Une année de post-pandémie marquée par la sécurité, l'interopérabilité et les solutions de mobilité

Retour sur la façon dont le secteur de l'identité aborde certaines des tendances et des défis qui ont façonné 2022 et qui marqueront encore les mois, voire les années, à venir.

JUSTICE ET SÉCURITÉ PUBLIQUE VOYAGE

POSTÉ LE 10.28.22

La société mondiale actuelle repose sur la facilité de communiquer, d'interagir et de réaliser des échanges commerciaux entre les individus par-delà les frontières nationales. Une société numérique fondée sur le télétravail et la vérification d'identité à distance ne peut prospérer à long terme que si les mêmes normes sont appliquées à l'échelle internationale, ou du moins régionale. Cependant la pandémie a mis en exergue plusieurs défis qui doivent encore être relevés pour que les citoyens puissent faire valoir leurs droits, en prouvant leur identité à distance, ou puissent remplir leurs missions professionnelles avec plus de flexibilité :

- La **sécurité** demeure une préoccupation majeure tandis qu'un nombre croissant de personnes interagissent et ont besoin de technologies pour accéder à des données à distance.
- En touchant tous les pays, au mépris des frontières, la pandémie a aussi révélé un autre facteur important dans l'équation : **l'interopérabilité**.
- Enfin, la **mobilité** et la flexibilité sont des mots-clés qui ont beaucoup influé sur notre manière de travailler au cours des deux dernières années. Alors que beaucoup de salariés retournent au bureau au moins deux ou trois fois par semaine, l'intérêt pour une organisation flexible, souvent synonyme de gain de temps, demeure. Les forces de l'ordre ne faisant pas exception, au cours des derniers mois, nous avons observé des demandes croissantes pour mettre à leur disposition des solutions plus mobiles.

Replongeons de manière plus détaillée dans ces tendances marquantes de 2022, qui subsisteront très vraisemblablement pendant les mois, voire les années, à venir.

Sécurité

Les technologies biométriques simplifient la vie des individus et leur permettent de vivre dans un monde plus sûr et sécurisé. L'on n'insistera jamais assez sur la sensibilité des données biométriques et nous avons d'ailleurs déjà présenté plusieurs solutions pour les utiliser de façon sécurisée dans des articles précédents. Cependant, dans les paragraphes qui vont suivre, nous souhaitons cette fois explorer d'autres dimensions que la sécurisation des données, et pousser la réflexion au-delà des défis actuels.

Intervenir en amont : protéger les appareils dès la phase de production

Du fait de leur facilité d'utilisation et de la sécurité qu'ils apportent, l'installation d'appareils connectés, comme des terminaux de contrôle d'accès biométriques, a nettement augmenté. Toutefois, le revers de la médaille d'une technologie à succès est que celle-ci devient souvent une cible privilégiée. La sécurité étant toujours tributaire du maillon le plus faible, les fournisseurs de technologie ont dû réévaluer l'ensemble du cycle de vie des produits, et en particulier la première étape : la production, pour **garantir le niveau de sécurité le plus élevé**.

Sans des mesures adéquates, **un produit est particulièrement exposé au cours du processus de fabrication**. Par exemple, le firmware peut être copié ou modifié afin d'y intégrer des failles de sécurité qui pourraient être exploitées ultérieurement, une fois que le produit sera mis en service. La contrefaçon et la copie de produits, ainsi que le vol d'informations protégées (comme des clés), constituent aussi des risques à prendre en compte lors de la fabrication d'un appareil.

Bien que la **production sécurisée existe depuis de nombreuses années**, pour les puces à microprocesseur utilisées dans les cartes bancaires et les technologies SIM par exemple, son application à la fabrication d'appareils connectés est récente.

La production sécurisée s'appuie sur trois piliers :

- **Une « racine de confiance » fondée sur l'utilisation de clés cryptographiques, de firmware et de matériel sécurisés**
  La racine de confiance se compose d'au moins trois éléments : un microprocesseur ou autre élément sécurisé qui est capable de créer un « coffre-fort sécurisé » dans l'appareil, un logiciel signé et crypté associé à une fonctionnalité de démarrage sécurisé, ainsi qu'un module de sécurité matériel (HSM). L'objectif du HSM est de protéger les principaux secrets et la liaison de communication avec l'appareil au cours du processus de fabrication.
- **L'audit et la certification du processus d'approvisionnement du fabricant**
  L'audit permet de s'assurer que le processus de fabrication est conforme aux règles de sécurité définies et que seuls des composants de sécurité certifiés sont utilisés.
- **La traçabilité des appareils fabriqués**
  La traçabilité implique le suivi et l'enregistrement de toutes les étapes du cycle de vie de l'appareil, depuis la première étape de la chaîne d'approvisionnement jusqu'à la livraison de l'appareil au client.

