount details and proof of address.

Secure offline connectivity – why it matters, also for Central Bank Digital Currencies

Enabling secure digital interactions is indeed essential for payments to prevent fraud but must also support both online and offline modes, given that internet connectivity is not always available and many of today's payment solutions already support offline interactions. This is for example the case for point-of-sale interactions with payment cards or some GAFAM-pay solutions that use NFC communication protocols for interactions with payment terminals.

But this is also to be the case for Central Bank Digital Currencies (CBDCs) aiming to digitise cash transactions which today can be successfully completed with irrevocability and finality whilst both parties are offline – a factor, together with full anonymity, contributing to the enduring appeal of cash. Whilst many aspects of retail CBDCs remain to be specified, anti-money-laundering requirements will apply and lead to identity checks being performed, which can only occur offline when robust wallet-based identity attributes are exchanged with payment instructions, leaving digital identity wallets as prime candidates to act as CBDC wallets.