Trust in central government

Nikolaos Saklampanakis comments: "Germany is a by design federal country. The need for decentralization of responsibilities and authority is claimed from both societal and governmental sides. On a political level, this has become even more evident after the adoption of an official blockchain strategy from the federal government.

"Unlike in other European nations and countries around the world, central government is trusted in Germany, but people feel that local societies can better influence their governments for policy making that has a real impact on their everyday lives. The central government is trusted for long-term planning and state continuity, but it feels a bit disconnected from the citizens. Moreover, concentration of power is generally not favorable due to historical reasons in Germany too."

The practical difficulties experienced when implementing digital identity solutions

But even when there is appetite for digital identity solutions, often practicalities can impact the viability of the solution for citizens.

"Spain rolled out the first digital ID (eDNI) in March 2006, and since then every Spaniard has an eDNI", says Carlos Cordero.

"Every eDNI integrates in a secure chip all of the information printed on the card, plus the face of the owner, their handmade signature, fingerprints and most importantly, digital certificates allowing the user to digitally interact with many public services, as well as banks and online shopping for example. No other personal information is stored on the eDNI whether health, fiscal, or penal.

"But its use hasn't spread, which is down to technological difficulties – until Windows 10, it was very problematic to install the software stack to be able to use eDNI from a computer, not to say on Linux or MacOS.

"From a cultural perspective, Spanish citizens would be happy to use an Elliptic Curve Cryptography (ECC) certificate digital ID where eDNI would be integrated.

"For example, initiatives such as Alastria_ID – a digital identity model for use in digital service and inspired on Self Sovereign Identity (SSI) concept – has been proposed to be used as European standard and has become a benchmark in Spain and Europe.

Frederik de Breuck adds, "For a self-sovereign identity solution to work for example, it must be secure, controllable and portable. Specifically, the identity and information must be kept secure, the user must be in control of who can see and access their data, and the user must be able to use their identity data whenever they want and not be tied to a single provider.

"Regulations like the Electronic Identification, Authentication and Trust Services will pave the way to a cross-European digital identity scheme but this has yet to be fully implemented in al the countries. The Alastria_ID model for example goes beyond Distributed Ledger Technology itself and if it is accepted as a European standard, will accelerate the SSI concept and minimize any cross-border challenges."

Digital identity with integrity provided by Distributed Ledger Technology

Whilst it is dangerous to hold all citizen data through centralized means, digital identity with integrity provided by Distributed Ledger Technology (DLT) empowers citizens by ensuring that "digital wallets" held by each individual will be connected to the distributed system.

Giving citizens control of each wallet will hold personal data for identification purposes, as well as a range of other records such as transaction accounts, financial history, medical records, consent tracking and academic records. Individuals can then prove who they are, the assets they own, and their levels of education for example.

DLT-based systems have the following characteristics:

- They do not have to be controlled by a single authority and are based on consensus.
- They provide an immutable record of transactions which are time-stamped, ensuring users have a reliable record of interactions.
- They create a transparent record of transactions that can be validated by anyone participating in the network.

Whilst there are different approaches for digital identity solutions – SSI being one approach – the technology has the potential to strengthen the way citizens, governments, and businesses interact, by enhancing privacy and trust, reducing risk, and improving the efficiency of operations. It is something that is being implemented, tested, and trialed today.

> "[DLT-based systems] provide an immutable record of transactions which are time-stamped, ensuring users have a reliable record of interactions."

Zug ID

This initiative pioneered by the local government in the Swiss city of Zug, saw a digital decentralized, sovereign identity provided to each of its citizens, enabling them to participate in government-related activities such as being verified by city officials, casting votes, and accessing government services.

One early example of how the system was used was by enabling citizens to vote on the presence of fireworks at an upcoming festival. The adoption of a decentralized identity is seen as the first step in enabling the creation of many smart services in the city. In the future this could include the use of autonomous buses and library services for example.

Credit Bureau of the Future

In 2018, a pilot was launched between international non-profit Kiva, Sierra Leone and United Nations Capital Development Fund (UNCDF) to test a DLT-based digital identification system. This was designed to provide users with greater control over their personal, transaction and credit information, with the fundamental objective of the system being to support the financial inclusion of every resident in the country.

