NEWS AND INSIGHTS FROM THE WORLD OF ID SECURITY

DECEMBER 2021 | #32

The VAULT

A NEW **DIGITAL** FUTURE?

FEATURED ARTICLE

The challenges of changing travel habits
Infineon Technologies

ALSO IN THIS ISSUE

Mühlbauer ID services
Ready for the revolution?

Infineon Technologies
Securing today's digital lifestyle gets easier with SECORA™

AUSTRIACARD
The new age – digital without cards

Infineon Technologies
FIDO: A users best friend for secure authentication

cryptovision
Self-sovereign identity & eID documents: two worlds colliding?

Wibu-Systems
The IT Security Club – where innovation meets community

TrustSEC
Bringing about frictionless financial freedom with HASHWallet

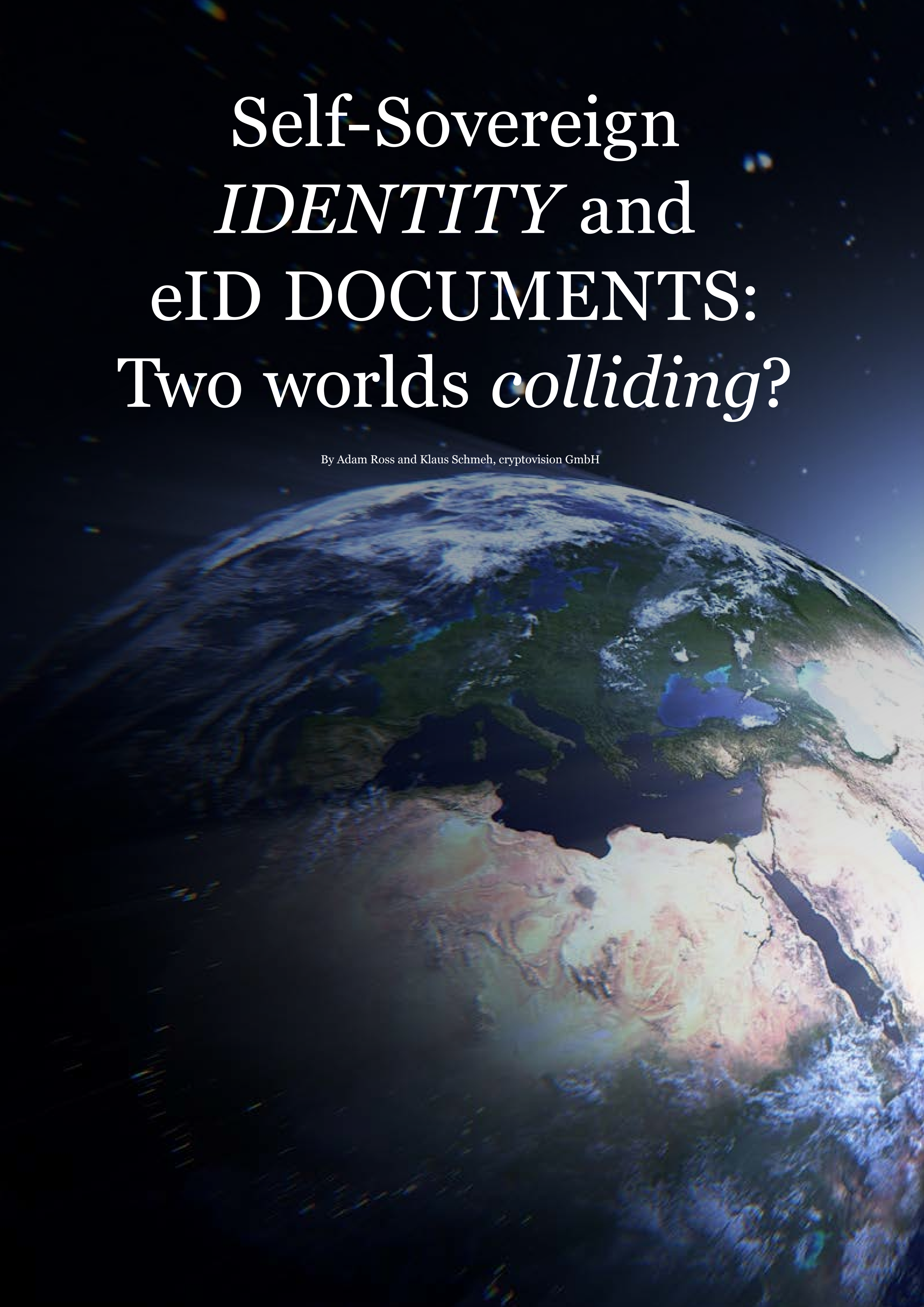
Looking to move on?
Applet Suite certified on
Infineon
NXP
Veridos
We are with you on all eID platforms, enabling multiple applications.
cryptovision

