STRONG AUTHENTICATION

THE eIDAS2 REGULATION HERALDS IDENTITY-BASED PAYMENTS

Michael ADAMS

Quali-Sign
Mobile apps for eID & SCA

Stéphane MOUY

SGM CONSULTING
Digital transition expertise
for financial services

While the convergence of identity and payment in mobile applications now appears to be a major structural development, the pace of its deployment is still uncertain. The recently adopted eIDAS2 regulation could well herald an innovative evolution for merchants and digital identity wallet users alike through a new authentication approach that will be mandatory for banks.

We all know the importance of strong authentication in digital payments since the introduction of the 2nd Payment Services Directive (PSD2), which is now firmly established in the practices of payment service providers. This is a role with major legal consequences, since the absence of strong authentication when it is required prevents the payment service provider from validly opposing the payer's request for reimbursement of the payment, except in cases of proven fraud of the payer.

This welcome development is taking place against a backdrop renewed by the increase of Authorised Push Payment (APP) fraud on the Internet, which have circumvented the obstacle of strong authentication by developing scenarios for manipulating the payer to validate a payment that he would not have authorised with full knowledge of the facts. In this context, it is clearly necessary to ensure that the payer is properly informed about the payment he is about to validate, particularly with regard to the real identity of the payment beneficiary.

Checking the identity of the parties to the payment therefore plays a major role in securing payments, and while this is not new, it is being reinforced by the regulatory verification of payee requirement for instant payments but also the roll-out of European digital identity wallets announced for the end of 2026 under the new eIDAS2 regulation. As we know, these eIDAS2 wallets will ensure the secure storage of certified identity and status attributes of their user and will have to be accepted by service providers by the end of 2027.

And since wallets are already used on a massive scale to store and manage means of payment through X-pay type applications (Apple Pay, Samsung Pay, Google Wallet to name a few), the convergence of identity, status and payment attributes within mobile applications appears to be a structural development likely to profoundly transform retail payment practices. The time will soon come for digital interactions combining various attributes presented and/or requested by the payment recipient and validated by the wallet user for transmission and implementation by payment service providers.

How soon? Within a short- or medium-term horizon? Nobody really knows, because while the prospect is very real, the path to achieving it has not yet been written. Let's be clear, we believe that this development is both desirable and necessary, and that it would benefit from being anticipated, as a lack of preparation could lead some payment service providers to experience it as a constraint over which they will have no control. The role played by Apple in digital identity in the United States (via the mDL - mobile driving licence - application and the ISO 18013-5 standard) and, closer to home, Mastercard's positioning as a major supplier of digital identity should be seen in the light of these developments.

A significant factor in this development is likely to be the role played by eIDAS2 wallets in strong authentication of payments. Let us explain.

Redirection or embedded Strong authentication?

The strong authentication required by PSD2 and its implementing regulation is currently largely based on redirection schemes to the payment service provider holding the payer's account. When it is applied - and it should be remembered that it is not always required and that the methods used can vary, in particular to include a 'dynamic link' with the payment transaction in question by displaying the amount and the beneficiary of the payment - the payer is redirected to the environment of his bank, usually his mobile banking application, who is responsible for organising the strong authentication using digital procedures that he will have defined and validated.

This so-called redirection scheme, which is currently the predominant way of implementing strong authentication, is logical when strong authentication is seen as the responsibility of account-holding institutions, which is precisely the approach of PSD2 and, to date, of the draft Payment Services Regulation (PSR). Under this approach, the account-holding institution defines the procedures for implementing strong authentication as well as those relating to the expression of its customers' consent to payments - two distinct but closely related subjects, since strong authentication is used in practice to ensure that the legitimate account holder is indeed the one who has acted remotely to authorise the payment.

And since it defines the procedures, these are also binding on Third Party Service Providers, particularly payment initiation service providers, who have often advocated an alternative strong authentication scheme known as 'embedded', whereby the strong authentication proof is directly integrated into the message transmitted by the payment initiation service provider to the payer's account-holding institution, and therefore strong authentication takes place upstream of the latter's intervention.

This position, which puts banks in a privileged position with regard to the methods of implementing strong authentication, is logical in the light of the provisions of PSD2 and its implementing regulation, and was validated by the European Banking Authority in 2020. The EBA stated that banks are not required to implement on-board strong authentication when they do not make it available to their own customers.

This situation is to be regretted, as the embedded authentication is a source of innovation and increased security for payments, particularly because it offers greater flexibility in the management of payment data and enables more competition between payment means as well as the introduction of new value-added services. Finally, it enables the widespread use of the dynamic link, which is a powerful tool in the fight against new forms of fraud.

