Comment le règlement eIDAS2 pourrait redessiner les paiements de demain

Si la convergence de l'identité et du paiement dans les applications mobiles apparaît aujourd'hui comme une évolution structurelle majeure, son rythme de déploiement est encore incertain. Le règlement eIDAS2, récemment entré en vigueur, pourrait bien être le facteur déclenchant. Au travers d'une nouvelle approche de l'authentification qui s'imposera aux banques, il pourrait porter une évolution porteuse d'innovations pour les commerçants, mais aussi les titulaires de portefeuilles d'identité numérique.

Stéphane Mouy

Président-fondateur
SGM Consulting

Michael Adams

Fondateur
Quali-Sign Ltd

Chacun sait la place prise par l'authentification forte dans les paiements numériques depuis la mise en place de la 2e directive sur les services de paiement (DSP2), aujourd'hui bien ancrée dans les pratiques des prestataires de services de paiement. Un rôle aux conséquences juridiques majeures puisque l'absence d'authentification forte lorsqu'elle est requise empêche le prestataire de service de paiement de valablement s'opposer à la demande de remboursement du paiement par le payeur, sauf en cas de fraude avérée de ce dernier.

Cette évolution bienvenue s'inscrit aujourd'hui dans un contexte renouvelé par le développement des mécanismes de fraude sur internet qui ont contourné l'obstacle de l'authentification forte en développant des scénarios de manipulation du payeur visant à lui faire valider un paiement qu'il n'aurait pas autorisé s'il avait agi en connaissance de cause. Dans ce contexte, garantir une bonne information du payeur sur le paiement qu'il s'apprête à valider, notamment concernant l'identité réelle du bénéficiaire du paiement, apparaît évidemment nécessaire.

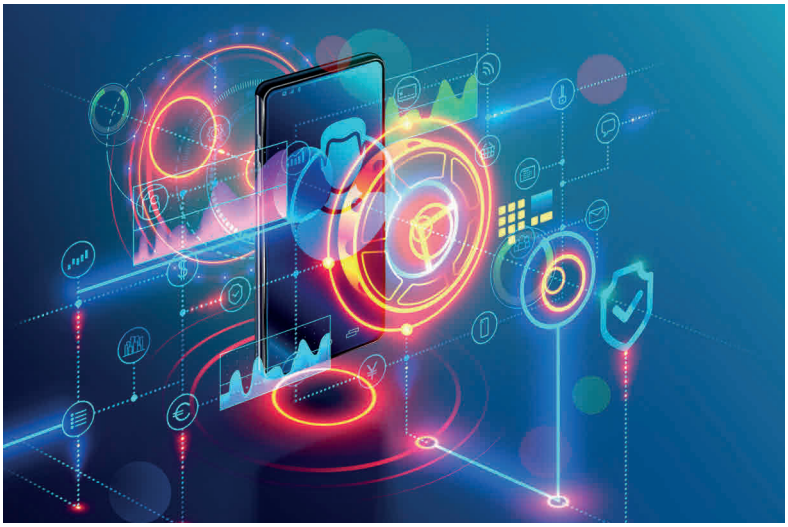
La vérification de l'identité des parties au paiement joue donc un rôle majeur dans la sécurisation des paiements, qui n'est certes pas nouveau mais est aujourd'hui renforcé par les exigences de vérification des bénéficiaires des paiements inscrites dans le règlement sur les paiements instantanés et le projet de règlement sur les services de paiement (RSP) mais aussi le déploiement annoncé pour la fin 2026 des portefeuilles (*wallets*) européens d'identité numérique mis en place par le nouveau règlement eIDAS2. Comme on le sait, ces *wallets* eIDAS2 assureront la conservation sécurisée d'attributs certifiés d'identité et de statut de leur titulaire et devront être acceptés par les prestataires de services fin 2027.

