No need to turn up personally: SisuID improves electronic authentication

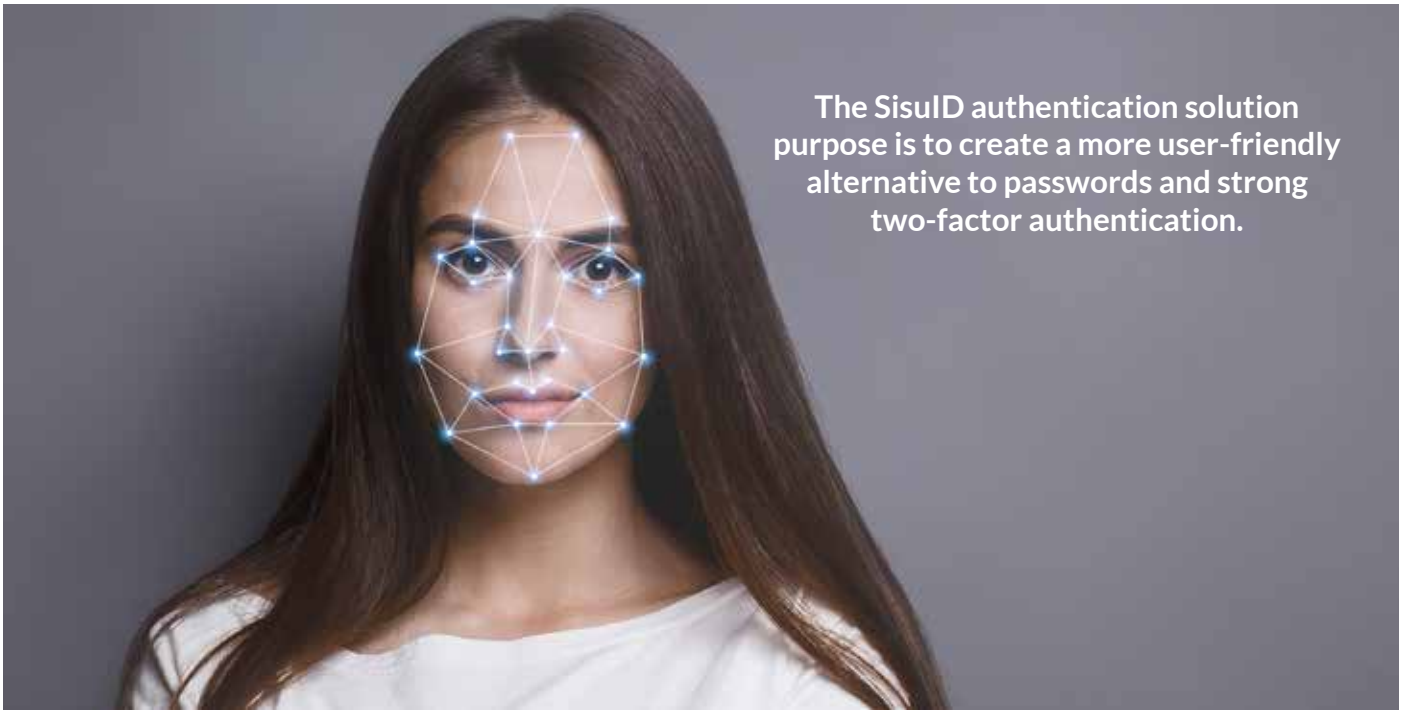
In order for researchers to access the digital services of various research infrastructures, their identity and relationship with the research organisation must be verified. Until now, this has required a personal visit to a registration point where their identity document has been checked. Finland has been testing a new solution for strong electronic identity proofing that does not require a personal visit to a registration point.

Authentication ensures that the person is who he or she claims to be. At the moment, researchers can use their home organisation's credentials when logging into infrastructure services. Logging into services containing sensitive data, for example, nevertheless requires a more reliable authentication method, but these are not available in all home organisations.

"Traditionally, identity proofing is considered reliable if a person has to visit a registration point in person, with trained personnel checking his or her passport or other identification document issued by an authority", says Senior Application Specialist **Mikael Linden** of CSC.

"ELIXIR's AAI service enables electronic user authentication and the authorisation."