Things would no doubt remain as they are with the future PSR - the current project is in line with the PSD2 in this respect - were it not for a new element that has reshuffled the cards, namely the eIDAS2 regulation, which has just been adopted and stipulates that digital identity wallets will provide the strong authentication required for payments if their users wish to use them for this purpose. This strong authentication will then be mandatory for payment service providers and cannot be refused by them or made conditional on the implementation of additional measures.

The eIDAS wallet strong authentication: a change of perspective

In the eIDAS2 approach, strong authentication is no longer a functionality implemented by financial intermediaries for their customers' payments, but a legally recognised mechanism provided by approved digital applications meeting the requirements of the high Level of Assurance and benefiting from a specific liability regime stemming from the eIDAS regulation. The change of perspective from the PSD2 approach is structural as the strong authentication of eIDAS wallets is a legally autonomous mechanism which cannot be seen as a task contractually outsourced by the payer's bank- unlike what the draft regulation on payment services envisages for X-pay wallets (pass-through wallets). This is welcome.

Let's take the example of payments conditional on proof of age, a situation typical of online betting but also of car hire and many other uses. Rather than having to manage the setting up of the service and then its payment separately, it will be possible, via an on-board strong authentication mechanism, to associate directly with the payment authorisation message one (or more) identity or status attributes requested by the service provider and available on the consumer's wallet, such as proof of age, residence or eligibility for a price reduction. Ultimately, this change will result in better services for merchants, particularly for reconciling payment flows with accounting data, and more secure and flexible interactions.

Full-function eIDAS2 wallets for payments

Although the eIDAS2 regulation defines the role of wallets in strong authentication processes, it says no more about it and is not intended to do so for payments, which opens up two possible options.

A first minimal approach option would be to limit the role of wallets to the strong authentication of payments provided for in the eIDAS2 regulation, on the understanding that the means of payment remain stored and managed by another mobile application (an X-pay wallet or a banking application) a situation bearing resemblance with what is today the case for the ITSME digital identity application used in Belgium for payment validation. This is certainly possible, but this does not capture the full potential of eIDAS2 wallets, it has the disadvantage of degrading the user experience by causing significant friction - or even making it impossible to implement in offline interactions. We believe its prospects are therefore limited.

A second approach, which we recommend, is to take advantage of the fact that eIDAS2 wallets are intended to store and manage electronic credentials and to give them a full role in payments by entrusting them with the management of means of payment in addition to strong authentication. This approach is fully in line with the eIDAS2 regulation and its ambitions for payments.

How can we best support such a development?

The first step would be to resolve the drafting discrepancy between the eIDAS Regulation and the draft PSR prepared without taking into account the role of digital identity wallets in payments. By way of illustration, we might mention the fact that the draft PSR gives in practice an exclusive role to the payer's account service provider in defining the procedures for the payer's consent to payment without mentioning digital identity wallets on this point. It is hard to see how this authorisation topic can be dissociated from strong authentication, which in practice aims to guarantee that the legitimate holder of the debited account is indeed the person who approved the payment and not a third party. The logical thing to do would be to say that when the eIDAS2 wallet used for the management of strong authentication, which is now enshrined in the eIDAS2 regulation, the payer consent procedure should be subordinate to it- which is covered by the draft regulation on payment services.

The second is to clarify the liability regime for account-holding service providers under PSD2 and the future PSR, which the eIDAS2 regulation is clearly not intended to overturn, just as it is not intended to redefine the cases in which strong authentication applies. However, a harmonious relationship between the two texts seems possible: payment service providers remain "legally responsible" for strong authentication in payments under the conditions defined by the PSD and the future PSR, but when an eIDAS2 wallet is used, their role is no longer to implement it but simply to verify that it has been used.

This clarification will undoubtedly be part of the future implementing regulation based on the technical regulatory standards that the European Banking Authority will be responsible for drawing up in application of the PSR, in particular for the purpose of taking eIDAS2 wallets into account. However, it assumes that the strong authentication of eIDAS2 wallets offers a robust, simple and practical verification mechanism. By happy coincidence, this is precisely the case for the electronic signature, which is included in the specifications for eIDAS2 wallets.

