Enhancing eID documents security: the crucial role of field updates

IDENTITY

POSTED ON 03.26.24

You Wouldn’t Wait 10 Years for Your Phone to Fix Itself – Would You?

In an increasingly connected world, where patches and updates are delivered to your smartphone on a daily basis, Juliette Thomas and Jérôme Boudineau from IDEMIA Smart Identity ask why do we need to wait for an electronic ID card to be reissued before we can get an updated operating system? Well now, we don’t!

Automatic updatable operating systems began with Windows Update in 1996, allowing users to receive patches and fixes automatically. As smartphones emerged, iOS and Android operating systems adopted automatic update mechanisms, ensuring regular security patches and feature enhancements. With Windows 10, Microsoft shifted to continuous updates, mirroring the more frequent update cycles of mobile platforms. Today, automatic updates and new versions are the cornerstones of computing, the Internet of Things, and personal communications, providing not only a better experience for the user but also bolstering security across devices.

Whole lifecycle protection

Once issued, electronic ID (eID) documents (passports, ID cards, driver’s licences, residence permits etc.) are typically valid for around 10 years. During this period, fraud techniques will inevitably evolve, and security of the document may be threatened. To protect against this, ID issuing authorities need to future proof eID documents by ensuring they remain highly protected, and that security is optimal throughout the document’s validity period.

To achieve this, the operating system of the electronic document and its application have to be updatable, even after issuance and in circulation. New security regulations are being introduced that would impose such evolution requirements.

The first of these is the EU Cybersecurity Act (CSA). The initial proposal for regulations in the CSA, which was first published in 2019, has now been approved and should soon be published in the official journal. The related EU Cyber Resilience Act (CRA), introduces mandatory cybersecurity requirements for manufacturers and retailers of devices connected to the internet. The CRA also mandates that this protection should extend throughout the whole expected lifecycle of the product. The affected stakeholders will have to comply with the mandate within 36 months from the publication date of the Act.

Improving security and experience

Discussions continue, in some quarters, as to whether eID documents should even be considered as 'connected objects' under the terms of the CSA and CRA. On the one hand, a key function of an eID document is that it can access a range of services when online, but they can equally operate as a standalone document when offline.

> *I don't get too hung up about the debate on whether eID documents should be considered as 'connected objects'. It's good practice to update security protocols in line with potential threats. And if you can improve user experience at the same time then we, as a company, are committed to it.*
>
> Juliette Thomas – ID Cards and Service Product Manager

There is one significant difference though, between receiving an update directly from a technology firm that supplied you with, say, a smartphone and a government issued eID document that contains a lot of personally identifiable information (PII). In this case, the software developer will have to provide the government that issued the document with the update, who then in turn becomes the update issuer.

The good news is that all electronic ID documents contain a chip and updates can be conducted through the operating system.

JPatch

At the forefront of the move toward field updatable eID documents is the JPatch technology developed by IDEMIA Smart Identity. JPatch enables remote upgrades of embedded software in eID documents, without compromising user data or privacy.

To make the process as convenient as possible, IDEMIA Smart Identity's Post Issuance system and Credential management system (CMS) enable upgrades to be seamlessly executed at any time and from any trusted location. This eliminates the necessity for costly and time-consuming replacements, streamlining the update process.

> *Needless to say, convenience never takes priority over privacy or security. JPatch technology doesn't put the user's data that is stored in the embedded software at risk. In particular, personal data is unaffected during the upgrade, so it isn't necessary to safeguard it outside the embedded software. This approach guarantees the safety, confidentiality and privacy of the data.*
>
> Jérôme Boudineau – Senior Product Manager

Technical data (certificates, private keys, PIN etc.) also remain unaffected on the card, so it is not necessary to generate and import it after the upgrade. The association between the card, the holder and the issuer is maintained.

Once implemented, JPatch also saves time and money for all stakeholders. It eliminates the need for cardholders to apply for a new card when updates are required, and for issuing authorities to process the application.

In the era of consumer demand for convenience and user experience, innovative technologies like JPatch can help ensure that eID documents remain secure, up-to-date, and seamlessly integrated into the digital world...without you having to lift a finger!