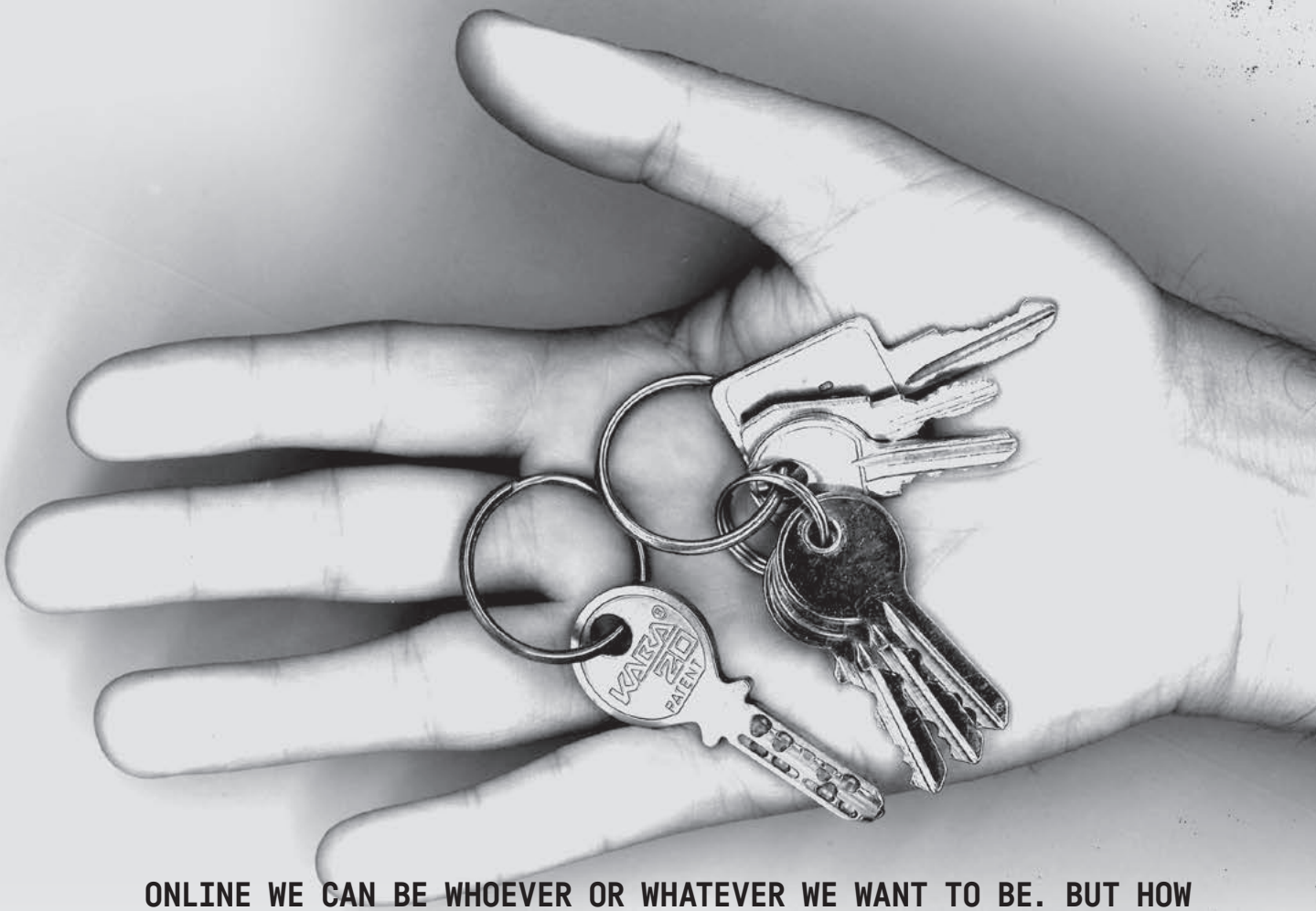
Self-sovereign identity: an ecosystem of digital identities



ONLINE WE CAN BE WHOEVER OR WHATEVER WE WANT TO BE. BUT HOW DO YOU MAKE SURE AN ONLINE IDENTITY IS GENUINE? SELF-SOVEREIGN IDENTITY IS A NEW WAY OF CREATING TRUST IN THE DIGITAL WORLD – AND IT GOES WAY BEYOND WHAT WE CURRENTLY UNDERSTAND AS IDENTITY.