Together with the Czech centre (Institute of Organic Chemistry and Biochemistry of the CAS), the ELIXIR Finnish centre, CSC, has long been developing authentication services for infrastructure. ELIXIR's AAI service (Authentication and Authorisation Infrastructure) enables electronic user authentication and the authorisation. Access to gene data, for example, is always decided



by the data owner, but the AAI will make access to data quicker.

The AAI service is effective but requires that the researcher is reliably authenticated. In general, the solution is a federated identity management, which is simple and easy to manage. A single log in and your home organisation's user ID also provide researchers with access not only to services outside their organisation, but also to closely protected data collections. What if your home organisation cannot provide sufficiently reliable authentication?

CSC has been working together with the Sandbox of Trust project, which also involves the cybersecurity services company Nixu. The project has developed the SisuID authentication solution, the purpose of which is to create a more user-friendly alternative to passwords and strong two-factor authentication. A user uses a smartphone application to enrol their unique identity. A combination of these also enables the secure transfer of personal data between services, based on the person's own approval.

"In a research infrastructure like ELIXIR, identity proofing in a network of registration points would be expensive and cumbersome for end users. With the SisuID concept, identity proofing is carried out by taking a photo of themselves and their passport with the SisuID mobile phone application, which will check that the two match", says Mikael Linden.

Algorithmic facial recognition

SisuID is an open source code identification method that has been tested in five different pilot projects. According to **Joonatan Henriksson**, Head of Digital Business at Nixu, various ways have now been tested of reliably registering and identifying Finnish and foreign persons.

"In Finland, strong electronic authentication can currently be carried out using bank credentials, but this is not possible for foreign researchers, and not all countries have a national strong authentication method in place", says Mr Henriksson.

He points out that, with the cross-border solution now being tested, persons performing identity proofing will use their mobile device to take a photo of their passport or ID card, and a photo of their face. These are compared algorithmically.

"The comparison can also make use of registers available in the country that issued the identity document, and, for example, Interpol databases for forged identity documents."

But there are also more stringent identification criteria.

"If the service provider does not consider the remote identification sufficient, we can increase the identification reliability level by having the person visit a physical location for identity proofing, after which the more reliable identity will be available to all service providers using SisuID."

According to Henriksson, the identification criteria will comply with the eIDAS EU regulation. The eIDAS regulation creates a framework for providers of identification services, on which, for example, the Finnish Act on Strong Electronic authentication and Electronic Signatures is based. By complying with the eIDAS regulation, providers of electronic authentication and signatures can apply for official approval of their services, qualifying the authentication method for cross-border central government transactions.

"We will also be able to access a facial image on a passport's NFC chip, signed by the party that issued the passport, and take a liveness video of the face, further increasing the electronic reliability of the registered identity."

To produce the SisuID solution, anon-profit identification cooperative is being set up that will divide the benefits, costs and risks of the identification service between the organisations that use it.

Once a person can be authenticated efficiently and reliably, the only problem that remains is that the data related to the person is located in silos. For the moment. Access

to services provided by ELIXIR, for example, could be granted by combining two pieces of data: a reliably registered digital identity and assertions related to a person. A researcher can convert a university's assertion on their affiliation or an EU grant decision into electronic format, making their research status official.