The European Blockchain Services Infrastructure

The EBSI is a joint initiative from the European Commission and the European Blockchain Partnership (EBP) to deliver EU-wide cross-border public services using DLT. A key aspect of this is the potential to implement a generic self-sovereign identity (SSI) capability, allowing users to create and control their own identity across borders without relying on centralized authorities.

ID_Alastria

Founded in 2017, with Fujitsu as a founding member, Alastria is a non-profit association that promotes the digital economy and anticipates the needs of society, in relation to the use of products and services based on decentralized technologies.

ID_Alastria is a digital identity model proposed by the association, based on an SSI model that allows transactions on the Alastria network to be legally valid and confirm to European regulations.

Enhancing Operations and related values

While an element of this debate is about changing the rules in issuing identities, the key focus for a DLT-based digital identity solution is to manage the proof of identity for the ease of the citizen. By enabling citizens to selectively disclose proofs of attributes that are bound to their identity, tracking and managing the consents that were given, the way you manage and run your day-to-day operations can be enhanced.

Increased operational inefficiency is the key driver behind the adoption of DLT for 62% of organizations.[1]

So, how can this work in practice?

Today's application of Distributed Ledger Technology

"DLT technology will become very pervasive with a variety of applications (leveraging the power of smart-contracts) in sectors such as banking, transport, logistics, document management, agri-food, health, human resources, NGOs and education among others", says Carlos Cordero.

"Digital identity will be a key component of most if not all of those applications. Specifically we're already seeing its use through DiplomE, a global ecosystem from the Italian Government in which marks and certifications of students are managed safely reducing the risk of counterfeiting.

"Claudia, is also a decentralized autonomous organisation (DAO) that pursues the United Nations sustainable development goal (SDG) 10 (Reduce inequality within and among countries) through which government activities can be carried out, including voting, surveys, and assessments."

Creating essential trust in a post-pandemic world

In a post-pandemic world this could be more important than ever. Nikolaos Saklampanakis offers the following illustrative example.

"A citizen holds an analog/paper certificate, issued by a regional hospital in the Netherlands, proving her immunity to a virus during a pandemic. The holder is currently in Berlin and shows the certificate to the entry guard of a conference in Berlin, to be allowed to enter. The entry guard must be able to verify the validity of that paper certificate, by analysing its physical properties: It must look and feel genuine and valid, and then he can choose to accept it or not based on his own judgment.

"With a DLT digital certificate, the holder can provide proof of holding an immunity certificate and the entry guard can verify the validity of the certificate based on its digital properties and cryptographic attributes in a secure and verifiable way: as easy as scanning a QR code with a mobile app. It's not about how the certificate looks and feels, it is about what it actually is and claims.

"Such a digital certificate would provide both parties – prover and verifier – the benefits of digital nature, but also the propagation of trust due to the DLT layer behind it.

"In this example, the validity of the digital certificate can be proven by the conference organizer due to the traceability of the chain of trust the DLT enables: it is issued by an actual hospital in the Netherlands, recognized by a Dutch national health organization, which is a recognized authority by the German state. Even though the conference systems for the event in Berlin are not directly integrated with the hospital in Netherlands, the entry guard can securely verify the validity of the certificate and allow entry."

Successful digital government innovation

"This kind of invisible government – one that proactively anticipates the events in each citizen's life and giving them what they need when they need it – is already in operation in Estonia", confirms Patrick Stephenson.

"That comparatively tiny country in northern Europe is the world leader in terms of delivering e-services to its population. And it's all based on the principle that citizens should be able to choose what happens with their data.

"It is clearly better for the individual people, but it also helps the government run more efficiently.

"Returning to our previous disability benefit example from the UK, currently, disability benefit has to be independently vetted by an external contractor. In an automatic, digitally-enabled system, the cost of this external contractor could be removed.

"And of course, the time efficiencies speak for themselves.

"Civil servants won't have to spend so much time chasing paperwork, while citizens get access to the services they need faster. It's better for everyone."

1. Taking The Pulse of Enterprise Blockchain, a commissioned study conducted by Forrester Consulting on behalf of Fujitsu, May 2020.

Implementing government digital identity solutions

Currently the debate might feel a little conceptual. You may have questions about the viability of a digital identity system right now or have concerns about the practicalities of implementation.