EXPERT ARTICLE

_CATHARINA DEKKER
Consultant
Ergon Informatik AG
_MICHAEL DOUJAK
Product Manager Airlock
Ergon Informatik AG

Published in SMART insights 2022 magazine

ergon

smart people – smart software®

Online you can be anyone you want, from a prince or model to a billionaire heiress. It's difficult to officially verify digital identities. That's set to change soon. What the identity card or passport is to the physical world, the self-sovereign identity (SSI) is to become to the digital world. SSI enables physical proofs of identity to be translated into the digital world. It's standardised and trustworthy, highly tamper-proof and verifiable – and just as importantly, it's data protection compliant.

2 Username and password are insufficient

If you want to identify yourself on a web service you currently need a username and password. Most service providers use a local identity model to identify their users uniquely. There are many disadvantages to this. Providers have a duty to manage these data securely, and in the event of a data breach face the prospect of financial damage by way of consequential costs and loss of reputation. Users have to manage their many different accounts and passwords, which requires a lot of effort. To remedy this, in recent years federated identity has been established, with users able to identify themselves with the login of third-party services such as Google or Facebook. This single sign-on is particularly useful for access solutions with lower security requirements. But it's not enough for companies that require strong authentication. What they need is decentralised identification.

Creating a legal framework

Efforts are presently under way to create a legal framework for internationally recognised decentralised identities. After Swiss voters rejected the E-ID scheme in 2021, legislators in Switzerland are now working towards what's called self-sovereign identity or SSI. The consultation period for the new law is due to open in mid-2022. The EU has created a framework for a European SSI scheme, with pilot projects planned in the next few years. North America is also taking this path: the W3C standardisation body is working on a standard for self-sovereign identities. SSI is a good solution from a data protection point of view: it functions in accordance with the regulations on the processing of personal data that are currently widespread. Decentralised identification also makes it easier for providers to manage data. Thanks to the peer-to-peer character of SSIs, basically fewer service providers are involved in the data management chain. And because they store less sensitive data, the consequences of data breaches are less drastic.

