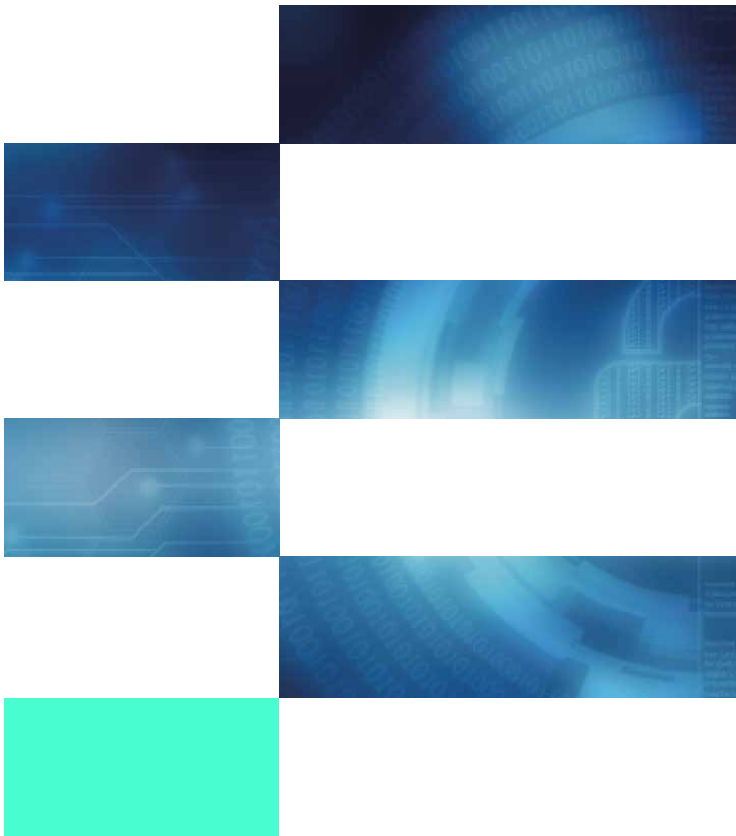
esatus

A trusted internet.
Easy and secure.
For everyone.

Enabled by digital credentials and SSI technology.



05
21

Building trust through digital credentials and Self-Sovereign Identity (SSI) – user-friendly and available for everyone

Digital processes, wherever they are available at all, are often exceedingly complex. We want to make the digital world accessible to everyone, in an easy way and without barriers. This can only be achieved through a solid trust base.

The prerequisites already exist under the name of Self-Sovereign Identity (SSI), a new, decentralized technology. Thanks to SSI, we can move around in the digital world just as easily and with the same amount of control as in real life. Usernames and passwords are no longer needed. Fraud protection and up-to-date validity become the new norm. To achieve this, SSI uses digitally verified credentials.

Self-Sovereign Identity (SSI)
The digital credentials described here follows „Self-Sovereign Identity (SSI)". This is a secure digital identity model that respects privacy. It follows various human-centric principles, such as interoperability, decentralisation, representation, portability, security, verifiability and authenticity (Principles of SSI - Sovrin). In essence, this means that SSI gives users full control over their personal data and allows them to determine who has access to which of their data and for what purpose. Accordingly, there is no controlling authority that grants or tracks access to this data.

Credentials are quite easy to use. Think of them as the digital version of an ID card or a driving licence: instead of carrying them in a wallet, you store these credentials in a digital wallet app on a mobile device. This allows you to have all your credentials at hand any time, and to present them when needed, for example at a government office, a car rental agency, or an employer. Wallet apps from various providers can be used. Credentials based on SSI technology ensure that all essential data which are required for the verification of the credential are stored in encrypted form on decentralised databases[1]. This includes information on the credential issuer and the current validity status (a driving licence, for example, can be revoked). This information can be verified at any time. The data is permanently stored in the database and cannot be deleted, therefore credentials are secure against manipulation.