Et puisque des *wallets* sont déjà massivement utilisés pour conserver et gérer des moyens de paiement au travers d'applications de type X-pay (Apple Pay, Samsung Pay, Google Wallet pour ne citer que quelques-unes), la convergence d'attributs d'identité, de statut et de paiement au sein d'applications mobiles apparaît comme une évolution structurelle susceptible de profondément transformer les pratiques de paiement de détail. Bientôt des interactions digitales combineront dans des parcours unifiés différents attributs pré-

sentés et/ou demandés par le bénéficiaire du paiement et validés par le titulaire du wallet pour transmission et mise en œuvre par les prestataires de services de paiement.
Bientôt ? Demain ou après-demain ? Personne ne le sait vraiment car si la perspective est bien réelle, le chemin pour y parvenir n'est pas encore écrit. Disons-le clairement, cette évolution nous semble à la fois souhaitable et nécessaire et gagnerait à être anticipée car le manque de préparation risque de conduire certains acteurs des paiements à la vivre comme une contrainte sur laquelle ils n'auront pas prise.
C'est à l'aune de cette évolution que doivent être appréciés, entre autres exemples, le rôle joué par Apple dans l'identité numérique aux États-Unis (*via* l'application *mobile driving licence* – MDL – et la norme ISO 18013-5) ou, plus près de nous, le positionnement de Mastercard comme fournisseur majeur d'identité numérique.
Un facteur significatif de cette évolution devrait être le rôle joué par les *wallets* eIDAS2 dans l'authentification forte des paiements. Expliquons-nous.

Le choix regrettable de l'authentification forte par redirection

L'authentification forte requise par la DSP2 et son règlement d'application est aujourd'hui massivement orientée autour des schémas de redirection vers le prestataire de service de paiement teneur de compte du payeur. Lorsqu'elle est appliquée – et rappelons ici qu'elle n'est pas toujours requise et que ses modalités peuvent varier pour notamment intégrer un « lien dynamique » avec l'opération de paiement considérée en affichant le montant et du bénéficiaire du paiement – le payeur est redirigé vers l'environnement de son teneur de compte, le plus souvent son application bancaire mobile, à charge pour ce dernier d'organiser l'authentification forte au moyen de procédures numériques qu'il aura définies et validées.
Ce schéma dit de redirection, aujourd'hui très dominant pour la mise en œuvre de l'authentification forte, est logique lorsque l'on considère l'authentification forte comme une responsabilité des établissements teneurs de compte, ce qui est justement l'approche de la DSP2 et, à ce jour, du projet de Règlement pour les services de Paiement (RSP). Dans cette approche, en effet, l'établissement teneur de compte définit les modalités de mise en œuvre de l'authentification forte ainsi que celles relatives à la manifestation du consentement de ses clients aux paiements – deux sujets distincts mais de fait très liés car l'authentification forte sert en pratique à s'assurer que le titulaire légitime du compte est bien celui qui a agi à distance pour autoriser le paiement.
Et puisqu'il en définit les modalités, celles-ci s'imposent aussi aux Tiers Prestataires de Services, tout particulièrement les prestataires de services d'initiation de paiement, lesquels ont souvent préconisé un schéma alternatif d'authentification forte dite « embarquée » (*embedded*) par lequel l'authentification forte est directement intégrée au message transmis par le prestataire de service d'initiation de



paiement à l'établissement teneur de compte du payeur et intervient donc en amont de l'intervention de ce dernier.
Cette position mettant les teneurs de compte en position privilégiée sur les modalités de mise en œuvre de l'authentification forte, logique au regard des dispositions de la DSP2 et de son règlement d'application, a été validée par l'Autorité bancaire européenne en 2020. Celle-ci précise en effet que les teneurs de compte ne sont pas tenus de mettre en œuvre une authentification forte embarquée lorsqu'ils ne la mettent pas à disposition de leurs propres clients.
Cette situation peut être regrettée car le schéma d'authentification embarquée est porteur d'innovations et de sécurité accrue pour les paiements, notamment parce qu'il offre plus de souplesse dans la gestion des données de paiement et permet, outre une plus grande concurrence entre moyens de paiement, la mise en place de services nouveaux à valeur ajoutée. Enfin, il permet la généralisation du lien dynamique qui est un outil puissant de lutte contre les formes nouvelles de fraude.
Les choses en resteraient sans doute là avec le futur RSP – car le projet actuel se situe aujourd'hui dans la droite ligne de la DSP2 sur cet aspect – si un élément nouveau ne venait justement rebattre les cartes, à savoir le règlement eIDAS2 qui prévoit que les portefeuilles d'identité numérique assureront l'authentification forte requise pour les paiements si leur titulaire souhaite les utiliser à cet effet. Cette authentification forte s'imposera alors aux prestataires de services de paiement et ne pourra être refusée par eux ou conditionnée à la mise en place de mesures complémentaires.