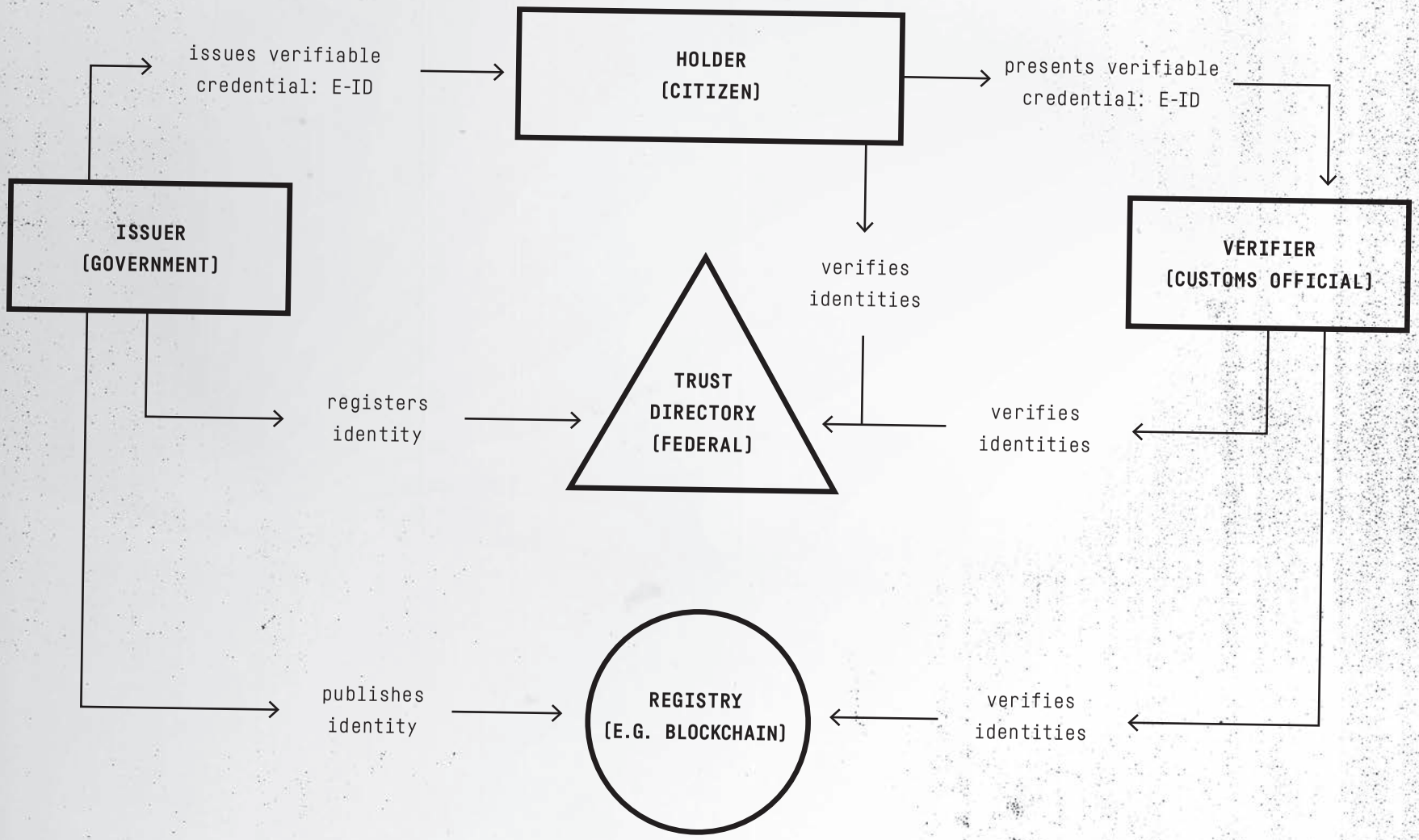
Users in charge of their data

The decentralised nature of SSI represents a paradigm change. Rather than providers, it's now the users themselves who manage the authentication data. To do this they store verified identity data, known as credentials, in a wallet on their smartphone or another device. From a driving licence to a certificate to social media history, these credentials are far broader than those represented by an analogue passport or identity card. An issuer attests to the correctness of the credentials electronically, and the service providers, or verifiers, also check them electronically. The holder or user gets to decide what data a verifier sees. It's the holder, and only the holder, who has sovereignty over their data. But this privilege also comes with duties. For example, if you lose your wallet you have to take care of replacing your entire IDs and documents yourself. The upside is that there are no complicated log-in procedures and the need to manage passwords accordingly.

What SSI can do in real life

An SSI has many advantages. Banks, for example, will benefit from the recognised digital E-ID: instead of going to a local branch or going through a complicated online identification process, all the customer will

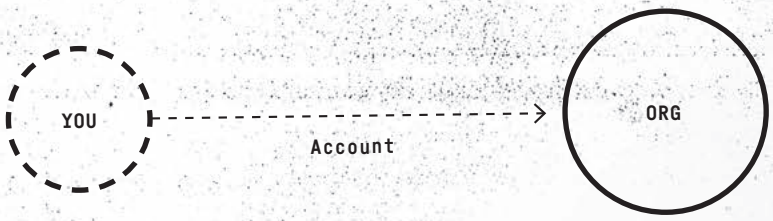
The SSI concept illustrated with the example of the Swiss E-ID



Three types of digital identity

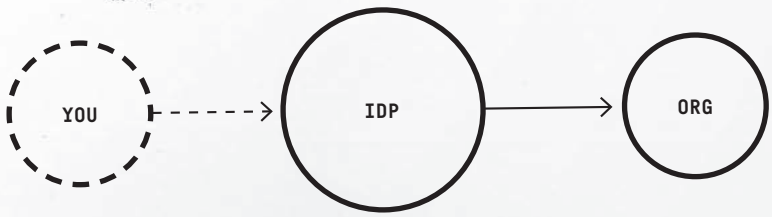
Description

SILO



- Users have their own user account for each provider
- The oldest and most widely used digital identification model

IDENTITY PROVIDER



- Users have their user account at an identity provider
- The identity provider confirms the user's identity to service providers

SSI

- Holders (users) have their own wallet in which they store their verified personal data
- Issuers the holder trusts are permitted to put data in their wallet
- Verifiers (service providers) get only data approved by the holder