La production sécurisée permet aux entreprises de collaborer avec des sous-traitants, sans crainte que l'appareil ne soit modifié ou détourné par un élément extérieur. Elle garantit aussi que l'appareil sera bien préparé à résister aux enjeux de sécurité auquel il pourrait être confronté à l'avenir.

Au lieu de créer un produit, puis d'essayer de le protéger, la production sécurisée vise à éliminer les vulnérabilités à la source.

Avoir une longueur d'avance : préparer l'avenir avec la cryptographie post-quantique

Depuis le début des années 1990, de grands progrès ont été réalisés pour démontrer comment un ordinateur s'appuyant sur la mécanique quantique pourrait accélérer la résolution de problèmes numériques insolubles. À l'heure actuelle, des efforts ont été entrepris au niveau mondial pour fabriquer des processeurs d'information quantique. Si le chemin vers un ordinateur quantique à usage général est encore très long et incertain, de puissantes machines à usage spécifique pourraient faire leur apparition dans les années à venir. L'un des domaines qui sera affecté par ces progrès est la cryptographie : la technologie utilisée pour **sécuriser notre vie numérique par le biais du cryptage, de l'authentification et des signatures numériques**.

Des chercheurs ont déjà créé des algorithmes quantiques qui pourraient être utilisés pour accélérer les attaques sur les technologies cryptographiques actuellement utilisées. Pour certains algorithmes, l'accélération est limitée et il suffit d'élargir la clé cryptographique pour contrer la menace. Cependant, pour d'autres algorithmes, qui sont au cœur de tout protocole de sécurité moderne, cela signifie que, dès lors qu'un ordinateur quantique suffisamment puissant sera disponible, il sera très difficile d'assurer la confidentialité. Pour que les solutions de sécurité puissent résister aux ordinateurs quantiques, elles doivent être actualisées avec **de nouvelles techniques cryptographiques, appelées cryptographie post-quantique (PQC)**, qui seront capables de résister à une telle menace.

Aujourd'hui, toutes les données cryptées échangées peuvent potentiellement être enregistrées et stockées jusqu'à ce qu'une machine suffisamment puissante pour menacer la cryptographie actuelle soit disponible, permettant ainsi de révéler les données brutes. Pour certaines applications, les données doivent rester en sécurité pendant plusieurs décennies, sans oublier que la migration vers de nouveaux systèmes pourrait prendre des années. Le National Institute of Standards and Technology (Institut américain des normes et de la technologie) a initié un **processus de normalisation** de la PQC. Cette initiative a démarré à la fin de l'année 2017, sous la forme d'un « concours » ouvert et transparent auquel 69 candidats ont participé et, d'ici à 2024, quelques algorithmes seront normalisés.

Toutefois, le passage à cette nouvelle cryptographie ne sera pas chose aisée. Tout d'abord, l'accroissement notable de la **complexité algorithmique** et de la **taille des données** (clés et textes chiffrés) devra être compensé par **de nouveaux matériels et l'optimisation des logiciels**. De plus, les nouveaux algorithmes nécessiteront des années d'étude pour atteindre le degré élevé de confiance de la cryptographie actuelle, à laquelle la société a consacré des décennies de recherche. Pour relever ce défi, les organismes publics et les grands acteurs du secteur vont travailler en étroite collaboration, dans un premier temps, pour déployer des protocoles hybrides associant avec soin la cryptographie actuelle et la PQC, afin d'**éviter une régression** et d'**appliquer la crypto-agilité** : des mécanismes qui permettent d'actualiser les protocoles pour des produits déjà sur le terrain. IDEMIA et les autres grands acteurs du secteur sont bien conscients de leur responsabilité envers la société. Ils savent que pour atténuer les risques de demain, ils doivent commencer à investir dès aujourd'hui.

Interopérabilité

Les portefeuilles numériques ne datent pas d'hier. Cependant, jusqu'à présent, l'accent était mis sur les moyens de paiement : le portefeuille numérique remplaçant le portefeuille physique et la nécessité de retirer de l'argent. Les utilisateurs ont aussi déjà l'habitude d'avoir leur carte d'embarquement électronique ou leurs cartes de fidélité sur leurs smartphones. La nouveauté tient dans la création d'un portefeuille numérique conçu pour nos différents justificatifs d'identité, y compris nos précieuses pièces d'identité. En 2022, Apple et Samsung, deux géants des technologies numériques, ont ajouté des offres d'identité numérique dans leurs solutions de portefeuilles numériques. Une autre nouveauté est la volonté de créer une solution internationale allant au-delà des systèmes nationaux. A ce propos, penchons-nous sur le portefeuille numérique de l'UE, l'un des sujets phares de 2022.