Data sovereignty is arguably the decisive advantage of these credentials. The user alone has complete control over access to his personal data, because it is only stored in his wallet on his mobile device, not on the database. He decides with whom he shares which data and can see who has access to it. This ensures compliance with the highest regulations on data protection, such as the General Data Protection Regulation (GDPR).

Sample use case: test credential

More than a year after the start of the Corona pandemic, we all long for more normality. Imagine being able again to safely attend an event, visit a restaurant or travel without risking to infect others or get infected yourself. All this may soon be possible again - thanks to innovative credentials based on Self-Sovereign Identity technology. We would like to use a current use case to illustrate how digital credentials are issued and used. Please follow our protagonist Sam through a day during the Covid-19 pandemic of 2021.

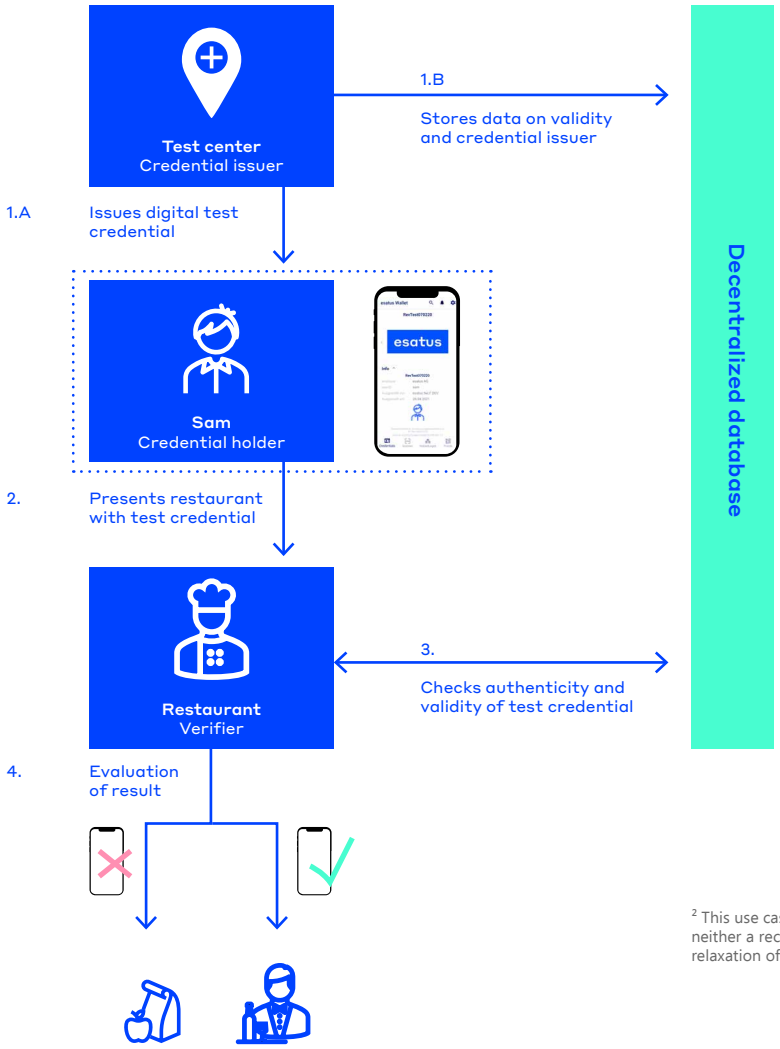
[1] For the sake of simplicity, we will refer to a decentralised database only as "database". For more information on this subject please see the info box on p. 3.

Functional principle of credentials[2]

Decentralised database
Decentralised databases are based on a distributed system, a network of databases (distributed ledger), which all store the same information, synchronise it and make it available at any time. Distributed ledgers offer high availability, scalability, resistance to manipulation and are excellent for interoperability. They act as a trust anchor for the stored data and ultimately for the credentials. Distributed ledgers are not to be confused with blockchains! The latter have a very high energy consumption due to the consensus process. Distributed ledgers, as used in this example for an identity network, work with a different mechanism than the classic blockchain and therefore have very low energy requirements.