While it might appear too far in the future, the reality is that the first steps can be followed now. However, before any action can be taken, it is crucial to look closely at your current ways of working, systems and processes to understand what the best potential solution could be. Only then could it become a reality.

Digital identity and the technology landscape

Digital identity is no doubt a hot topic, with SSI being one way to deliver it, but there are many others. Here our panel explain more about digital identity and the landscape of technologies in the space.

The fundamental principles of self-sovereign identity

"SSI allows the holder to present verifiable credentials in a privacy-safe way", says Leopold Sternberg. "The fundamental principles are described as follows

- Organizations can grant credentials with given attributes to a holder
- The holder is enabled to disclose selectively, attributes of those credentials to those who ask them based on context
- The party who asks for such credentials from the holder can cryptographically verify their validity in a way that preserves the privacy of the holder (following the zero-knowledge-proof idea)
- The holder can decide what they show to whom in what context and is the sovereign of their attributes that characterize the identity

"This means that a user can interact with a range of government services with a flexible use of their identity as a citizen, an employee and as a customer for example. Specifically, this removes any password or credential chaos as well as avoiding any misuse and theft of their personal data. Most-importantly, the user can manage the data themselves and control what they do or don't reveal.

"For governments themselves this promotes user friendly services, strengthens trust with citizens, and ensures compliance with regulations. Crucially, it creates the ability to concentrate on the core mission of reducing administration efforts, increasing efficiency and promoting integrity of data and processes."

The advantages and disadvantages of SSI solutions

"SSI is not the only model for managing digital identities but seems to be a very good option for use in digital services, as individuals or businesses have sole ownership over the ability to control their data", says Carlos Cordero.

"Other identity management solutions require an intermediator – an identifier – to ensure the user of business is who they say they are. With SSI, identifiers do not need an intermediary.

"SSI also ensures the three key principles of Security, Controllability and Portability and is made up of claims (assertion of identity made by user, business or even a thing), proofs (eDNI, passport may act as evidence for a claim) and attestations or validations (another party validates the claim is true).

One of the disadvantages of SSI is there may be multiple identity platforms, hence the user or business may have to use multiple applications, says Frederik de Breuck. "But this will be overcome if for example a cross-border solution can be implemented on a common SSI platform.

"Another disadvantage is the fact that users, businesses, and things are responsible for their own security and data. But there are also many advantages on the SSI side (and big ones at that). It is more secure, less prone to breaches, data is more private, users, business and things have a higher control over their data and there is no need for intermediates to monetize your own data."

Protecting and tracking citizens' private data

Patrick Stephenson comments, "This technology makes information immutable. You can see if something has been changed, when it has been changed, and by whom – which is ideal for protecting and tracking citizens' private data.

"You can also secure it and choose to share it only with a select group of people. In much the same way that people already share data between the apps on their smartphones.

"And using DLT isn't impossible or scary. It's not really a new technology and certainly not the sole preserve of digital currencies – Estonia has been using it since 2008."

Integrating with existing systems and processes

The question that many governments have, is would this not completely change systems and processes for governments and their agencies?

"SSI does not change how certificates are issued", confirms Frederik de Breuck.

"Issuance of SSI certificates is not challenging the status quo of the authorities that adopt them or the technologies they already employ. SSI based certificates enable their holders to use them based on the context of interactions.

"When a city registry issues a paper certificate of residence, the certificate states not only the fact that the holder is resident of the city, but reveals more personal information like date of birth, exact address, full name, potentially the family status and more. Every time the holder needs to prove that he is resident of the city, he needs to reveal all this information, regardless of the context, which can be a potential privacy risk. At the same time, the verifier, has the challenge to decide on the validity of the certificate based on its physical properties, and also has the liability of handling sensitive information that might not be of any value to him (that can cause other challenges in terms of GDPR compliance)."

Privacy and data protection regulations

Privacy is a key factor to consider in the context of data protection regulations.

"SSI based certificates can help with this, even in parallel with the more traditional paper certificates", states Carlos Cordero.

"When issuing a traditional certificate, the city registry can also provide the citizen with the certificate in an SSI form. The process of issuing the certificate remains the same, as well as the regulations and the prerequisites. What changes, is the fact that the citizen, now has the chance to use their SSI form in a way that preserves their privacy, based on context. For example, they can prove that they are a resident of the city, to participate in a relevant decision-making process, while keeping all the rest of the information private – this is termed zero knowledge proof. The verifying party can also be sure that the SSI is valid due to its cryptographic attributes and without being liable for handling irrelevant private information."