Les *wallets* eIDAS2 changent la perspective

Dans l'approche eIDAS2, l'authentification forte n'est plus une fonctionnalité mise en œuvre par les teneurs de compte pour les paiements de leurs clients mais un mécanisme légalement reconnu assuré par des applications numériques agréées répondant aux exigences du niveau de garantie élevé et bénéficiant d'un régime spécifique de responsabilité issu du règlement eIDAS. Le changement de perspective avec l'approche de la DSP2 est structurant car

l'authentification forte des *wallets* eIDAS2 est un mécanisme juridiquement autonome qui ne peut dès lors pas être vu comme une mission contractuellement déléguée par le teneur de compte du payeur – à la différence de ce que prévoit le projet de RSP pour les *wallets* X-pay (*pass-through wallets*). Il est aussi bienvenu.

Prenons l'exemple de paiements conditionnés à la preuve de majorité, situation typique des paris en ligne mais aussi de la location de voiture et de nombreux autres cas d'usage. Plutôt que de gérer séparément la mise en place du service puis son règlement, il sera possible, *via* un mécanisme d'authentification forte embarquée de directement associer au message d'autorisation de paiement un (ou plusieurs) attributs d'identité ou de statut demandés par le prestataire de service et disponibles sur le *wallet* du consommateur, comme par exemple une preuve de majorité, de résidence ou d'éligibilité à une réduction de prix. À terme, ce changement permet de meilleurs services pour les commerçants, notamment aux fins de réconciliation des flux de paiement avec les données comptables, et des interactions à la fois mieux sécurisées et plus fluides pour les consommateurs.

Comment eIDAS2 est RSP doivent se mettre en cohérence

Si le règlement eIDAS2 définit le rôle des *wallets* en matière d'authentification forte, il n'en dit pas plus et n'a d'ailleurs pas vocation à le faire pour les paiements, ce qui ouvre deux modalités pratiques possibles.

Une première option, a minima, serait de limiter le rôle des *wallets* à l'authentification forte des paiements prévue par le règlement eIDAS2, étant entendu que les moyens de paiements restent conservés et gérés par une autre application mobile (un wallet X-pay ou une application bancaire). Ce schéma s'apparente à celui pratiqué en Belgique avec l'application d'identité numérique ITSME utilisée pour la validation de paiements. Il est certes possible mais, outre le fait qu'il ne tire pas pleinement parti du potentiel des *wallets* eIDAS2, présente l'inconvénient de dégrader l'expérience utilisateur en entraînant une friction significative – voire l'impossibilité de le mettre en œuvre dans les interactions hors ligne. Ses perspectives nous semblent donc limitées.

Une deuxième approche, que nous préconisons, est de tirer parti du fait que les *wallets* eIDAS2 ont vocation à conserver et gérer des attestations électroniques et de leur donner un rôle de plein exercice pour les paiements en leur confiant, outre l'authentification forte, la gestion des moyens de paiement. Cette approche s'inscrit pleinement dans la logique du règlement eIDAS2 et de l'ambition qu'il porte pour les paiements.

Comment accompagner au mieux une telle évolution ?

La première chose serait de mieux intégrer le rôle des portefeuilles d'identité numérique dans le projet de RSP. À titre d'illustration du décalage entre les deux textes, on mentionnera le fait que le projet de RSP donne en pratique un rôle exclusif au teneur de compte du payeur pour la définition des procédures de consentement du payeur au paiement sans évoquer les portefeuilles d'identité numérique. On voit mal comment dissocier ce sujet de consentement de l'authentification forte qui vise en pratique à s'assurer que le titulaire légitime du compte débité est bien celui qui a autorisé le paiement et non un tiers. La logique serait de dire que lorsque le wallet eIDAS2 est utilisé pour gérer l'authentification forte, ce qui est maintenant acté par le règlement eIDAS2, la procédure de consentement du payeur devrait lui être subordonnée – ce qui relève du projet de RSP.