Our eID solutions* are flexible, secure, certified. So you can do things just the way you want. Our Government ID experts and our global network of qualified partners will lead the way. Find out more on **cryptovision.com/eID**

*Java Card^{TM} Applet Suite | Personalization | Middleware | Certificate Management

Self-Sovereign *IDENTITY* and eID DOCUMENTS: Two worlds *colliding*?

By Adam Ross and Klaus Schmeh, cryptovision GmbH



> *"The combination of SSI and eID documents has great potential, from which both technologies can benefit.*
> *– Ben Drisch, cryptovision*

□ A Self-Sovereign Identity (SSI) gives a person sovereignty over their identity data. Every individual can decide to whom his or her name, age, university degrees or purchase records are revealed, and who vouches for the accuracy of this information. At first view, the SSI approach is at odds with the electronic identity documents used in many states, as in the latter model it's the state that has sovereignty over its citizens' identity data. On closer inspection, however, SSI and electronic identity documents can complement and even benefit from each other.

Identity management traditionally followed a centralized approach, where a state, for example, managed the identities of its citizens. In the last few years, globally operating, technology-driven and cross-industry oriented platforms, successfully pushed the market for digital identity management systems, based on an already significant customer base. When it comes to data protection, these approaches meant that an individual had to trust a state authority, an employer, or a global technology platform. This meant that users needed to trust the major software suppliers, social media operators, and other parties that have an interest in using personal data for commercial interests.

The individual strikes back

There is, however, a technology that enables the individual to strike back: Self-Sovereign Identity (SSI). In SSI environments, it's the user who generates a digital identity and who controls it – typically with a software called "wallet". With their wallet, a user can add the identity data they want and delete the pieces of information they don't want to be included any more. The data that a user chooses, may be authenticated by a third party with a digital signature or a blockchain entry. In addition, the wallet allows the individual to grant access to their identity information, based on their personal requirements.

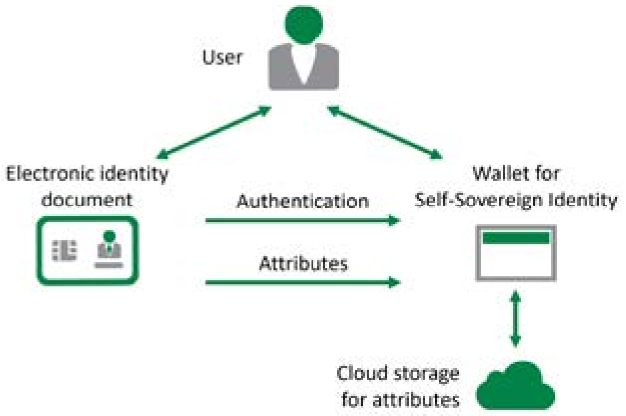
As SSI is still a new topic, current activities in this area are either experimental in nature, or concerned with standardization. For instance, a working group of the European Union is currently exploring the possibilities of SSI within the European Blockchain Services Infrastructure (EBSI). One of their goals is to create an eIDAS-compatible "European Self-Sovereign Identity Framework" (ESSIF). Among other things, ESSIF specifies a data structure, called a "decentralized identifier" (DID), which can be used by a wallet for storing identity data.