Understanding the right approach to digital identities

There is no one-size-fits-all solution to improve the level of service to citizens.

Only 10% of DLT solutions have been fully rolled-out.[2]

Through a tailored solution that works with the needs of your citizens and improves their lives by empowering them with access services more easily through transparent, secure and personalized services, you can begin to enhance and promote your current ways of working and solve existing inefficiencies.

When an off-the-shelf solution is sought it will lack the flexibility to slot into current ways of working and to integrate with existing systems and processes.

The first steps involve a deep understanding of your government organization and the key issues to be addressed. Crucially, it is essential to collaborate with the right partner to find the most appropriate custom solution.

Why Fujitsu?

Fujitsu DLT incorporates an outcomes-focused co-creation approach. We work alongside key stakeholders and evaluate your organization to establish whether there is a need for a digital identity solution and the viability of DLT to provide this with integrity. We collaborate with you to establish whether a business case exists and will even provide support to scale these transformations to production.

The initial evaluation can be completed within a maximum of five days with an exercise called Proof of Business. This ensures proper alignment and understanding of the jointly selected use case prior to moving to a larger implementation or deeper testing; if Proof of Business is agreed upfront.

Our technology-agnostic approach and understanding that DLT solutions need to integrate with existing systems and processes, begins with the question of how to solve an operational need. The specifics and the unique nature of your organization defines the solution and the most appropriate mix of technologies.

This ensures that a one-size-fits-all technology platform is never imposed, with key infrastructure choices left in your hands.

> "The application of our Human Centric Experience Design (HXD) methodology – our unique exible, and proven iteration of design thinking – enables innovative concepts to be created at speed."

The following underpins Fujitsu's co-creation approach:

Focus on digital transformation solutions.
We understand that DLT is not the answer to all operational problems. By implementing decision tree approaches, we identify the most appropriate action. This underpins our commitment to co-creating trusted digital transformation solutions.

Through the pragmatism provided by our digital transformation and acceleration experts, and our platform agnostic approach, we retain focus on the issues and requirements of your organization as opposed to a technology solution. We ensure that DLT is only identified as a solution if it brings real added value to the needs of your organization.

Rapid and unique methodologies.
Within our global Digital Transformation Centers, our talented and experienced DLT-experts around the world, facilitate collaborative engagement alongside key stakeholders to achieve a dynamic mix of knowledge, creativity, ideation, and concept development.

The application of our Human Centric Experience Design (HXD) methodology – our unique, flexible and proven iteration of design thinking – enables innovative concepts to be created at speed.

Global ability to deliver end-to-end solutions.
Fujitsu's multi-disciplinary team includes IT developers, technology specialists, business engineers & analysts, process engineers, scrum masters, enterprise & IT architects, and legal experts.

By offering an end-to-end suite of modules, platforms, offerings and services, we enable efficient and quick resolutions to be sought. As a top five global integrator, our specialist knowledge ensures DLT systems are integrated deep within your organization, driving additional value across the wider ecosystem.

2. Taking The Pulse of Enterprise Blockchain, a commissioned study conducted by Forrester Consulting on behalf of Fujitsu, May 2020.

Summary

Improving the lives of its citizens is key on every governments' agenda. Digital identity has been a hot topic to support this objective for several years and is one that continues to attract debate across the globe. It is also one that stirs passion in people throughout the world on either side of the argument.

And while it may feel conceptual, through the open dialogue with our Fujitsu digital technology specialists, we've seen that it is a very real possibility for governments anywhere in the world. Digital identity with integrity provided by DLT can enhance the way that governments run and manage their day-to-day operations as well as empower their citizens and promote trust.

It might feel like a future topic, but with the right approach it can become a reality.

Learn more about Fujitsu's co-creation approach to Distributed Ledger Technology through speaking to one of our experts, and understand the potential to empower your citizens and enhance their well-being.

FUJITSU
1250 East Arques Avenue Sunnyvale, CA 94085-3470, U.S.A.
Tel: 800 831 3183 or 408 746 6000
Email: askFujitsu@us.fujitsu.com
fujitsu.com/us