Renforcer la sécurité des documents d'identité électroniques : le rôle crucial des mises à jour sur le terrain

IDENTITÉ

POSTÉ LE 26.03.24

Accepteriez-vous d'attendre une décennie avant de réparer votre smartphone ?

Dans un monde de plus en plus connecté où les patches et les mises à jour sont effectués directement et quotidiennement sur les smartphones, Juliette Thomas et Jérôme Boudineau d'IDEMIA Smart Identity se demandent pourquoi nous devrions attendre qu'une carte d'identité électronique soit réémise pour obtenir un système d'exploitation mis à jour. Eh bien, désormais, cette attente n'est plus nécessaire !

L'évolution des systèmes d'exploitation vers des mises à jour automatiques a débuté en 1996 avec Windows Update, offrant aux utilisateurs des patches et des correctifs automatisés. Avec l'émergence des smartphones, les systèmes d'exploitation iOS et Android ont adopté cette pratique, garantissant des correctifs de sécurité et des améliorations fonctionnelles de manière régulière. Avec Windows 10, Microsoft est passé à des mises à jour continues, reflétant les cycles de mise à jour plus fréquents des plateformes mobiles. Aujourd'hui, les mises à jour automatiques sont devenues essentielles dans le domaine de l'informatique, de l'Internet des objets et des communications personnelles, non seulement pour améliorer l'expérience utilisateur, mais aussi pour renforcer la sécurité sur tous les appareils.

Protection sur l'ensemble du cycle de vie du document

Une fois délivrés, les documents d'identité électroniques tels que les passeports, cartes d'identité, permis de conduire, permis de séjour, etc., ont généralement une validité de 10 ans. Pendant cette période, les techniques de fraude évoluent inévitablement, mettant en péril la sécurité du document. Pour contrer cette menace, les autorités émettrices doivent garantir une protection optimale et continue tout au long de la validité du document.

Pour ce faire, le système d'exploitation du document électronique et son application doivent être mis à jour, même après leur délivrance et leur mise en circulation. De nouvelles réglementations en matière de sécurité qui imposeraient de telles exigences d'évolution sont en cours d'introduction.

La première d'entre elles est le EU Cybersecurity Act (CSA), la règlementation européenne sur la cybersécurité. La proposition initiale de réglementation dans le CSA, publiée pour la première fois en 2019, a maintenant été approuvée et devrait bientôt être publiée dans le journal officiel. Le règlement européen sur la résilience cybernétique (EU Cyber Resilience Act – CRA) introduit quant à lui des exigences de cybersécurité obligatoires pour les fabricants et les détaillants de dispositifs connectés à Internet. Le CRA stipule également que cette protection doit s'étendre sur l'ensemble du cycle de vie attendu du produit. Les parties prenantes concernées devront se conformer au mandat dans les 36 mois suivant la date de publication de la loi.

Amélioration de la sécurité et de l'expérience utilisateur

Les discussions se poursuivent, dans certains milieux sur la question de savoir si les documents d'identité électroniques devraient même être considérés comme des « objets connectés » au sens du CSA et du CRA. D'une part, une fonction clé d'un document d'identité électronique est qu'il peut accéder à une gamme de services en ligne, mais ils peuvent également fonctionner comme un document autonome lorsqu'ils sont hors ligne.

> *Je ne me soucie pas outre mesure de ce débat sur la question de savoir si les documents d'identité électroniques devraient être considérés comme des « objets connectés ». C'est une bonne pratique de mettre à jour les protocoles de sécurité en fonction des menaces potentielles. Et si vous pouvez améliorer l'expérience utilisateur en même temps, alors nous, en tant qu'entreprise, nous nous y engageons.*
>
> Juliette Thomas – ID Cards and Service Product Manager

Il y a cependant une différence significative entre recevoir une mise à jour directement d'une entreprise technologique qui vous a fourni un smartphone par exemple, et un document d'identité électronique émis par un gouvernement qui contient beaucoup d'informations personnelles identifiables (IPI). Dans ce cas, le développeur de logiciels devra fournir au gouvernement qui a délivré le document la mise à jour, qui devient alors à son tour l'émetteur de la mise à jour.

La bonne nouvelle est que tous les documents d'identité électroniques contiennent une puce et que les mises à jour peuvent être effectuées via le système d'exploitation.

JPatch

En tête du mouvement vers des documents pouvant être mis à jour sur le terrain se trouve la technologie JPatch développée par IDEMIA Smart Identity. JPatch permet les mises à niveau à distance des logiciels intégrés dans les documents électroniques, sans compromettre les données utilisateur ou la vie privée.

Afin de rendre le processus aussi pratique que possible, les systèmes post-émission et de gestion des identifiants (CMS) d'IDEMIA Smart Identity permettent d'effectuer les mises à niveau de manière fluide, à tout moment et depuis n'importe quel emplacement de confiance. Cette approche élimine le besoin de remplacements coûteux et longs, simplifiant ainsi le processus de mise à jour.

> *Inutile de dire que la commodité ne prend jamais le pas sur la confidentialité ou la sécurité. La technologie JPatch ne met pas les données de l'utilisateur stockées dans le logiciel intégré en danger. En particulier, les données personnelles ne sont pas affectées pendant la mise à niveau, il n'est donc pas nécessaire de les protéger en dehors du logiciel intégré. Cette approche garantit la sécurité, la confidentialité et la vie privée des données.*
>
> Jérôme Boudineau – Senior Product Manager

Les données techniques sur la carte telles que les certificats, clés privées, PIN, etc. n'étant pas affectées, il n'est donc pas nécessaire de protéger les données en dehors du logiciel intégré. L'association entre la carte, son titulaire et l'émetteur

est maintenue.

Une fois déployé, JPatch permet également d'économiser du temps et de l'argent pour toutes les parties prenantes. Il élimine le besoin pour les titulaires de carte de demander une nouvelle carte lorsqu'une mise à jour est nécessaire, et réduit également la charge administrative des autorités émettrices.

À une époque où les consommateurs exigent davantage de commodité et une meilleure expérience utilisateur, des technologies innovantes comme JPatch peuvent contribuer à garantir que les documents d'identité électroniques demeurent sécurisés, à jour et pleinement intégrés dans le monde numérique… sans que vous ayez à lever le petit doigt !