Another European research activity, IDunion, is developing an open SSI infrastructure that is meant to be used by individuals all over the world. IDunion is operated by a consortium of mainly German companies and organisations. GAIA-X, a project operated by the German Federal Ministry for Economy and Energy (Bundesministerium für Wirtschaft Und Energie - BMWi), is aiming to build a secure, cloud-based data infrastructure for Europe. This infrastructure, which is independent from US suppliers and compliant with European data protection regulations, includes an SSI-type identity management. And then, there's Modular Open Source Identity Platform (MOSIP) a project that aims to establish a foundational ID that can then be used to access a wide variety of government and private services, via a progressive open source digital identity system that nations can reuse freely.

One of the first projects that puts the SSI approach into practice is the "ID Wallet", a smartphone app launched by the German government (German ID Wallet – page 25).

Self-sovereign identity meets electronic identity

Contrary to these SSI activities, the national electronic identity documents used in many states (e.g., Belgium, Estonia, Finland, Germany, Spain, Ghana, and Nigeria) follow the traditional, centralized identity management approach. Attributes, such as the name, the birth date, or the fingerprint, are managed by the issuing authority. The user has only very limited possibilities to decide which information is stored on their document and the individual or institution who will verify the correctness of the data.


User
Electronic identity document
Wallet for Self-Sovereign Identity
Authentication
Attributes
Cloud storage for attributes

Source: cryptovision

An eID document (left) may complement and support an SSI wallet (right). It may also serve as an authentication means for cloud storage connected to an SSI wallet.

Despite SSI and eID documents taking a different approach to similar goals, they are not necessarily opposites. Ben Drisch, cybersecurity specialist at cryptovision, believes that the two technologies can even profit from each other. “The eID document is an ideal means for the user to authenticate against the wallet,” says Drisch. “It’s more secure and more convenient than a password-based solution.” If a wallet is connected to cloud storage, which might often be the case, the identity document can be used for access protection, too.

In addition, an eID document can contribute attributes to a self-managed identity. For example, the document holder might want to take data, such as the name, the date of birth, or health information from their eID card and include this information in their SSI wallet. Says Ben Drisch, “This means, technically speaking, that a user is capable of transferring data from the Logical Data Structure of their eID document to a decentralized identifier.” As the Logical Data Structure card is digitally signed by the issuing state, a proof of authenticity is automatically present in the DID represented as a verifiable credential.

These decentralized identifiers and verifiable claims provide censorship and tamper-resistant means, for citizens to give permission for validation of specific attributes of their identity data, while ensuring that other aspects of their identity remain private.

“All in all, the combination of SSI and eID documents has great potential, from which both technologies can benefit,” says Ben Drisch. Whether this potential will be seized, certainly depends on the states that issue eID documents. If these states are willing to provide their citizens the possibility to manage their digital identities themselves, we might see powerful SSI schemes cooperating with eID-document systems in the future. If, on the other hand, governments don’t support the SSI concept, it will be difficult to establish SSI-eID cooperation against their wills. The current EU activities suggest that at least some governments welcome SSI. ☒

German ID Wallet: A Promising Technology with Teething Trouble

With the “ID Wallet” (a smartphone app) the German government launched one of the world’s first SSI application pilots. The purpose of the ID Wallet is to store identity data of all kinds to allow the user to manage and share it.

As the first major application of the ID Wallet, the German Ministry of Transport together with the Federal Motor Vehicle Agency (Kraftfahrt-Bundesamt) and the Federal Printing Authority (Bundesdruckerei) created a digital driving licence. This virtual document, which can be used by every German citizen who has the permission to drive, simplifies car rental and car sharing. It is planned that the digital driving licence will completely replace the physical document used in Germany so far.

The first version of the ID Wallet, introduced in September 2021, soon became a victim of its success. The high demand for the new app led to the server infrastructure being heavily overloaded. In addition, experts found potential security holes allowing for data and identity theft. As a reaction, the ID Wallet app was withdrawn from the app stores after only one week.

These problems can be regarded as the usual teething trouble every new technology encounters. It is expected that the server infrastructure will be extended and the security weaknesses fixed within a few weeks. All in all, the ID Wallet and the digital driving licence are generally seen as promising innovations that might lay the foundation for other SSI projects to come