La seconde est de clarifier le régime de responsabilité des prestataires de services teneurs de compte issu de la DSP2 et du futur RSP, que le règlement eIDAS2 n'a évidemment pas vocation à bousculer, de même qu'il n'a pas pour objectif de redéfinir les cas d'application de l'authentification forte. Une articulation harmonieuse entre les deux textes paraît toutefois possible : les prestataires de services de paiement restent « en responsabilité juridique » sur l'authentification forte dans les paiements dans les conditions définies par la DSP et le futur RSP mais, lorsqu'un wallet eIDAS2 intervient, leur rôle n'est plus de la mettre en œuvre mais simplement de vérifier qu'elle est bien intervenue.

Cette clarification relève sans doute du futur règlement d'application basé sur les standards techniques réglementaires que l'Autorité bancaire européenne aura pour mission d'élaborer en application du RSP, notamment aux fins de prendre en compte les *wallets* eIDAS2. Elle suppose toutefois que l'authentification forte des *wallets* eIDAS2 offre un mécanisme de vérification robuste, simple et pratique. Heureuse coïncidence, c'est justement le cas de la signature électronique qui figure au cahier des charges des *wallets* eIDAS2.

Le rôle clef de la signature électronique

La signature électronique présente en effet de nombreuses vertus pour les paiements numériques en combinant robustesse et flexibilité d'utilisation dans un mécanisme idéalement adapté à la manifestation de décisions du titulaire du wallet pour assurer l'irrévocabilité des paiements. Parce qu'elle fait usage de procédés cryptographiques sécurisés et implique nativement une authentification forte, elle offre un excellent niveau de protection contre la fraude. De plus, elle offre une grande flexibilité d'utilisation en s'appliquant tout à la fois au message de paiement mais aussi aux différents attributs susceptibles d'accompagner celui-ci – par exemple IBAN ou autres références de moyens de paiement – tout en supportant aussi bien le mode en ligne que le mode hors ligne, lorsque le wallet du payeur interagit avec le terminal du commerçant *via* un protocole de proximité de type NFC ou autre. Enfin, cerise sur le gâteau, elle est bien adaptée à l'exigence du lien dynamique, qui partage avec elle de nombreuses caractéristiques.

Mais ce qui distingue vraiment la signature électronique des autres spécifications techniques considérées pour les *wallets* eIDAS2, c'est l'existence d'un fichier de preuve attaché au message signé indiquant « *qui a fait quoi* », vérifiable par toute personne et utilisable dans le cadre de procédures contentieuses. Et lorsque la signature est basée sur un certificat qualifié garantissant l'identité du signataire – ce qui est recommandé – le niveau d'assurance offert par la signature électronique s'avère alors nettement supérieur aux pratiques actuelles en matière d'authentification forte.
On le voit, l'utilisation de signatures électroniques pour l'authentification forte des *wallets* eIDAS2 offre un mécanisme d'authentification robuste et facilement vérifiable pour les prestataires de service de paiement, leur permettant de gérer de façon simple leur responsabilité au titre de la DSP2. Et dans l'hypothèse, à vrai dire très improbable, où cette authentification serait techniquement mise en défaut, il leur sera également possible d'activer les recours prévus par le règlement eIDAS à l'encontre du fournisseur de wallet, gestionnaire du mécanisme d'authentification, voire même de l'État sponsor dudit *wallet*.

Quelle réponse collective pour assurer l'autonomie stratégique des paiements européens ?

