Committed to Europe

Position d'Orange sur la révision du règlement sur l'identification électronique et le projet d'Identité Numérique Européenne

Résumé

Orange, en tant qu'opérateur multiservices, salue l'initiative de la Commission européenne concernant la révision du règlement sur l'identification électronique et les services de confiance pour les transactions électroniques (eIDAS). Nous soutenons les propositions ambitieuses visant à étendre le champ d'application du règlement au secteur privé, et à introduire de nouvelles règles d'authentification pour les terminaux numériques ainsi qu'un système européen d'identité numérique (EUid) pour accéder aux services publics et privés en ligne.

Il nous semble important que la révision comprenne ces trois améliorations. Ceci permettrait non seulement de faciliter la numérisation des documents officiels (ex : permis de conduire, assurance maladie, etc.) et de renforcer la fiabilité de ces documents numérisés, mais aussi de sécuriser les transactions dans un monde numérique hyper-connecté. Les solutions sur terminaux mobiles ont un grand potentiel, ces derniers étant largement utilisés par les citoyens européens. Mais la mise en place d'un cadre juridique favorable est indispensable pour stimuler leur déploiement au sein du marché unique et éviter toute fragmentation ou solutions propriétaires fermées.

Pour tirer profit du potentiel des services d'identification numérique et des services de confiance sur les terminaux numériques, Orange propose les modifications suivantes au règlement :

- Les services eIDAS doivent être mis à la disposition de tous les citoyens et étendus au secteur privé et aux terminaux numériques (smartphones) ;
- La mise en œuvre de services eIDAS sur les terminaux numériques doit reposer sur des solutions interopérables et indépendantes de tout type d'acteurs, en intégrant une approche de « sécurité dès la conception » ;
- Les solutions conformes au règlement eIDAS doivent être fondées sur des éléments sécurisés et standardisés, tels que les composants sécurisés hardware des terminaux mobiles ;
- Les fournisseurs de services conformes au règlement eiDAS doivent pouvoir déployer les solutions standardisées interopérables disponibles sur tous les types de terminaux mobiles (smartphones).

Notre société est de plus en plus numérisée, mais les solutions d'identité numérique restent fragmentées, ce qui représente un risque pour la souveraineté numérique de l'UE

Avec le premier règlement eIDAS, les institutions européennes ont créé un cadre juridique permettant d'accéder aux services de confiance en toute sécurité et d'effectuer des transactions en ligne transfrontières. Après cette étape, Orange salue la volonté de la Commission européenne de réviser ce règlement afin de fournir à tous les citoyens, entreprises privées et administrations publiques des solutions d'identité numérique sécurisées.

Les solutions d'identité numérique deviennent essentielles, en particulier sur les terminaux mobiles. De plus en plus de citoyens européens utilisent des services sur leurs mobiles ; leur donner la possibilité de recourir à des systèmes d'identification sécurisés est indispensable, par exemple pour accéder à des services numériques sécurisés, qu'ils soient publics (e-gouvernement, e-santé, etc.) ou privés (ex : services bancaires, transports). Les solutions sécurisées sur mobiles ont donc un grand rôle à jouer.

Cependant, les prestataires de services des secteurs public et privé éprouvent des difficultés à déployer leurs services sécurisés sur mobiles dans l'UE pour les raisons suivantes :

- Ils ne peuvent pas déployer leurs solutions sur l'ensemble des smartphones ;
- Il n'est pas possible de fournir un niveau de sécurité homogène pour l'ensemble des appareils; ce niveau dépend en effet des solutions déployées par chaque fabricant de système d'exploitation ou d'appareil ; les fournisseurs de services n'ont d'autre choix que de s'y adapter ;
- Le cadre juridique actuel est complexe (contractuel, technique…) ;
- La fragmentation du marché est élevée ; il existe une forte dépendance vis-à-vis des principaux acteurs mondiaux, tels que les fabricants de terminaux ou les fournisseurs de systèmes d'exploitation qui déploient leur propre technologie et ont tendance à promouvoir leurs propres services.

Cela crée une situation où la compétitivité et la souveraineté de l'UE sont menacées :

- Les acteurs européens risquent d'être globalement affaiblis pour le développement de services sécurisés sur mobiles ;
- Les États membres risquent de se trouver en situation de dépendance vis-à-vis de solutions technologiques et de systèmes d'identification non définis au sein de l'UE.

La révision du règlement eIDAS constitue donc une réelle opportunité pour mettre en œuvre une stratégie ambitieuse sur les solutions d'identité numérique et ainsi dynamiser le marché numérique européen.