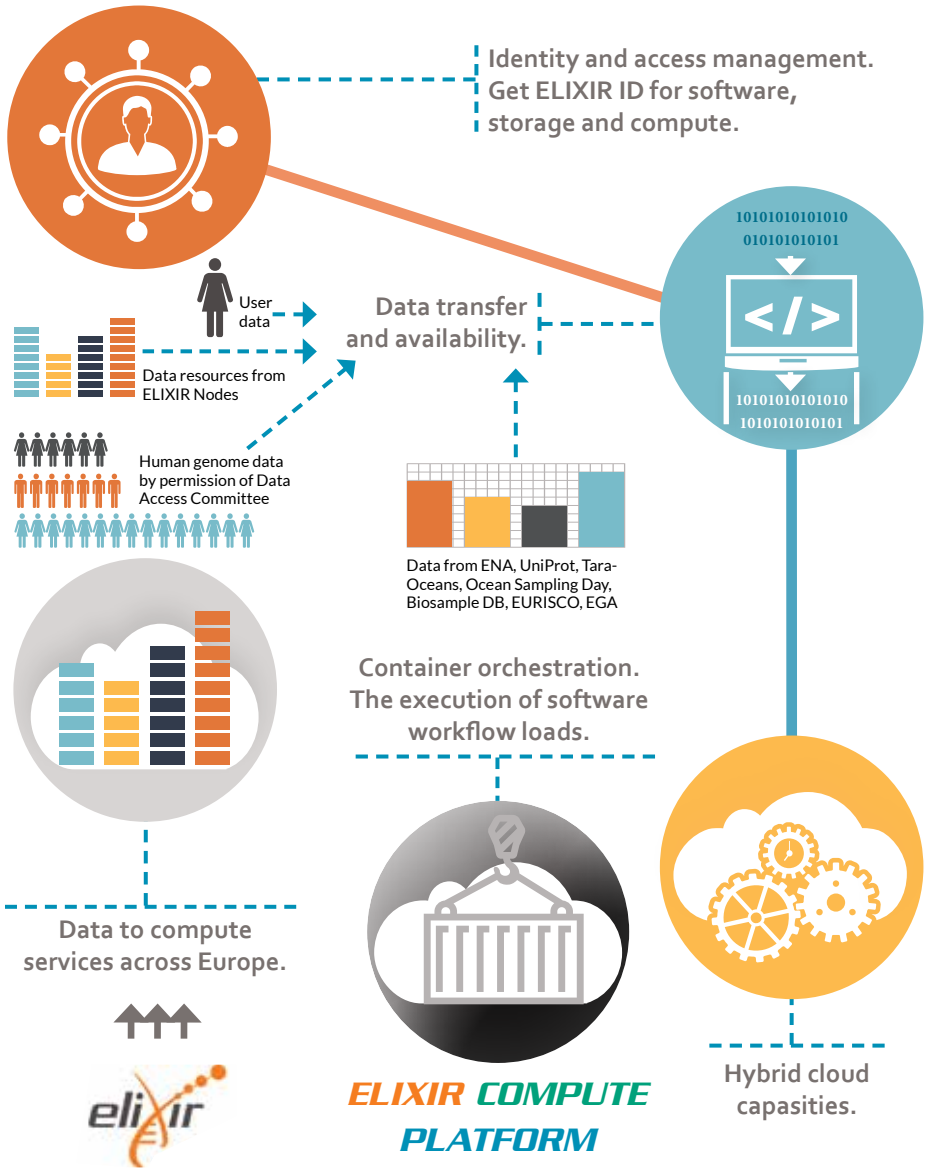
"In future, such electronic data linked to an identified person's digital identity could be sent between actors by means of distributed, confidence-building, cross-border blockchain networks."

As the name implies, data is stored in blocks in blockchains. A block is connected to the previous one with an algorithm that turns the data into a character string. Data entered in a single block cannot be changed afterwards, because the blockchain has been distributed to several computers.

This method enables the digital distribution of confidential data without

having to reveal the interfaces of national registers, for example. The fact that blockchains cannot be changed ensures reliable data transfer by the users themselves, which means that no direct integration between the interfaces is required. Examples of this include EU-level testing in the European Blockchain Services Infrastructure (EBSI) project concerning the transfer of electronic educational certificates.

Ari Turunen



MORE INFORMATION:

https://sisuid.com/fi/

https://www.nixu.com

CSC – IT Center for Science
is a non-profit, state-owned company administered by the Ministry of Education and Culture. CSC maintains and develops the state-owned, centralised IT infrastructure.
http://www.csc.fi
https://research.csc.fi/cloud-computing

ELIXIR
builds infrastructure in support of the biological sector. It brings together the leading organisations of 21 European countries and the EMBL European Molecular Biology Laboratory to form a common infrastructure for biological information. CSC – IT Center for Science is the Finnish centre within this infrastructure.
http://www.elixir-finland.org
http://www.elixir-europe.org

SUOMEN ELIXIR
Puh. +358 9 457 2821 ● e-mail: servicedesk@csc.fi
www.elixir-europe.org/about-us/who-we-are/nodes/finland

www.elixir-finland.org

ELIXIR PÄÄMAJA
EMBL-European Bioinformatics Institute
www.elixir-europe.org