Sam has just received the result of his Covid-19 test from the test center. His test certificate is now issued as a digital credential (step 1.A in figure). To do this, Sam simply scans a QR code with his smartphone, confirms receipt of the test credential, and saves it in his wallet app - Sam's „Corona" credential is ready!
This credential is only valid on the day it is issued. The validity and all other data which are required to authenticate the credential are stored on a decentralised database (step 1.B in figure), as well as the information about the issuing entity (here: the verified test centre). The database thus represents a trust anchor and vouches for the authenticity of the credential without storing any of Sam's personal data - which is solely located on Sam's smartphone in his wallet app.

That same evening, Sam wants to go out dining in a restaurant. To minimise the risk of infection, a staff member of the restaurant checks each guest at the entrance to see if they have a valid test result. When it is Sam's turn, he scans a QR code on the tablet of the staff member with his smartphone. A prompt appears on Sam's smartphone asking him to provide proof of a valid Covid-19 test. Sam's wallet app sends a response with the information about the test result to the staff member's tablet (step 2 in figure). Personal data such as Sam's insurance number or date of birth are not transmitted. On the back-end, the restaurant's app checks the authenticity and validity of the requested information on the database (step 3 in figure). The wallet app confirms Sam's test result (step 4 in figure) – and thus enables him to enter the restaurant.



[2] This use case is a virtual scenario to illustrate the benefits and functionality of digital credentials. It is neither a recommendation for behavior during the Corona pandemic, nor is it intended to advocate a relaxation of current Corona procedures.

This is just one of many use cases for SSI technology - discover the wide range of applications.

Automotive

A practical use case for credentials based on SSI-technology has reached production stage in Switzerland. esatus has implemented an efficient and future-proof identity and authentication process at Cardossier, a platform for vehicle documentation. In the future, users will be able to identify themselves much more easily with credentials and to log in without a password. Find out more in our press release.

User authentication in an eco-system

Healthcare

Whether at work, with friends or in public areas – it is helpful to know that my counterpart has formed antibodies. This proof is issued as a digital certificate, stored in the wallet app and presented as a QR code on request. The verifying party scans the QR code and immediately sees the result. esatus developed this prototype ready for production for the COVID-19 Credentials Initiative (CCI).

Covid-19 immunity certificate based on detected antibodies

Construction Sector

For several months, digital credentials have been applied at a large construction site in a pilot application. They are used to efficiently control and document site access and for checking specific permissions. Considering the many companies involved (subcontractors, suppliers, specialist planners, architects and many more), the procedure ensures greater efficiency and smooth handling for construction site management.

Access control at a large construction site

Transport & Logistics

Digital credentials have successfully passed a two-month test implementation at DB Systel GmbH. Without entering a password, employees can now access the group software by simply scanning a QR code with their mobile device, so that they are identified and authorized to access the system. Our solution SeLF could be integrated without the need for changes to the existing IT infrastructure. For more details read our press release.

Log-on process for a software application (PoC within a corporate structure)

Publisher: esatus AG

Copyright Fotos: jijomathai_XL/ Fotolia; Tierney/Adobe Stock; Smileus/ Adobe Stock; CREATIVE WONDER/ Adobe Stock; TTstudio_XXL/ Fotolia

Version: 1.0

A trusted internet.
Easy and secure.
For everyone.

esatus stands for a free, secure, and human-centric digital future. We build bridges between today and tomorrow.

We shape digitalization processes in a future-oriented way and offer solutions from a single source – from conception to individual software development to operational management. Another focus is the field of information security (InfoSec). We take a holistic approach when advising companies on the topic of identity & access management and help them to implement compliance and data protection requirements (GRC).

Since 2015, we have been a passionate driver of Self-Sovereign Identity (SSI) in Germany and are now one of the global technology leaders. SSI places the individual at the centre of the digital ecosystem and enables user-friendly and self-determined control of personal data.

esatus