Pros	Cons
• Widely established • Service providers manage compliance, liability, and other risks • Good privacy protection because no central body is involved • Well accepted in the population	• Very hard to scale for individuals • Reuse of passwords is a security risk • People lose track: where did I create my profiles? • Every provider must become an expert in identity management and security • Authentication is unilateral rather than bilateral → makes phishing possible
• Users can reduce the number of user accounts (and passwords) they have to manage themselves • Identity providers offer an SSO experience • Easy for service providers to implement with little integration work and expense	• Privacy insufficiently protected. The identity provider knows all my service providers • Few service providers accept identity providers • Most identity providers work at a low level of trust and are not suitable for e-banking or healthcare • Identity providers hold large volumes of personal information → security risk • Authentication is unilateral rather than bilateral → makes phishing possible • Only works for individuals, not for authenticating companies or objects
• Holders retain control of their data • High level of privacy protection because there is no central entity that could monitor holders • Verifiers receive verified data • Issuers can declare data as invalid (e.g. home address) • Data can become invalid after a certain time (e.g. tickets) • Standardised and interoperable → no dependence on a manufacturer • Access data, relationships and history aren't lost when a service provider is changed	• Standards are only now being created and could still change • Solutions enabling holders to safeguard their wallet from defects or loss still have to be worked out • People still have reservations and security concerns because the technology is complex and not yet widespread

"SSI will revolutionise our digital interactions."
_Catharina Dekker, Consultant, catharina.dekker@ergon.ch

have to do is pull out their wallet and have the necessary credentials ready. SSI will also make hiring a car easier because it will no longer be necessary to copy your ID card and driving licence. It might even be possible for people hiring a car to jump in and drive off directly because the smart car will be able to find and check its key in the form of verifiable credentials in the wallet.

Digitally certified documents such as references and diplomas will also make job applications easier, and potential employers will be able to check the authenticity of the documents on an automated basis.

To grant someone a young person's or senior citizen's discount you have to know their age. But there's no need to reveal your exact date of birth to a transport company or museum. When you also consider that 99.999% of people in Switzerland can be clearly identified on the basis of their full name and date of birth, it's obvious that processing dates of birth is particularly sensitive from a data protection point of view.

In e-commerce, traders will benefit because SSI will enable an instant credit check and rapid payment – with credentials that are directly linked to the purchaser's bank. Purchasers will also be able to check the trader's credentials to avoid buying at the wrong online shop and losing money.

Broad definition of identity
Credentials aren't necessarily limited to individuals. Companies and institutions will also be able to obtain an SSI and use it in communications with customers and suppliers. That could be new bank details for customer invoices or the current extract from the commercial register for suppliers and partners. It would even be conceivable for autonomous vehicles to have their own wallet, which they could use, for example, to pay tolls and workshop repairs independently. In this case their "identity" could be linked to their vehicle ID number. These examples show what enormous potential SSI has. If governments manage to resolve the "chicken-and-egg" problem of introducing SSIs, an increasing number of use cases are also likely to be economically viable as well, especially with digitalisation progressing by such leaps and bounds. The McKinsey Global Institute has predicted that in 2030, digital ID coverage could unlock economic value equivalent to three per cent of GDP in industrialised countries and as much as six per cent in emerging economies.

"The question isn't if SSI will come – but when."
_Michael Doujak, Product Manager Airlock, michael.doujak@ergon.ch

Can trust be managed?
For all the benefits of self-sovereign identity, there are challenges as well. How, for example, do you make sure issuers are really trustworthy? One solution would be to create trustworthy directories. Issuers – health insurers, say – could be verified and entered in the directory for inspection by verifiers and holders. Public authorities could have a government directory. This is how trust could be managed, so to speak. Another problem has to do with life-cycle management for credentials. How can they be updated in a way that's legally watertight? What happens if someone loses their wallet or a credential has an expiration date? Here ways need to be found of creating digital trust.

Early adopters profit
Even though some questions are still unanswered, self-sovereign identities will unlock enormous economic value. If you want to get some initial experience with SSI you can try the available open-source technologies. A successful proof of concept will enable companies to see the possibilities of the new technology and harness this potential more effectively. SSI is so much more than a digital identity card: it takes the definition of identity into dimensions that can't yet be imagined. If we as users have our digital identity under control, it also changes the way we approach privacy in the digital space. We might no longer be able to pass ourselves off as princes, models or billionaire heiresses, but our digital relationships and interactions will take on a whole new form. />