Le portefeuille d'identité numérique européen : sécurisé, interopérable et pratique

Aujourd'hui, seulement 60 % environ de la population de l'UE, dans 14 États membres, est en mesure d'utiliser sa carte d'identité électronique (eID) nationale au-delà des frontières.[1] Annoncé en juin 2021, le portefeuille européen d'identité numérique sera **disponible pour les citoyens et résidents de l'UE** qui souhaitent s'identifier ou fournir la confirmation de certaines informations personnelles. Utilisé à la fois pour des services en ligne et hors ligne dans les secteurs public et privé dans l'UE, ce portefeuille numérique sécurisé pourra contenir les justificatifs d'identité d'une personne, comme sa carte d'identité, son permis de conduire, ses diplômes, ses moyens de paiement, son carnet de vaccination, etc.

Une fois mis en place, le portefeuille numérique de l'UE sera accessible via une application sur le smartphone des utilisateurs, leur permettant de **garder le contrôle sur leurs justificatifs d'identité** à tout moment. Ils pourront ainsi

décider des éléments spécifiques qu'ils souhaitent partager. Par exemple, si un utilisateur a besoin de prouver qu'il a plus de 18 ans, il pourra fournir la preuve de cette seule information, sans communiquer sa date de naissance exacte, son âge, son nom, son adresse ou d'autres renseignements personnels.

Le portefeuille numérique de l'UE permettra aussi aux organismes ou entreprises avec lesquelles les personnes partagent leurs justificatifs d'identité de vérifier que ces documents sont authentiques et qu'ils appartiennent bien au détenteur du portefeuille. Le portefeuille numérique de l'UE vise à offrir une solution sécurisée, simple et sûre qui permettra aux citoyens de partager leurs informations avec des prestataires de services.

Plus important encore, indépendamment de la solution de portefeuille numérique approuvée par un État membre, **l'interopérabilité avec les autres États membres** sera garantie.

Mobilité

Avant la pandémie, la plupart des entreprises n'encourageaient pas le télétravail. L'accès au réseau sécurisé de l'entreprise via un VPN était acceptable pour quelques salariés ou dans des structures dans lesquelles la majorité des collaborateurs était régulièrement en déplacement. Des préoccupations de sécurité identiques ont aussi perduré au sein des forces de l'ordre, notamment pour les agents de terrain, ne leur laissant d'autre choix que d'effectuer leurs tâches quotidiennes au poste, perdant parfois un temps précieux qui pourrait être consacré à protéger les citoyens dans les rues.

Travail à distance pour les forces de l'ordre

Grâce à des technologies plus sécurisées, la confiance dans les solutions mobiles ne cesse d'augmenter, de sorte que les agents de police peuvent **réaliser à distance des tâches comme des vérifications d'identité**. En utilisant une application sur leur smartphone, reliée au système AFIS/MBIS national (via une plateforme Cloud dédiée), les agents peuvent désormais réaliser des contrôles biométriques sur le terrain pour vérifier ou établir immédiatement l'identité d'une personne sur la base de son visage ou de ses empreintes digitales, **comme ils le feraient au poste**. L'appareil photo à l'arrière d'un smartphone permet de prendre des photos suffisamment détaillées des empreintes d'une personne pour une correspondance 1:N.

Les solutions sur le Cloud destinées aux forces de l'ordre profitent de l'efficacité, de l'évolutivité et de l'élasticité de ces technologies, ce qui se traduit par **un temps de réaction rapide pour les agents sur le terrain**, ainsi que divers avantages généraux pour l'institution dans son ensemble. Par exemple, une plateforme Cloud peut être utilisée par de nombreux utilisateurs simultanément, comme des agents de terrain, sans nécessiter d'investissement dans de très grandes capacités informatiques. De plus, une telle plateforme peut être démarrée ou arrêtée en seulement quelques minutes, offrant aux forces de l'ordre une flexibilité optimale. En outre, des plateformes spécialisées pourraient être créées pour gérer des événements particuliers : de grandes manifestations publiques, comme les Jeux olympiques, ou des incidents majeurs de sécurité, etc. Grâce aux technologies développées ces dernières années et à la sécurité accrue qu'elles apportent, les forces de l'ordre peuvent désormais bénéficier d'un mode de travail plus flexible, similaire à celui qui a été adopté dans de nombreux autres secteurs du fait de la pandémie.

---

[1] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-digital-identity_fr

---