Digital Identity Wallets

Why the Offline Mode *Really* Matters

Offline mode support, often overlooked as a remote need for digital interactions, is critical for digital identity wallets, especially for payment and CBDC purposes

Michael Adams (Quali-Sign) & Stéphane Mouy (SGM Consulting)

Readers will likely concur with the view that digital identity wallets (DIWs) on mobile phones are soon to become a central element of our digital lives. Indeed, they will allow users to share identity and other attributes with third-party relying parties in order to access online services whilst keeping control over the use of their data. In the EU, the proposed eIDAS 2.0 draft defines European digital identity wallets as multi-purpose wallets, required to be accepted by most public as well as private service providers (including, notably, banking and financial services) and 'very large online platforms' (i.e., GAFAM & BATX).

DIWs allow users to connect to online services as well as authenticate themselves securely, but a poorly understood, yet critical aspect of DIWs is whether they can/should support the offline mode, i.e., the situation where the wallet user lacks internet access.

What is the offline mode?

Digital Wallet
123 456
123 456

An example of offline/online connectivity using NFC

The offline mode usually refers to the situation where the smartphone of the user has no internet connectivity when it needs to interact with the service provider terminal in order to access the required service. A critical consequence is that the data exchange between the user's smartphone and the service provider's terminal cannot take place online and must therefore occur via an offline technology, such as BLE, NFC or QR code scanning or, more likely, a combination of these technologies.

This is very far from an unusual situation. It happens for example with current Covid Health passes, where the wallet user displays a QR code, which is then read by the service provider's terminal and does not imply that the wallet user should have full (or even limited) internet connectivity. Another example in the payment area is when a bank card is presented to the merchant's terminal and exchanges data via an NFC protocol. The card obviously has no dedicated internet access but is nevertheless able to exchange data securely with the merchant's terminal. The same applies for GAFA-pay solutions. For example, making a payment using Apple-Pay does not require the mobile having an internet connection.

The most likely offline use case is 'offline/online connectivity'. This is the situation when the wallet user does not have internet connectivity, but the service provider terminal does (see picture above). A rarer case is 'offline/offline connectivity' or 'full offline'. This situation exists when neither party has internet connectivity when the need to exchange data arises. We will see that this latter use case is likely to be relevant and indeed critical for CBDCs.

Why is the offline mode relevant?

The simple answer is that, well, we live in an imperfect digital world, a situation likely to continue in the foreseeable future. There are indeed many situations where internet connectivity is limited or disrupted and where assuming full internet connectivity for data exchanges between the user's smartphone and the service provider's terminal is unrealistic.

A typical example is for (rural) areas with poor internet and/or cellular coverage (wireless dead zones), where citizens often experience structural digital integration problems. Even in areas where coverage is good, there are many places where internet access is not available – for example in basement or underground premises. Last but certainly not least, major event situations with temporary mass gatherings of people often lead to internet connectivity failures which rapidly become critical when this is required for access to premises.

Internet access is often too unreliable to be taken for granted in mutual interactions and relying on offline communication modes is therefore a choice of reason. This approach is for example reflected in the eIDAS 2.0 proposal defining European digital identity wallets as "*a product and service that allows the user to store identity data, credentials and attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, **online and offline**, for a service […]*" (emphasis added).

Acceptance of the DIW by the user community will imply that the DIW 'always works'. If it lets them down, then they will not use it again. An offline capability not only protects the user against a failure of network connectivity, but also against central server failures.

Interoperability implies a 'zero trust by default' approach – i.e., identity verification for every party

DIWs are meant to offer interoperability, i.e., the ability to use different wallets and to connect with different service providers, not just those affiliated to, or members of, a given identity network or scheme. This means that different users from different countries and having different wallets must be able to interact successfully 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:

- Every interaction with a relying party where identity or other attributes/credentials are to be exchanged must imply a two-way authentication (i.e., of the relying party by the wallet user and of the wallet user by the relying party) so that both parties can satisfy themselves that they are dealing with the right person or organisation. If this is not done users risk passing their sensitive personal data to unknown malevolent parties;

- In addition, the authentication process can (indeed should) meet strong (two-factor) requirements in order to guarantee the trustworthiness of the identities of the wallet user and relying party;
- This must apply irrespective of whether the interaction between them occurs online or offline.

Only by building these safeguards into the system can we meet the users' demands for their privacy to be respected. We should also note that these safeguards are equally important whether online or offline.

To meet this requirement each user must be able to authenticate the other party even whilst offline. In addition to local connectivity (e.g., QR codes and BLE) this requires the chains of trust for both parties to be held locally. We explain how this can be achieved in the next section.

Ensuring secure offline connectivity is both possible and practical

The offline mode, whilst recognised as desirable, is at times viewed as complex and/or onerous to implement, leading to attempts to limit its use for DIWs. In our view, this position is wholly misplaced and not grounded in reality. Indeed mature, open and readily deployable technologies exist today that can be used securely and effectively to achieve valid online as well as offline interactions between the wallet user and service provider/relying party.

