Digital Government Services Transformed with Digital Identity

By Gary Lac
Vice President of Solutions Development

In an era driven by digital transformation, digital identity is one of the most innovative technologies reshaping our world. Decentralized Identity (DID) services have evolved from a concept to a disruptive technology redefining how we verify identities. This paradigm shift, particularly within government services, offers a viable replacement for traditional identity verification methods with streamlined, secure alternatives. Digital Identity can revolutionize public sector operations.

STATE OF DIGITAL IDS AND THEIR APPLICATION

Our present digital ID landscape navigates two dominant standards - the World Wide Web Consortium Decentralized Identifiers (W3C DID) and the ISO mobile driver's licenses (mDL). Commercial entities favor W3C DID for its potential to facilitate secure remote transactions, while government entities predominantly adopt ISO mDL designed for in-person transactions.

A compelling use case of the mDL is its utilization by the Transportation Security Administration (TSA). However, such exclusive use cases have led to a dichotomy in the digital identity landscape, prompting the question – could a more efficient and comprehensive digital identity system exist? Can we consolidate the benefits of these divergent standards into one?

THE POTENTIAL OF DIDS OVER MOBILE DRIVER'S LICENSES

The potential of DID services is limitless. We envision spearheading a transition that preserves the robustness and interoperability of the existing mDL framework while introducing efficiencies that could render the need for mobile driver's licenses redundant.

DIDs can expedite registrations, reduce administrative paperwork, and provide quicker access to government services. This streamlined user experience is a value-add for the citizens and a step towards enhancing organizational efficiency, thereby driving greater satisfaction.

In many cases, DIDs leverage similar levels of identity assurance (NIST IAL2) as government-backed credentials.

As users create these strong identity credentials with commercial organizations, they should be portable and reusable in a government services context. In addition, commercial organizations are quickly rolling out DIDs supporting avariety of use cases, from travel to financial services to customer experience. As more and more people adopt these DIDs, we want to capitalize on the user base and create more value.

FRAMEWORKS FOR EFFECTIVE DID IMPLEMENTATION

A recent McKinsey report* reveals that digitization of government services could save up to *$1 trillion annually* in economic value worldwide.

The implementation of DIDs necessitates a robust framework that accommodates all government verticals, right from applying for benefits, IRS tax services, financial services, and social security. A recent McKinsey report* reveals that digitization of government services could save up to $1 trillion annually in economic value worldwide. This statistic underscores the urgency for an integrated, comprehensive digital identity solution.

Despite this, specific standards present hurdles to achieving interoperability for some use cases, such as mobile IDs (mID) in law enforcement. There are practical challenges to how government agencies can verify digital identities in an in-person field scenario. However, the transition to DIDs can drastically mitigate fraud, a persistent issue within government services. According to the Federal Trade Commission, identity theft resulted in a staggering $56 billion in losses in 2020**. Decentralized digital identity presents a formidable solution to such fraudulent activities.

By sharing trusted identity data across government and commercial ecosystems, service efficiency can be dramatically enhanced. DID solutions offer a unique value proposition in this landscape, emphasizing direct sourcing and potentially negating the need for an mDL. Our cloud-based digital IDs are particularly commercially focused and relevant for digital services. Leveraging DIDs that are highly interoperable with digital services and adding verified trusted identity data from government sources will enable a vibrant ecosystem for digital identities.

In conclusion, the potential of DIDs to revolutionize digital government services is massive. The time is now for government agencies and law enforcement to consider this technology. As we continue this movement, we invite all stakeholders to join us on this journey, paving the way for a more efficient, secure, and citizen-centric future.

According to the Federal Trade Commission, identity theft resulted in a staggering $56 billion in losses in 2020.**

The NEC Advantage

NEC's DID solutions allow government agencies to accelerate their digital transformation. We can reallocate resources from manual and administrative tasks to more strategic, tech-driven initiatives by reimagining traditional processes. This shift could lead to significant cost savings and add value to the human capital aspect of public service.

With NEC's approach, citizens can control their information, leading to more efficient processes and quicker service delivery. A compelling feature of our DID services is a proposed "Trust Score." This feature adds a unique dimension to DIDs, offering a score based on your interactions, thus fostering a truly open, truly trusted system.

SOURCES:

*McKinsey Report: "Digital government: The path to delivering exponential value."
https://www.mckinsey.com/industries/public-and-social-sector/our-insights/digital-government-the-path-to-delivering-exponential-value

**Federal Trade Commission Report: "2020 Consumer Sentinel Network Data Book".
https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2020/csn_annual_data_book_2020.pdf

Copyright 2023.