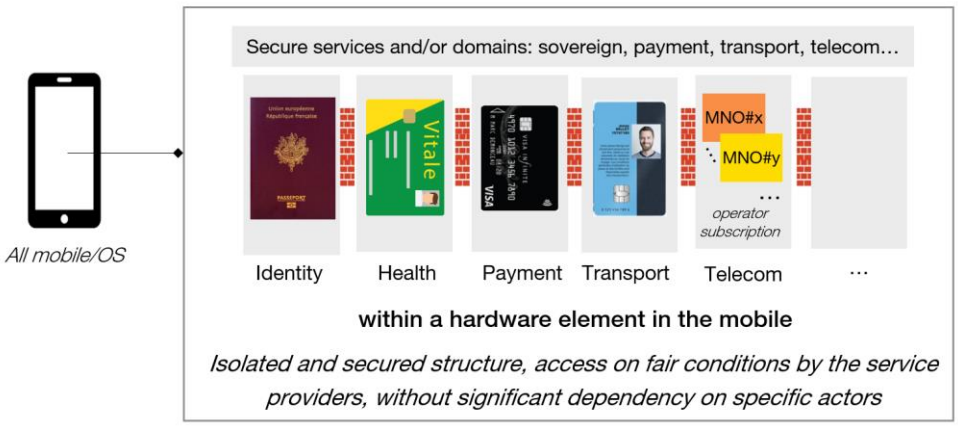
Une nouvelle solution pour un système d'identification interopérable et hautement sécurisé sur les appareils mobiles

Héberger les services sécurisés dans un composant hardware des appareils mobiles

L'industrie mobile s'est déjà fortement investie dans le développement de solutions d'authentification en ligne standardisées et faciles d'emploi, comme par exemple avec le service Mobile Connect.

Afin de compléter ces initiatives et de garantir une large accessibilité aux services qui requièrent un niveau élevé d'authentification, indépendamment de tout type de fournisseur, Orange a initié, avec l'industrie mobile et les fabricants, la standardisation d'une solution permettant d'héberger les services sécurisés et données sensibles (attributs, identifiants, attestations…) dans un élément hardware des appareils mobiles. Il s'agit du projet de standardisation « SAM » (« Secured Applications for Mobile ») mené au sein de la GSMA.

Cette solution hautement sécurisée dans un composant hardware de l'appareil mobile sera divisée en plusieurs «domaines» (par ex : identité, santé, transport, etc.) où tous les fournisseurs de services correspondants pourront être hébergés.



Avec cette solution, seul l'utilisateur final sera en mesure de gérer ses données sensibles, garantissant la protection et la confidentialité des données conformément au RGPD. En d'autres termes, l'identification et l'authentification en ligne seront effectuées indépendamment du fournisseur de services.

Cette solution d'hébergement doit être interopérable et accessible à tout fournisseur de services accrédité depuis leur back-end via des interfaces standardisées ; la sécurité et la certification des prestataires de services seront développées en fonction des besoins spécifiques des différents services et/ou domaines hébergés et délivrés par les autorités compétentes.

Les travaux de standardisation en cours

Les travaux de standardisation ont débuté en février 2020 dans le cadre d'un groupe de travail dédié de la GSMA rassemblant de nombreux acteurs clés : fabricants de terminaux, fabricants de systèmes d'exploitation, fournisseurs de composants et opérateurs mobiles du monde entier. La GSMA a défini des cas d'utilisation, qui incluent des services d'identité correspondants au niveau de garantie « substantiel » du règlement eIDAS, ainsi que la numérisation de documents officiels (ex. permis de conduire).

La définition des exigences techniques devrait être finalisée d'ici le quatrième trimestre 2020 et les spécifications techniques d'ici le premier semestre 2021, en étroite coopération avec les organismes de normalisation compétents (GlobalPlatform, ETSI).

Mise en œuvre de la solution standardisée

Cette solution standardisée pour les services sécurisés dans un élément sécurisé du hardware des appareils mobiles va créer un cadre interopérable et solide pour le déploiement de services d'identification numérique et autres services de confiance. Cette solution devrait être mise à la disposition des prestataires de services et de l'ensemble des citoyens, sans aucune forme de discrimination, par tous les fabricants de smartphones.

Recourir à cette solution standardisée est le seul moyen de couvrir une large gamme de smartphones tout en évitant les solutions propriétaires ou isolées de fabricants ou prestataires de services, qui à ce jour fragmentent le marché. En outre, cette solution pourrait être également utile pour développer l'identification numérique européenne (EUid) sur les appareils mobiles, réduisant à nouveau tout risque de fragmentation.

Cette approche ambitieuse permettrait le déploiement d'applications sécurisées sur mobiles dans les secteurs public et privé avec de nombreux avantages :

- Simplification et dématérialisation des services : y compris des services sensibles, pour un grand nombre d'utilisateurs et de citoyens ;
- Facteur d'innovation et de compétitivité pour les secteurs public et privé : grâce à une meilleure diffusion des services de confiance au sein de l'environnement mobile ;
- Cybersécurité améliorée : reposant sur une solution de sécurité certifiée répondant aux attentes des pouvoirs publics nationaux et européens ;
- Souveraineté numérique renforcée : puisque la possibilité de déployer des services est de façon significative indépendante des solutions propriétaires ;
- Soutien à l'adaptation à l'ère numérique et pour une meilleure harmonisation des processus administratifs des États membres européens.

Pour plus d'informations : https://www.orange.com/fr/groupe/orange-bruxelles, ou suivez-nous sur Twitter : @Orange_Brussels