Electronic signatures - a critical tool for securing strong authentication

The electronic signature offers many advantages for digital payments, combining robustness and flexibility of use in a mechanism ideally suited to the wallet user's decisions to ensure the irrevocability of payments. Because it uses secure cryptographic processes, it offers an excellent level of protection against fraud and natively involves strong authentication. In addition, it offers great flexibility of use, applying not only to the payment message but also to the various attributes that may accompany it - such as IBAN or other payment credentials - while supporting both online and offline modes, when the payer's wallet interacts with the merchant's terminal via NFC or another proximity protocol. Finally, the icing on the cake is that it is well suited to the dynamic linking requirement, which shares many of its characteristics.

But what truly distinguishes the electronic signature from the other technical specifications considered for eIDAS2 wallets is the existence of a proof file that incorporates the signed message indicating "who did what", verifiable by any person and usable in legal proceedings. And when the signature is based on a qualified certificate ensuring the identity of the signatory - which is recommended - the level of assurance offered by the electronic signature is clearly superior to current practices in terms of strong authentication.

As we can see, the use of electronic signatures for strong authentication of eIDAS2 wallets offers a robust and easily verifiable authentication mechanism for payment service providers, enabling them to manage their responsibilities under PSD2 in a straightforward manner. And in the highly unlikely event of a technical failure of this authentication, they will also be able to activate the remedies provided for in the eIDAS regulation against the wallet provider, the manager of the authentication mechanism, or even the State sponsoring the wallet.

The eIDAS trust environment, a key asset to be leveraged for payments

Awareness of the need for a European payments infrastructure is a recent development - all the more so as card payment systems, managed by non-European operators, now play a dominant role in the retail payments ecosystem in Europe, as the Paris Olympics were the latest remarkable illustration. This situation accentuates the structural dependence of payment service providers on the VISA/Mastercard duopoly and poses a major pricing problem for merchants and retailers, as the British Payment System Regulator rightly pointed out in its report of May 2024, when it reported that fees had risen sharply without any real correlation with the services provided.

It is hard to see what will change this situation in the years to come, other than more competition between payment means, especially at point of sale, and the introduction of new payment services combining identity, status and payment attributes, which will in any case require an appropriate payment infrastructure. A first approach could be to adapt the EMVCo specifications deployed by the card networks and currently very dominant, at the risk however of increasing the dependence of players in the payment ecosystem on these specifications.

Another method, which we prefer, would be to build on the eIDAS environment and develop for digital identity wallets a strong authentication scheme based on an open banking API that would no longer be conditional on the banks' agreement (which was the PSD2 approach) but would be mandatory for them (which is the eIDAS2 approach).

The eIDAS2 regulation can also be a powerful vector for modernising payments in Europe. In fact, one of the major contributions of the eIDAS regulation, which has received little attention, is the electronic attribute attestation, a new trust service that can cover the most diverse fields and, when qualified, has a legal value equivalent to paper attestations. Applied to payment means, electronic attribute attestations can play a major role in securing payments by automatically verifying the payee’s name is associated to their account. They can also make a powerful contribution to the establishment of a payment ecosystem natively integrating identity and payment attributes, in short, paving the way for the future of payments within the secure framework of the eIDAS environment.

With this in mind:

- Each service provider and EIDAS2 wallet holder would obtain from their financial intermediary an electronic attribute attestation for each of their IBANs or payment cards, using a uniform format throughout the European Union. This secure attestation guarantees the integrity of the information provided, and thus offers a self-supporting mechanism for verifying the payment beneficiary;
- Merchants and other payees would present it to their customers' or debtors' wallet via an electronically signed payment message, who would then validate the requested payment by means of an electronic countersignature;
- The attestations would be requested and presented in accordance with a standard API defined at European level by an authorised body (e.g. the Berlin Group) to which the banks would have to conform.

Admittedly, this approach requires a collective mobilization and a strong political will meeting the challenge of identity-based payments. While the effort is real and should not be underestimated, it is in our opinion necessary to prepare under the best possible conditions for the new era of identity-based payments managed by wallets that store and communicate, under the full control of their users, payment and identity attributes according to common procedures, in other words, the world of payments of tomorrow.

In view of its potential and the new services it will offer under improved security conditions, and at a time when the ECB/Eurosystem have highlighted the need to ensure the strategic autonomy and resilience of retail payments while developing the digitalisation and innovation of means of payment, it would be a real shame to let the opportunity for secure digital payments offered by eIDAS2 wallets pass us by as the construction of an alternative digital identity scheme dedicated to payments involves an even greater effort and will therefore be more time-consuming and uncertain.

Michael Adams

michael_adams@quali-sign.com

Stéphane MOUY

sgmouy@sgmconsultingservices.com

September 2024