This is particularly the case when using X509 digital certificates and electronic signature standards (notably ETSI 319 411-2 for qualified certificates). These support online as well as offline interactions, allowing in both cases full root-of-trust verification. It is a proven fact that it is today possible for digital identity wallets to provide efficient, secure data exchanges with third parties through advanced (or qualified[1]) electronic signatures supported by qualified certificates. This allows instant root-of-trust verification of both parties' identities, irrespective of whether the data exchange occurs in online or offline mode[2]. In addition, electronic signature standards allow 'mutual approval' or 'counter-signing', a key solution when ensuring and recording the parties' agreement on terms of engagement is needed, as is obviously the case for payments.

Payment-related interactions are critically dependent on secure offline communications

If there is one area where having secure and robust data interactions is essential and where the offline mode is also a prerequisite, it is for payments. Security hardly needs debating given the compelling need to prevent fraud in payments but being robust is also of critical importance given that 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 Apple-pay. Both use NFC communication protocols for interactions with payment terminals. In this context, a DIW that does not support the offline mode cannot, for practical purposes, be meaningfully considered for payment purposes and is therefore of limited value for banking and financial services.

[1] Qualified electronic signature status is dependent upon smartphones being recognised as QSCDs, a process likely to be implemented in conjunction with the eIDAS 2.0 implementation.

[2] There is one difference between online and offline interactions in that offline interactions cannot confirm that the other party's digital certificate has been revoked when the party is offline.

The use of strong cryptographic solutions coupled with dedicated wallet identity certificates[2] allows the secure exchange of information between wallet users and relying parties through advanced/qualified electronic signature interactions always meeting strong customer authentication requirements, therefore offering improved security and reliability for both online and offline interactions.

The eIDAS 2.0 proposal has this in mind when mandating DIWs supporting the offline mode *and* being accepted by private sector relying parties whenever strong customer authentication is required for banking and financial services.

The use of electronic signature standards also supports the counter-signing of payment messages, therefore allowing the full deployment, online and offline, of e-signed 'request-to-pay' messages issued by merchants (payees) and counter-e-signed by wallet users (payers) that can then be processed in accordance with the relevant payment scheme rules. Note that this mutual-approval functionality is not currently available with W3C specifications – which in any event do not support offline interactions.

Offline support is a defining test for Central Bank Digital Currency (CBDC) interactions

A key aim of retail CBDCs is to digitize cash and cash transactions can be successfully completed *with irrevocability and finality* whilst both parties are offline – a factor, together with full anonymity, no doubt contributing to the enduring appeal of cash today. Although many features of retail CBDCs remain to be specified, it is likely that users will use CBDCs with a wallet app that will also allow the exchange of identity attributes, leaving DIWs as prime candidates to act as CBDC wallets – in fact these will be viewed as enhanced DIWs. In order to emulate cash transactions, CBDC wallets must support the offline mode, i.e. have the ability to both receive and later re-spend the value received, all before going back online. (Note: CBDC transactions would of course also work when one or both parties are online.) In addition, it is equally clear that CBDC transactions must meet the stringent demands for security and the ability for each party to authenticate each other as described above.

The combination of these requirements can be regarded as even more demanding than the payments' transactions described above. The ability to achieve irrevocability and finality and re-spend value whilst offline represents additional requirements to those of payments.

To summarize…

- Digital Identity Wallets are meant to offer interoperability, i.e. the ability for different users to use different wallets and to connect with other user wallets as well as multiple service providers, not just those affiliated to, or members of, a given identity network or scheme.
- A Digital Identity Wallet needs to operate successfully (i) whilst both parties are online, (ii) whilst the Relying Party terminal is online and the wallet is offline – 'online/offline' and (iii) whilst the Relying Party terminal is offline and the wallet is offline – 'offline/offline'.
- Building an interoperable Digital Identity Wallet based upon established e-sign standards (i) is achievable (ii) offers interactions based upon advanced/qualified e-signatures and (iii) complies with strong customer authentication requirements. It uses X509 digital certificates and electronic signature standards (notably ETSI 319 411-2 for qualified certificates). It can be demonstrated as working today.

[3] The wallet identity certificate contains a public key, the corresponding private key of which is located in the secure element of the smartphone, with strong protection from tampering.

- Meeting interoperability requirements requires trust to be established between both parties participating in the transaction, regardless of whether the procedure takes place online or offline. In the absence of trust, we are inevitably left with a 'Closed Garden' approach where only 'approved members' are allowed to take part, as favoured for example by GAFAM as the only alternative.

- In the future, CBDC developments will further reinforce the need to support both interoperability and offline environments.

Sharing technical, regulatory and business expertise for multipurpose eWallets

eWALLET NETWORK

Quali-Sign
Mobile apps for eID & SCA

SGM CONSULTING
Digital transition expertise for financial services

Michael Adams

Michael_adams@quali-sign.com

Stéphane Mouy

sgmouy@sgmconsultingservices.com