La prise de conscience de la nécessité d'une infrastructure de paiements européenne est récente – nécessité d'autant plus affirmée que les systèmes de paiement par carte, gérés par des opérateurs non européens, prennent aujourd'hui une place dominante dans l'écosystème des paiements de détail en Europe et dont les jeux olympiques de Paris ont été la dernière remarquable illustration. Cette situation accentue la dépendance structurelle des prestataires de services de paiement au duopole VISA/Mastercard et pose un problème majeur de tarification pour les commerçants et marchands, comme l'a opportunément relevé l'autorité de régulation des paiements britannique dans son rapport de mai 2024 faisant état de commissions en forte progression sans réelle corrélation avec les services rendus.
On ne voit pas bien ce qui viendra changer cette situation dans les années à venir, si ce n'est une meilleure disponibilité des moyens de paiement alternatifs à la carte sur les points de vente et la mise en production de nouveaux services de paiement combinant attributs d'identité, de statut et de paiement, lesquels nécessiteront en toute hypothèse une infrastructure de paiement adaptée. Une première approche pourrait être d'aménager les spécifications EMVCo déployées par les réseaux de carte et aujourd'hui très dominantes, au risque toutefois d'accroitre la dépendance des acteurs de l'écosystème des paiements à ces derniers.
Une autre méthode, qui a notre préférence, consisterait à s'appuyer sur l'environnement eIDAS et développer pour les *wallets* d'identité numérique un schéma d'authentification forte basé sur une API d'open banking qui ne serait plus conditionné à l'accord des banques (ce qui était la logique DSP2) mais s'imposerait à elles (ce qui est la logique eIDAS2).
Car le règlement eIDAS2 peut être aussi un puissant vecteur de modernisation des paiements en Europe. En effet, un des apports majeurs du règlement eIDAS, trop peu mis en avant, est l'*attestation électronique d'attribut*, un nouveau service de confiance pouvant couvrir les domaines les plus divers et, lorsqu'elle est qualifiée, ayant une valeur juridique équivalente à l'attestation délivrée sur papier. Appliquées aux moyens de paiement, les attestations électroniques d'attribut peuvent jouer un rôle majeur de sécurisation des paiements en assurant une vérification automatique du bénéficiaire du paiement mais aussi puissamment contribuer à la mise en place d'un écosystème de paiement intégrant nativement attributs d'identité et de paiement, bref, préparer l'avenir des paiements dans le cadre sécurisé de l'environnement eIDAS.
Dans cette perspective :
– chaque prestataire de service et titulaire de *wallet* EIDAS2 pourrait obtenir de son teneur de compte une attestation électronique d'attribut qualifiée concernant chacun de ses IBAN ou cartes de paiement, selon un format uniforme au sein de l'Union européenne. Au travers d'un procédé cryptographique liant le nom du titulaire du compte et le moyen de paiement, cette attestation sécurisée garantit l'intégrité des informations fournies et offre donc un mécanisme autoporté de vérification du bénéficiaire du paiement ;
– les commerçants et autres bénéficiaires de paiement la présenteraient au *wallet* de leurs clients ou débiteurs par le biais d'un message de paiement signé électroniquement, à charge pour ces derniers de valider le paiement demandé au moyen d'une contre-signature électronique ;
– les demandes et présentations des attestations se feraient selon des API normées définies au niveau européen par un organisme habilité à cet effet (par exemple le Berlin Group) auxquelles les banques devraient se conformer.
Certes, cette approche nécessite une réelle mobilisation collective et une volonté politique affirmée pour mettre en œuvre un schéma d'*open banking* adapté aux enjeux des paiements numériques à base d'identité. Si l'effort est réel et ne doit pas être sous-estimé, il est à notre avis nécessaire pour préparer dans les meilleures conditions la nouvelle ère des paiements à base d'identité gérés par des *wallets* conservant et communiquant, sous le plein contrôle de leurs titulaires, des attributs de paiement et d'identité selon des procédures communes, c'est-à-dire le monde des paiements de demain.
Au regard de ses potentialités et des nouveaux services qu'il offrira dans des conditions de sécurité renforcées, et alors que la BCE/Eurosystème a mis en avant la nécessité d'assurer l'autonomie stratégique et la résilience des paiements de détail tout en développant la digitalisation et l'innovation des moyens de paiement, il serait vraiment dommage de laisser passer l'opportunité de paiements numériques sécurisés offerte par les *wallets* eIDAS2 car la construction d'un schéma alternatif d'identités numériques dédiées aux paiements implique un effort encore plus important et sera donc plus longue et aléatoire. ■